Cyberbiosecurity. A short review

Caterina TOMULESCU,
National Institute for Chemical-Pharmaceutical R&D, ICCF, Bucharest, Romania

caterina_tomulescu@yahoo.com

Abstract

In the new digital age, life sciences tend to converge with information technology and cybersecurity. With the new developments in biomedical research and the scientific progress of modern biotechnology, there is an exponential multiplication of related information sets, which require cloud storage and advanced methods of management and analysis, as well as ensuring an adequate protection of their content.

The bioeconomy global landscape involves common, multiple and diverse actions (i.e specific policies and framework regulations, international cooperation, national collaboration among interdisciplinary sectors and different actors of the public-private system). At the same time, biosecurity issues highlight a complex and rapidly emerging ecosystem, which involves high-risk vulnerabilities. Moreover, the current pandemic context, generated by the global spread of the new virus, SARS-CoV-2, has pointed out some issues (i.e the importance of strategic autonomy in supply chains - 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 use of infectious biological agents, natural or artificial).

As science evolves, relying on the application of new technologies in areas such as artificial intelligence, process automation, bioinformatics and synthetic biology, vulnerabilities such as data confidentiality (i.e clinical, genetic information), cloud storage, intellectual property, may represent opportunities which could be exploited. Cybersecurity needs to be as robust as possible, anticipating and incorporating possible biological threats into its strategies.

This paper presents a synthetic overview of cyberbiosecurity available data, with the view to emphasize some of its strategic approaches currently used in the world/at the international level.

***Keywords**: modern biotechnology, synthetic biology, big data, cybersbioecurity, biosecurity.*

1. Introduction

Latest industrial biotechnologies have gained great interest, due to their wide applications in the economy, human health and environmental protection, areas which are facing global challenges and have generated and still generate deep concerns regarding climate change, environmental pollution, human and animal health, natural resources and biodiversity loss, food shortages and water scarcity. (35)

In a world which is racing in the fourth industrial revolution and also, in the new era of digitalization, there is an increased demand for alternative technologies and sustainable products based on the principles of bioeconomy, such as alternative energy sources, biomass conversion processes, bio-based bulk chemicals, biofuels, renewable feedstocks and medicines etc. Biotechnology has an enormous economic potential and, at the same time, it is promoting innovative applications for our common benefits; it could be considered as a sustainable tool for our future development, in which –omics sciences (genomics, proteomics, metabolomics, transcriptomics) and synthetic biology are used to cope with the most challenging global problems. (35)

Furthermore, in a context which estimates an increase of the global population to 9 billion by 2050 (United Nations: approximately 66% will be urban populations; World Health Organization: 1.5 billion people will be over 65 years), concepts such as smart and climate-neutral cities are gaining the attention of governments and regional/local authorities. World's largest cities have already adopted smart sustainable development goals, decision which has set the path for an estimated global market of $ 1.565 trillion by 2020. This means that smart cities decision-makers have already adopted the paradigm shift, that which we have noticed is being talked about more and more in the current pandemic context of COVID-19, and which means digitalization and implementation of modern and scientifically advanced technologies (i.e to develop smart infrastructures, including to store and manage big data, to automatize technological processes - robotics, systems of communications – WiFi and 5G Internet of things (IoT) technologies). At the same time, this shift creates new risks (often identified as vulnerabilities and threats), especially in terms of security (including cybernetic security, given that all these technologies, sensors, networks and infrastructures are based on internet access). In a report of the European Cyber Security Organisation (ECSO, 2018), the smart city was defined as a complex task, “the integration of data and digital technologies by the human being into a strategic approach to economic, environment, social, technological sustainability for citizen wellbeing”. (2, 4, 8, 12, 37)

As regards the global level, ECSO estimated that approximately 50 billion devices will be connected to the Internet, by 2020, including an increase of 23.97 trillion USD for the Internet of Everything (IoE) market. This represents a real motivation leading to new strategies development, which are necessary to implement (IoT) architectures, and which are not limited to the smart city concept, but also include areas such as human health, agriculture, environment, transport, research & development and education, in which applications of modern biotechnology are successfully replacing devices, chemicals, fuels and energy, foods,

therapeutics etc. From this perspective, special attention should be given to cloud computing (storing big data on cloud platforms) and to the potential of artificial intelligence and special algorithms assessing and analyzing big data. In fact, biological sciences interact with information and computer sciences, being convergent, and such a phenomenon provides opportunities for new emerging fields of multidisciplinary study, like cyberbiosecurity.

Limitation of the study: Although the scientific information regarding the emergent discipline of cyberbiosecurity, especially related to its potential risks (i.e. for people, environment, economy, national security etc.) is not abundant, the present study had briefly reviewed a number of 30 specific articles only to give an overview about the meaning of cybersecurity and biotechnology interactions; also, it is worth noting that scientific papers related to the biosecurity and biosafety field, have not been assessed, due to the huge amount of available data, and mostly due to their impact on both of the strategic/governmental area (including measures and implementation actions at national level) and the technical applications in the multidisciplinary fields involved.

2. Methodology

The methodology utilized in this paper has involved a review method (similar with the scoping review), in which knowledge related to the cyberbiosecurity has been synthesized with the view of a preliminary assessment of a planned theoretical study aiming to encompass larger information about international biosecurity strategies.

3. Cyberbiosecurity

As previously mentioned, biotechnology touches a wide range of economic sectors and generates large percentages of GDP from different industries. One of the major challenges of the 21st century is to develop new bio-based products (including therapeutics and medical devices) or to enhance the quality of the existing ones, in order to obtain novel materials with new properties, and to optimize sustainable technologies for a competitive growing bioeconomy. As regards modern biotechnology, emerging technologies and products (food and feed, pharmaceuticals, chemicals etc.), based on genetic engineering and molecular biology, find applications on the global market, and some of them are completely revolutionary as they prove multiple benefits for the environment and the human wellbeing. In a nutshell, biotechnology is classified on the basis of a “Rainbow code” (since 2012), in which each color is characteristic for a specific area of study/interest, such as: agriculture and environment are represented by green, industrial biotechnology and environmental engineering by white, human health and medicine by red, nutrition and insect biotechnology by yellow, aquatic resources by blue, bioinformatics by gold, arid lands by brown, ethics and law by violet, and bioterrorism and biological weapons by dark/black. Genetically modified (micro)organisms, transgenic organisms, biopolymers, cosmetics, biofuels,

additives, pigments, pharmaceuticals (antioxidants, antimicrobials, antitumorals) represent some of the most important biotechnological applications. (35)

3.1. The need for cyberbiosecurity

3.1.1. Context

Important definitions:

Article 2 of the Convention on the Biological Diversity (CBD) provides a general definition of "Biotechnology", namely that it is "any technological application that uses biological systems, living organisms, or derivatives thereof, to make or modify products or processes for specific use". (15)

European Commission defines "Bioeconomy" as a bio-based sector, relying on "biological resources (animals, plants, micro-organisms and derived biomass, including organic waste), their functions and principles" and excluding "health biotechnology and biological medicines". (16)

"Biosecurity", according to Food and Agriculture Organization of the United Nations (FAO), means "a strategic and integrated approach to analyse and manage risks in food safety, animal and plant life and health, and biosafety". (17)

Nowadays, the society faces new challenges, generated by the beggining of a digital era, but also of the 4th industrial revolution. (24) The bioeconomy is a fast-growing sector (27), (in the US it is considered to be the main driver of national GDP, accounting over USD 4 trillion, approx. 25% of US GDP, in 2015) (11, 30), and research and innovation are recognized as priorities for funding and investments, due to their development potential and for their societal benefits. (22) Modern biotechnology has generated multiple industrial advantages, with concrete benefits, but at the same time, (bio)innovation coupled with the implementation of advanced information technologies has identified some new exploitable gaps, and also new risks (although many hypothetical). (7) There is an interest to include elements of economic analysis in the impact assessment undertaken for strategies promoting bioeconomy development and protection, but also to highlight the need for innovative cybersecurity solutions and robust measures to ensure the security of biological infrastructures and biodata. (23) The absence or insufficient control over biological information and materials may involve serious problems, for the economic and national security, but also for human health or the environment. New biosecurity risks have emerged along with the scientific and technological progress due to the convergence of life sciences with computer information sciences, leading to the need for development of a legislative framework to address biological cyber threats. (23, 25)

The field of biotechnology has substantially changed in the last 10-20 years and as regards the emerging new cyber-physical characteristics, only a limited expertise to identify, classify and assess these rising issues is available. The interactions between modern biotechnology and advanced IT technologies (artificial intelligence, automation, robotics) have led to successful applications, especially in fields such as health (i.e. precision personalized medicine, biomegatronics, smart biosensors), biopharmaceuticals (e.g. development of new drugs, gene therapies),

agriculture (i.e. precision agriculture) and, last but not the least, to a revolution in the field of genomics, through the discovery of genome editing technology (CRISPR/Cas9). (5, 26) Thus, a new paradigm has emerged, as a hybridized, interdisciplinary field, known as the cyberbiosecurity, which describes an intersection of disciplines that can not be found in another sector. (25)

3.1.2 Issues and needs

Digitalization, the rapidly growing bioeconomy, and the dependence on biotechnology, as well as the scientific progress of synthetic biology, coupled with dual-use research has led to a new vision and strategic planning on the need to respond to emerging new threats (such as cyberbiological), to develop and to implement measures for the protection, prevention and mitigation of these risks or other potential issues related to ethics, national security, resilience, etc. (36) In other words, digitalization of biological information entails a number of vulnerabilities, threats and risks. Cyber attacks could generate significant impacts on the national bioeconomies, like orienting production towards malicious purposes (i.e. low quality products, loss of technological process integrity, changes in manufacturing infrastructures), threats to patients health (i.e. inefficient medicines, loss of bioproduction, hazardous lots of therapeutic drugs unauthorized access to biomedical data, stealing of trade secrets, loss of intellectual property and of commercial advantage, algorithms or software that may influence the R&D processes, ransomware attacks, data coding, malware coding in DNA etc. (23, 24, 29) Computational biology generates additional security issues and risks that emerge at the border between biotechnology and cyberspace. (29, 34)

At the present date, policies that manage the risks posed by the biological sciences, in which potential threats are traditionally addressed, are divided into two categories, namely biosafety and biosecurity; some examples of biological threats are: exposure to pathogens or toxins or their release into the environment (through accidental or unintentional actions), and their deliberate spread, endangering human, animal and plant health, food supply, etc. (acts of bioterrorism). Existing policies manage a limited number of threats, and the emergence of new risks due to the multidisciplinary nature and the convergence of biological sciences with IT, triggers the need for a cyberbiological legislation, but only after conducting specific research in the field of biological materials and their associated data protection. (10, 29, 39) Specifically, it could be identified needs, such as: an enhanced awareness regarding new threats as a consequence of rapid technological advancement and numerous innovations in life sciences and IT, as well as due to their potential impact on the bioeconomy, society and even national security; a specific regulatory framework development and dedicated measures implementation; a new culture of cyberbiosecurity responsibility, for which is necessary a sustained effort of cybersecurity experts and from those of the life sciences; building a common language that promotes cyberbiosecurity, as an emerging discipline that requires extra attention from governments, academia and R&D, and particularly from industry; identifing vulnerabilities and creating an effective risk management to protect data security, human health and environment, while providing an enabling framework and adequate funding for cyberbiological innovations.

3.2. Synthetic biology

According to the Royal Academy of Engineering, the synthetic biology "aims to design and engineer biologically based parts, novel devices and systems as well as redesigning existing, natural biological systems". (33)

3.2.1. A short history

Nucleobases (nitrogenous bases: purines, adenine - A and guanine – G, and pyrimidines, cytosine - C, thymine - T and uracil – U), as a base for life on Earth, and which are found in the composition of nucleic acids (DNA and RNA), are arranged in an "alphabet" code through which genetic information is transmitted. During the evolution of the species, they have not changed, but in recent years, with scientific advances, researchers have developed some new pairs of bases; and this could lead in the future to a potential new genetic "alphabet". These artificial pair bases have demonstrated the ability to replicate and function alongside natural nucleobases. Alexander Rich designed a third pair of artificial bases as early as 1962, and pioneering studies related to the study of this newly identified pair started in the late 1980s. (14)

Genetic engineering has its origins in the 1970s, when recombinant DNA technology was discovered, allowing the development of new functions in host organisms. In recent years, the biological sciences, along with bioinformatics have rapidly evolved and made possible genome sequencing and de novo synthesis. Moreover, technologies have become more accessible and cheaper. First genetic circuits were created in the 2000s, and a revolutionary method was discovered in the area of genomics in 2013, namely CRISPR-Cas (Clustered Regularly Interspaced Short Palindrome Repeats Cas system) and for which scientists behind it were awarded with the Nobel Prize in Chemistry in 2020. The first genome – of the poliovirus, was synthesized in 2002; a prokaryotic genome, specific to the Mycoplasma genitalium JCVI-1.0 strain, was synthesized in 2008; the first artificial cell – Synthia, was created in 2010. All of these discoveries have been triggered more ambitious objectives among scientists, and this led to the Human Genome Project-Write (HGP) launching in 2016, with the major goal to synthesize a complete human genome by 2026, with an estimated funding of USD 100 million. (40)

The field of synthetic biology involves multidisciplinary research, combining biology with chemistry, mathematics, computer science, physics and engineering, and its available funding (public and private) demonstrates the enormous potential for future development and applications.

3.2.2 Applications

Bioinformatics has generated exploitable new targets for cyber attacks, along with synthetic biology evolution (which includes the use of synthetic metabolic engineering techniques to design and develop new genetic circuits). One of the sectors in which synthetic biology and transgenic technologies have a large applicability is that of agricultural and food system R&D. Genetically modified organisms have been included in international and national regulatory policies, but nowadays there is a global trend to promote an industrial transition to obtain food

from genetically modified crops, of course using precautionary approaches; however, the need for an update of the existing legislation through some new policies dedicated to monitor products resulting from the application of synthetic biology technologies, as well as setting ethical standards and principles, is a serious reality. Changes in traditional industries, which occurred as a result of the modern biotechnology uses, have led to emerging bioeconomies, but also to solutions for many associated issues related to human health and environment. Transgenic technologies, through which an exogenous genetic material (and more recently, artificial genes) is introduced into the genome of an organism, and which causes approximately predictable changes, or genetic editing, in which the genome is edited accurately but with possible off-target mutations, are increasingly assimilated in agricultural research. In 2018, 191.7 million ha of genetically modified crops were reported worldwide (obtained through the application of transgenic technology), while in 44 countries and regions, products thus obtained were imported (e.g. corn, soybeans, rapeseed, beets, cotton), as processing raw materials. The largest producing countries were: USA, Brazil, Argentina, India, Canada, all of them occupying 91% of the total GMO cultivation area worldwide, but also China, recognized mainly for the production of genetically modified cotton and papaya. By means of synthetic biology, metabolic pathways of plants are modified to improve resistance to diseases or other stressors, or to increase the efficiency of photosynthesis, and CRISPR/Cas9 technology has been widely utilized to improve stress tolerance and increase yields, in crops of rice, wheat, sorghum, rape, potatoes, soybeans, corn, mushrooms, apples, bananas, citrus fruits, and grapes. Moreover, the European Union has decided to regulate "artificial meat" in 2018, as a new food product (it can be obtained by using yeast cells, which have also the ability to synthesize fatty acids from milk or other proteins). All of these technologies could lead to undesirable effects that pose health and environmental risks. For example, exogenous genes inserted into microorganisms could lead to changes in the intestinal flora; gene transfer (e.g. resistant to pesticides, antibiotics) can occur in natural environment, and this could lead to risks for biodiversity and changes in the balance of species populations in certain ecosystems, affecting soil microbiota, invertebrates or insects, and implicitly it could contribute to changes in the soil ecology or it could lead to the development of new pathogens and to pest resistance. There are also some risks involving food safety, due to unintentional mutations following gene editing (e.g. one edited gene may affect the expression of another one), which could determine changes in the populations structure of species, and even to migration of edited genes to other species. Therefore, a strict regulation and effective measures established for the food management (obtained by genetic modification, and from modern biotechnology uses), as well as clearly definitions of risks associated with synthetic biology, represent an international necessity (USA, EU, New Zealand, France, UK, Australia already have strict control regulations). (13)

Production of (bio)pharmaceuticals and therapeutics, such as artemisinic acid in yeast (anti-malarial drug), and the most cited example of application, attenuated pathogenic agents for synthetic vaccines, antitumoral invasin (obtained by developing a synthetic circuit using a Yersinia pseudotuberculosis strain),

bacteriophages designed to produce specific enzymes to lyse biofilms, or utilization of synthetic genes (i.e specific to viruses) to rapidly diagnose diseases like Ebola or Zika (as biosensors on paper), or even the development of sustainable chemicals (biomaterials, biofuels) are amongst the most known applications of synthetic biology. (33, 40)

Some authors consider synthetic biology as of critical importance, due to its industrial potential applications, especially in the field of energy, health, agriculture and environment, and predict it „to produce a new era of wealth generation". They compare its potential economic impact with that of synthetic chemistry, from a century ago, which led to the pharmaceutical development, and assuming even more benefits for economy and society. Among both, the existing and envisaged applications (including those planned to be developed in the next 10-25 years), some are mentioned as follows: in the health and pharmaceuticals sectors – biosensors to detect different anomalies (e.g. arterial disease), urinary tract infections – UTIs (through fluorescent signals when entering in contact with pathogenic agents, including MRSA – methicillin-resistant Staphylococcus aureus) and with targeted drug delivery or to enhance human immune system, some of them associated with biologically based logic gates (i.e. AND, OR, NAND); biologically based memory; artificial monosaccharides; biodegradable nanoparticles; development of new medicines or enhancing the therapeutic properties of the existing ones (including adaptable antibiotics), with reduced side effects; tissue engineering, coupled with 3D bioprinting; in energy field – development of efficient biofuels (especially for aviation); agriculture – gene delivering technologies to produce seeds with enhanced and multiple genetic traits and to maximize the crops' production yields; environment – biosensors for bioremediation, to detect heavy metals and toxins, coupled with genetically modified bacteria, which are able to degrade or to neutralize them, or other chemical compounds (e.g. arsenium); lowering the CO2 emissions, through artificial photosintesis (artificial leaves); development of new ecological pesticides; artificial enzymes for detergent industry etc. (33)

3.2.3 Legal and ethical aspects

A definition related to a biosafety risks classification system, as promoted during a Conference of the Biological and Toxin Weapons Convention (BWC) stated that it is "the inherent capability of microorganisms to cause disease, of greater or lesser severity, in humans, animals and plants", and American Biological Safety Association mentioned the "containment principles, facility design, practices and procedures" as important biosafety issues "to prevent occupational infections in the biomedical environment or release of the organisms to the environment". (40)

In a review paper, the authors identified 44 risks associated with synthetic biology, and related to human health and the environmental protection; the most common were allergies, carcinogens, antibiotic resistance, toxicity, different changes in the environment, horizontal transfer of genes, competition with native species, and pathogenicity. Also, European Union has funded research studies on biosafety risks in relation to the deliberate release of genetic engineered organisms into the

environment, especially those used for plant growth or bioremediation. The conclusion was that these organisms had an environmental impact, but it was approximately similar to that of native microorganisms; however there is a possibility to temporarily gain a competitive advantage over native populations, but their survival depends on the ecological conditions of ecosystems. Horizontal gene transfer is a more serious risk which could cause changes in the genetic structure of the ecosystems, and especially considering that this phenomenon has a growing rate in synthetic/modified organisms than in natural microorganisms (i.e the bacterial cell has a transformation rate of 107). However, a new emerging branch of synthetic biology, xenobiology, involves the synthesis of xenonucleic acids using xenonucleotides (e.g. the non-natural base pair dNaM-d5SICS - utilized in DNA belonging to a strain of Escherichia coli), or proteins using non-canonical amino acids (e.g. L-4,40-biophenylalanine), as components that do not exist in nature, could provide synthetic organisms without any risk of horizontal gene transfer. The development of strains that have genes with increased antibiotic resistance is another potential risk that should be considered. (40)

In accordance with an accepted definition, biosecurity means “security against the inadvertent, inappropriate, or intentional malicious or malevolent use of potentially dangerous biological agents or biotechnology, including the development, production, stockpiling, or use of biological weapons, as well as outbreaks of newly emergent and epidemic disease”, with the major risks mainly in the bioterrorism activities. (40)

The dual use of synthetic biology could generate biosecurity risks, taking into account that information about genome synthesis exist publicly (i.e. horsepox virus, a close relative of variola virus was synthesized using mail-ordered DNA fragments, in 2017); in addition to the extraordinary benefits of genome editing technology, CRISPR/Cas9 (i.e. its applications in human organ transplantation, development of cancer/viruses resistant cells, treatment of genetic diseases), it can also be utilized to increase pathogenicity, virulence or to produce toxins. (40)

After the creation of Synthia, international discussions approached the ethics of this subject; moreover, the former president of the USA, Barack Obama, requested a report to clearly identify the ethical limits of synthetic biology. To date, no biosecurity incidents related to synthetic biology have been reported, but risks must be considered to prevent future crises. Awareness is very important among scientific communities, which is why codes of conduct are recommended, and in some countries they are already implemented (e.g. Australia - "Code for the Responsible Conduct of Research", Japan - "Code of Conduct for scientists”, China – “Self-discipline of the moral behavior of scientific and technical workers”) or are proposed (China and Pakistan - “Model code of conduct for biological scientists”). The dual use of synthetic biological research could have economic consequences and threaten national and/or international security. In this regard, the landscape of potential threats related to defense field tends to widen, including cyber attacks targeting biotech applications (threats that can endanger a national bioeconomy, and exposing it even to possible unforeseen events, such as Black Swan). (20, 40)

In 2012, synthetic biology techniques were considered by an European scientific group of representatives from France, the Netherlands and Germany to still fall within the scope of Directive 2009/41/EC on the contained use of genetically modified microorganisms (GMMs) and Directive 2001/18/EC on the deliberate release into the environment of genetically modified organisms (GMOs). However, the European Union considered that organisms and/or products resulting from the xenobiology applications should be subject to a new regulatory system, due to the fact that artificial organisms may lead to different and new vulnerabilities. (40) Under Directive 2001/18/EC, GMOs are defined as "organisms, with the exception of human beings, in which the genetic material has been altered in a way that does not occur naturally by mating and/or natural recombination, while organism means "any biological entity capable of replication or of transferring genetic material'. Under Directive 2009/41/EC, GMM is defined as a "microorganism in which the genetic material has been altered in a way that does not occur naturally by mating and/or natural recombination", while microorganism means "any microbiological entity, cellular or non-cellular, capable of replication or of transferring genetic material, including viruses, viroids, and animal and plant cells in culture". (1)

Currently, considering that about 30 nations have introduced elements in their legislations that directly or indirectly envisage the clinical uses of germline editing, scientists worldwide are calling for a temporary international moratorium on heritable genome editing (especially in embryons), but excluding it from research uses, until the new technolgies are better understood regarding the risks, ethics and social implications, and in addition, they propose extensive studies, including on human population genetics. (19)

Along with the cyberbiosecurity implications of synthetic biology, many ethical and societal issues could arise with its innovative developments. In addition to a regulation framework, these issues must be carefully addressed by scientists, ethicists, philosophers and, as well, a public dialogue must be built, both to promote the benefits for society which synthetic biology generates, but also to answer to some questions about its major objective, namely the DNA synthesis and the creation of new life forms. According to a public statement recently appeared, DNA will no longer evolve in nature, but in laboratories and clinics ("not in nature but in the laboratory and clinic"). In the US there is a concern about biosecurity risks that can be generated by synthetic biology (especially, creation of harmful organisms and their deliberate or accidental release), which are also associated with social risks. However, experts in the field of biotechnology sustain that there are no imminent problems, as survival of synthetic organisms in nature would be rather difficult than in artificial environments, and in addition, genetic mechanisms/functions could be designed to make them dependent of artificial nutrients, etc. (33)

Therefore, ethical concerns were raised publically in 2010 (when the artificial cell Synthia was created), which led to a global debate and to the formulation of five ethical principles, namely: "public beneficience; responsible administration; intellectual freedom and responsibility; democratic deliberation; and justice and fairness". Nevertheless, a code of conduct is required for scientists in the field of synthetic biology, especially for those who conduct research with double use

potential, as an important tool for responsibility, awareness, prevention and/or defense in relation to ethical and/or biosecurity. (40)

3.3 Cyberbiosecurity – a new discipline

The concept of cyberbiosecurity emerged in the US, following a study conducted in 2014 and coordinated by the FBI, the American Association for the Advancement of Science and the United Nations Interregional Crime and Justice, but also following the project led by the US National Strategic Research Institute and several workshops organized by the US National Academies of Sciences, Engineering and Medicine (NASEM). (36) Therefore it was acknowledged an emergence of a new field, addressing potential and real malicious threats with a significant impact on the bioeconomy, human health and environment, with risks of exploitation and misuse of data, materials and processes, which are generated at the interface between life sciences and digital space. (32) The new discipline started to be promoted, having its main aim to understand and manage its unique risks, associated with the interactions of life sciences and IT field, in particular those generated by the digitization and /or automation of biology and biotechnology, and which triggered a new way of thinking, due to its new vulnerabilities (e.g. a virtual environment allows access to biological materials and physical infrastructure), and which are created by digitalizing biological data and big data and cloud management, by the use of bioinformatics tools, or control systems of industrial bioproduction processes, which are connected to network and automated etc. (26, 34)

Cyberbiosecurity was introduced initially in the meaning of "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". (27)

As regards the convergence of cybersecurity with biosecurity and modern biotechnology, some general elements of strategies, policies and standards which apply to the virtual space activities (e.g. network security, minimizing threats, diplomacy and international cooperation, incidents response, stability infrastructure etc.) interfere with strategic approaches to human, animal and plant life or environment risks, extending the traditional biosafety landscape, which is more focused on genetically modified organisms, and includes new biological threats which target new biotechnologies and infectious agents (dangerous pathogens), which can cause damage, while an increased attention to the scientific developments of synthetic biology, genomics, proteomics, bioinformatics (in terms of de novo synthesis of organisms, namely the manipulation of digital genetic sequences for the purpose of and biological weapons, or designing new functions in existing organisms, including the improvement of virulence, pathogenicity) is given. The FBI has expressed concerns about the use of genomic and medical data, which may be vulnerable to cyber attacks. (29, 34, 36)

Some approaches focusing on cybersecurity relation with biological sciences, exist at international level; for example, some are relevant in agriculture and food systems and they were initiated in the UK, some contribute to train professionals in this field and were initiated in the US, through NICE (Cybersecurity Workforce Framework), or some are concentrating on the applications in precision medicine, using genetics and artificial intelligence, at China initiative. Moreover, in literature it is mentioned the competitive planning of the USA against China, but also a trade agreement between these two, to improve agriculture in North America. (22)

Reed et al. (2019) propose a distinction between cyberbiosecurity and cyberbiosafety, implicitly a new terminology, cyberbiorisk management, and which refers to "identification, elimination and/or control of cyberbiosecurity vulnerabilities in the life science enterprise". Cyberbiosafety vulnerabilities include some of the followings: network-connected biological infrastructure systems (an unauthorized change may present risks of environmental contamination or could endanger human, animal or plant health) or the manipulation of digital genetic sequences (exposure to hazardous pathogens, environmental contamination). (30)

Examples of risks and/or vulnerabilities associated with cyberbiosecurity:

Nowadays we discuss about modern biotechnology (and possibilities to design living organisms with new or enhanced functions, modifying the DNA or even synthesizing new organisms), but also about laboratories of the future - LotF (led by virtual assistants, with automated techniques, artificial intelligence, complex neural networks, virtual reality, cloud computing and blockchain). Even so, with all these new scientific advancements, it is necessary to remember some important names that brought a significant contribution to the early developments of biotechnology: the agronomist Karl Ereky, considered the father of biotechnology, Edward Jenner, the English doctor who helped to the recognition of the vaccination importance (due to smallpox vaccine testing experiments), Alexander Fleming, the Scottish bacteriologist who discovered penicillin, Louis Pasteur, the French microbiologist who is linked to the discovery of brewer's yeast fermentation and many others. (7, 18, 30) We are the witnesses of a rapid growing evolution of biotechnological research, which has enormously evolved since then, and some common examples are: insulin production by recombinant DNA technique, human genome sequencing, genetic editing through the tool of synthetic biology, CRISPR/Cas9 (with benefits in the treatment of genetic diseases, HIV/AIDS, anti-cancer treatments), genomic synthesis (nowadays, it can be performed in just a few weeks, comparative with some years ago, when the poliovirus genome was synthesized in 3 years) etc. (18). With all these scientific developments and an increasing venture capital investments in biotechnology and artificial intelligence R&D (e.g. in 2016, the synthetic biology industry received USD 1 billion, and the AI, USD 5 billion), new issues arise, those of double uses of research and, the risk of cyber attacks (i.e. in the medical and pharmaceutical field), and given that digital dependence of research laboratories in which biological (-omics) data is managed, is increasing. (5, 7, 21) Typically, biological risks have been managed by implementing standard biosecurity practices, identifying vulnerabilities and then mitigating the risks through policies, standards, trainings, and physical security. For example, dangerous pathogens and toxins have

been regulated by their inclusion in the Biological Select Agents and Toxins (BSAT) list, and by the Biological Weapons Convention (BWC), which has the major objective to ban the development, production and storage of weapons derived from biological agents. The US and Russia are supposed to have smallpox strains in their BSL-4 laboratories, but given that a lot of genomes/genetic sequences are available online, and due to advances in genetic engineering (CRISP /Cas9 technology), new risks arise, mainly related to viral or bacterial genome editing (e.g. avian influenza virus - H7N9, with a mortality rate more than 40%, and which presently requires only 3 mutations to become more contagious and to rapidly spread to humans) or to new pathogens synthesis, which are not classified and regulated as potential threats. (7, 34)

Malicious actions on data flows (e.g. in biopharmaceutical production processes), unauthorized access to sensitive information (e.g. private biomedical data, technological information), data theft (intellectual property information, trade secrets, patients' private data, data belonging to forensic laboratories) and payments requests (ransomware attacks) are some of the most well-known risks in cyberspace. With the evolution of genomics, new plausible scenarios have emerged regarding cyber threats, including the insertion of a malicious code written into DNA (a malware encoded into a genetic molecule), which is intended to affect bioinformatics tools. (27) The production of genetic data has doubled every 7 months since 2010, and their digital availability increased exponentially, and this has led to an awareness of a potential threat of cyber attacks in various sectors of the life sciences. (3, 9) Genetic sequences manipulation is typically performed using CAD software, while cyber vulnerabilities are introduced into a genetic code using GenoCad (in a combination of PHP and JavaScript, and using an Apache server, usually). Common tools used for online genomic data screening and to download data sets, are the Galaxy application, and the PostgreSQL database. (27, 28)

With the evolutions of new genetic techniques, actions such as file encryption with the intention of payments receiving (ransomware attacks), industrial hacking, corporate espionage, commercial sabotage, are joining the other new challenges that expand the landscape of cyber risks, such as dual use of research and designing new potentially dangerous infectious agents. (10, 26) In 2014-2015, FBI reported a 53% increase involving industrial espionage incidents in the US, and a 10% increase for cybersecurity incidents involving the medical field, from the beginning of 2010. In 2017, 18% of cyber incidents targeted hospital IT systems (especially those of the private healthcare systems) and they were classified as ransomware attacks for critical data retrieval. (38) In 2014, a hacking attack, known as Anthem Blue Cross, affected 4.5 million patient records. (21) In the UK, another ransomware attack, known as WannaCry, targeted the same sector. In 2017, the chemical and pharmaceutical Merck company's network, suffered from the cyberattack known as NotPeya (the most expensive in history, with a global damage estimated at over USD 10 billion), which targeted the production control system and affected both, the company's international business operations (lost sales of USD 135 millions and other additional costs of USD 175 millions, and a total of USD 1 billion in one year) and the production of the Garadasil vaccine (IUU), Human Papillomavirus Vaccine.

Another malware has targeted the biopharmaceutical field, and which is believed to be used also for sabotage, known as Dragonfly. After these events, the pharmaceutical industry could be considered as an attractive target for cyberattacks. To support the medical system, cybersecurity experts and scientists were invited to a joint online dialogue, through the Biohacking Village initiative (https://www.villageb.io/). Also, in 2019, the US Department of Health and Human Services (HHS) announced the opening of the Health Sector Cybersecurity Coordination Center (HC3). (11, 25, 31)

Therefore, cyber vulnerabilities associated with networked biological data systems and, consequently, the associated infrastructure and equipments, R&D laboratories become subject to malicious exploitation, with cybersecurity risks and potential impact on both, bioeconomy and health. (25) Scientific progress and new genomic approaches in the life sciences also lead to new vulnerabilities and security risks in the management of genetic data. This information is particularly relevant not only for R&D and industry, but also for the public health, food and agriculture, and environment. However, even if cybersecurity focuses mainly on ensuring the confidentiality, availability and integrity of digital data, there are no systemic studies to include the emergence of biological cyber threats, especially in terms of security breaches involving genetic databases. To date, as far as is known, no cyberattacks have been reported on these databases, probably because the motivation for biohacking is weaker than that for attacks which target personal data, and in addition, the number of users of genomic data is much smaller. (31) However, with the expansion of the genomic databases, which have become an integral part of biological and biomedical research, and with an increased funding for the field of experimental genomics, as well as the free accessibility of digital genetic information to anonymous users, a new concern arises for cybersecurity, in particular for the identification and monitoring of genetic sequencing operations involving pathogens that may present risks of malicious use, and which requires dedicated research and systematic studies on the protection of biological data against cyber attacks. (38)

In 2018, 1737 databases with information on molecular biology were reported, and publicly accessible, of which 30 were dedicated to genomic information for viruses, 71 for prokaryotes and 35 for fungi, with applicability mostly in pathogens research. The most well-known genomic databases are hosted by NCBI (National Center for Biotechnology Information) and EMBL (European Molecular Biology Laboratory). NCBI stores 180914 bacterial associated genetic data, 4055 fungal specific data and 23816 viral specific data (e.g. genes, genomes, nucleotides, proteins), and also hosts many other smaller genetic databases, such as SRA (with “raw” genetic sequences resulting mainly from projects research), RefSeq (for genetic annotations), GEO (genomic data on gene expression regulation), BLAST (nucleotide sequences, proteins). EMBL, similar to the GenBank database (which contained approximately 20% of bacterial genomic sequences in August 2017), holds mainly genetic data corresponding to pathogens from several databases, such as EnsemblGenomes, EnsemblBacteria (with 44048 bacterial genomes), EnsemblFungi (811 fungal genomes), Array Express (transcriptomic data, RNA-seq, DNA-seq, CHIP-seq). Biomart is commonly used as an interface for accessing EMBL

data, but alternatively REST, MySQL, APL PERL, API R can also be used, the molecular sequences being stored in FASTA or FASTQ formats, and some are binary data (those recorded in SRA). Other genomic databases are: JGI (hosted by the Joint Genome Institute), which stores integrated comparative data (for genomics and metagenomics research), MycoCosm (fungal associated genomic data), GOLD (genomic metadata resulting from research projects), PATRIC (it holds 202602 bacterial genomes and other several thousand for different species of Archaea and bacteriophages), EuPathDB (genomes associated with eukaryotic pathogens, but also of non-pathogenic related species or host organisms), ViPR (viral specific genomic data required in phylogenetic and comparative analyzes, or for genomic annotations), PHIbase (for the study of host-pathogen interactions), PAMDB and PhytoPath (genomic data associated with phytopathogens), GenomeTrakr (FDA-managed network for monitoring food pathogens; it holds associated data for more than 2000 microorganisms with potential risks, but also common clinical pathogens). (38)

4. Conclusions

In this paper, the author has aimed to highlight the new concept of cyberbiosecurity and to synthesize some of the main aspects related to the life sciences and cyber space convergence, which have led to a new emergent multidisciplinary field. Cyber and biological contributions to bioeconomy, health, and environment reshape the security landscape. We are witnessing times of new industrial trends due to the present biorevolution, which is based not only on biotechnological scientific progress, but also on network connections, digital DNA and enhanced competitiveness. Business interest moved forward to modern biotechnology field. Smart laboratories include networked systems and devices, international interconnections, and artificial intelligence. All of the above generate opportunities, but also vulnerabilities and risks. Experts in cybersecurity issues recognize the biological implications, and they are starting to work with biotechnologists or other scientific experts, in order to promote a common language, definitions and knowledge, to better understand the new field, to identify security gaps, to foster awareness about cyberbiological threats and to develop strategies and countermeasures. Furthermore, a call for action is launched among policy makers, academia, industry and various stakeholders to design principles, standards and policies, to mitigate the cyber attacks and other related biosecurity issues (e.g. dual use research, combinational weapons), having in mind to strengthen the safeguarding capacities to protect human, animal and plant health, and business interests. (10, 24)

Acknowledgements

The author acknowledges National Institute for Chemical-Pharmaceutical Research & Development, INCDCF-ICCF, Bucharest, Romania for general support; there is no conflict of interest to declare.

References

[1] Akpoviri, F., Zainol, Z.A., Baharum, S.N. (2020), Synthetic biology and biosafety governance in the European Union and The United States, IIUMLJ, vol. 28, no. 1, pp. 37-71;

[2] Al-Azzam, M.K., Alazzam, M.B. (2019), Smart City and Smart-Health Framework, Challenges and Opportunities, International Journal of Advanced Computer Science and Applications, vol.10, no. 2, pp. 171-176;

[3] Bajema, N.E., DiEuliis, D., Lutes, C., Lim, Y.B. (2018), The Digitization of Biology: Understanding the New Risks and Implications for Governance, https://wmdcenter.ndu.edu/Publications/Publication-View/Article/1569559/the-digitization-of-biology-understanding-the-new-risks-and-implications-for-go/;

[4] Bause, M., Khayamian, E.B., Forbes, H., Schaefer, D. (2019), Design for health 4.0: exploration of a new area, International Conference on Engineering Design, ICED 19;

[5] Berger, K.M., Schneck, P.A. (2019) National and Transnational Security Implications of Asymmetric Access to and Use of Biological Data, Front. Bioeng. Biotechnol., vol. 7, no. 21, doi: 10.3389/fbioe.2019.00021;

[6] Caswell, J., Gans, J.D., Generous, N., Hudson, C.M., Merkley, E., Johnson, C., Oehmen, C., Omberg, K., Purvine, E., Taylor, K., Ting, C.L., Wolinsky, M., Xie, G. (2019), Defending Our Public Biological Databases as a Global Critical Infrastructure, Front. Bioeng. Biotechnol., vol. 7, no. 58, doi: 10.3389/ fbioe.2019.00058;

[7] Dunlap, G., Pauwels, E. (2017), The Intelligent and Connected Bio-Labs of the Future: Promise and Peril in the Fourth Industrial Revolution, https://www.wilsoncenter.org/sites/default/files/media/documents/misc/the_intelligent_connected_biolabs_of_the_future.pdf;

[8] European Cyber Security Organisation – ECSO, (2018), Smart cities and smart buildings sector report - Cyber security for the smart cities sector, http://www.ecs-org.eu/documents/uploads/smart-cities-sector-report-032018.pdf;

[9] Farbiash, D., Puzis, R. (2020), Cyberbiosecurity: DNA Injection Attack in Synthetic Biology, ArXiv abs/2011.14224;

[10] George, A.M. (2019), The National Security Implications of Cyberbiosecurity, Front. Bioeng. Biotechnol., vol. 7, no. 51, doi: 10.3389/fbioe.2019.00051;

[11] Guttieres, D., Stewart, S., Wolfrum, J., Springs, S.L. (2019), Cyberbiosecurity in Advanced Manufacturing Models, Front. Bioeng. Biotechnol., vol. 7, no. 210, doi: 10.3389/fbioe.2019.00210;

[12] Hallett, S.H. (2017), Smart cities need smart farms. Environmental Scientist, vol. 26, no. 1, pp. 10-17, ISSN 09668411, https://www.the-ies.org/resources/feeding-nine-billion;

[13] He, R., Cao, Q., Chen, J., Tian, J. (2020), Perspectives on the management of synthetic biological and gene edited foods, Biosafety and Health, vol. 2, pp. 193–198, http://dx.doi.org/10.1016/j.bsheal.2020.07.003;

[14] Hirao, I., Kimoto, M., Yamashige R. (2012), Natural versus Artificial Creation of Base Pairs in DNA: Origin of Nucleobases from the Perspectives of Unnatural Base Pair Studies, Accounts of Chemical Research, vol. 45, no. 12, pp. 2055-2065, DOI: 10.1021/ar200257x;
[15] https://www.cbd.int/abs/;
[16] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0673;
[17] http://www.fao.org/;
[18] https://futureoflife.org/background/benefits-risks-biotechnology/;
[19] https://media.nature.com/original/magazine-assets/d41586-019-00726-5/d41586-019-00726-5.pdf;
[20] https://portal.nifa.usda.gov/web/crisprojectpages/1019771-fact-regional-multisector-cyberbiosecurity-workshop-to-safeguard-the-agriculture-and-food-bioeconomycommunity-building-training-strategy.html;
[21] Kozminski, K.G. (2015), Biosecurity in the age of Big Data: a conversation with the FBI, Molecular Biology of the Cell, vol. 26, no. 5, pp. 3894-3897, DOI:10.1091/mbc.E14-01-0027;
[22] Mack, R., Miller, R. (2020), Cyberbiosecurity–A Compilation of Summaries of Peer-Reviewed Publications, Government Publications, and Relevant Resources, https://www.cpe.vt.edu/cyberbiosecurity/Cyberbiosecurity_article_summaries.pdf;
[23] Mantle, J.L., Rammohan, J., Romantseva, E.F., Welch, J.T., Kauffman, L.R., McCarthy, J., Schiel, J., Baker, J.C., Strychalski, E.A., Rogers, K.C., Lee, K.H. (2019), Cyberbiosecurity for Biopharmaceutical Products, Front. Bioeng. Biotechnol., vol. 7, no. 116, doi: 10.3389/fbioe.2019.00116;
[24] Millett, K., dos Santos, E., Millett, P.D. (2019), Cyber-Biosecurity Risk Perceptions in the Biotech Sector, Front. Bioeng. Biotechnol., vol. 7, no. 136, doi: 10.3389/fbioe.2019.00136;
[25] Mueller, S. (2019), On DNA Signatures, Their Dual-Use Potential for GMO Counterfeiting, and a Cyber-Based Security Solution, Front. Bioeng. Biotechnol., vol. 7, no. 189, doi: 10.3389/fbioe.2019.00189;
[26] Mueller, S. (2021), Facing the 2020 pandemic: What does cyberbiosecurity want us to know to safeguard the future, Biosafety and Health, vol. 3, pp. 11–21, http://dx.doi.org/10.1016/j.bsheal.2020.09.007;
[27] Murch, R.S., So, W.K., Buchholz, W.G., Raman, S., Peccoud, J. (2018), Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy, Front. Bioeng. Biotechnol., vol. 6, no. 39, doi: 10.3389/fbioe.2018.00039;
[28] Nawrocki, S.R. (2019), Cyber Threats to the Bioengineering Supply Chain, SANS Institute, Information Security Reading Room, https://www.sans.org/reading-room/whitepapers/threats/cyber-threats-bioengineering-supply-chain-38805;
[29] Peccoud, J., Gallegos, J.E., Murch, R., Buchholz, W.G., Raman, S. (2018), Cyberbiosecurity: From Naive Trust to Risk Awareness, Trends in biotechnology, vol. 36, no. 1, DOI: 10.1016/j.tibtech.2017.10.012;

[30] Reed, J.C., Dunaway, N. (2019), Cyberbiosecurity Implications for the Laboratory of the Future, Front. Bioeng. Biotechnol., vol. 7, no. 182, doi: 10.3389/fbioe.2019.00182;
[31] Richardson, L.C., Connell, N.D., Lewis, S.M., Pauwels, E., Murch, R.S. (2019) Cyberbiosecurity: A Call for Cooperation in a New Threat Landscape, Front. Bioeng. Biotechnol., vol. 7, no. 99, doi: 10.3389/fbioe.2019.00099;
[32] Richardson, L.C., Lewis, S.M., Burnette, R.N. (2019), Building Capacity for Cyberbiosecurity Training, Front. Bioeng. Biotechnol., vol. 7, no. 112, doi: 10.3389/fbioe.2019.00112;
[33] Royal Academy of Engineering, (2009), Synthetic Biology: scope, applications and implications,ISBN: 1-903496-44-6,www.raeng.org.uk;
[34] Schabacker, D.S., Levy, L.A., Evans, N.J., Fowler, J.M., Dickey, E.A. (2019), Assessing Cyberbiosecurity Vulnerabilities and Infrastructure Resilience, Front. Bioeng. Biotechnol., vol. 7, no. 61, doi: 10.3389/fbioe.2019.00061;
[35] Tomulescu, C., Moscovici, M., Stoica R.M., Vamanu, A. (2021), A Review: Klebsiella pneumoniae, Klebisella oxytoca and Biotechnology, Rom Biotechnol Lett., vol. 26, no. 3, pp. 2567-2586, DOI: 10.25083/rbl/26.3/2567.2586;
[36] Turner, G. (2019), The Growing Need for Cyberbiosecurity. Proceedings of the Informing Science and Information Technology Education Conference, Jerusalem, Israel, pp. 207-215, https://doi.org/10.28945/4337;
[37] Vargiu, E., Zambonelli, F. (2017), Engineering IoT Systems Trough Agent Abstractions: Smart Healthcare as a Case Study, https://doi.org/10.1007/978-3-319-70887-4_2;
[38] Vinatzer, B.A., Heath, L.S., Almohri, H.M.J., Stulberg, M.J., Lowe, C., Li, S. (2019), Cyberbiosecurity Challenges of Pathogen Genome Databases, Front. Bioeng. Biotechnol., vol. 7, no. 106, doi: 10.3389/fbioe.2019.00106;
[39] Vinatzer, B.A., Heath, L.S., Almohri, H.M.J., Stulberg, M.J., Lowe, C., Li, S. (2019), Cyberbiosecurity Challenges of Pathogen Genome Databases, Front. Bioeng. Biotechnol., vol. 7, no. 106, doi: 10.3389/fbioe.2019.00106;
[40] Wang, F., Zhang, W. (2019), Synthetic biology: Recent progress, biosafety and biosecurity concerns, and possible solutions, Journal of Biosafety and Biosecurity, vol. 1, pp. 22–30, https://doi.org/10.1016/j.jobb.2018.12.003.