PLOVDIV UNIVERSITY
"PAISII HILENDARSKI"

ФИСН
ФАКУЛТЕТ ПО ИКОНОМИЧЕСКИ И СОЦИАЛНИ НАУКИ

kamegpa ПННС

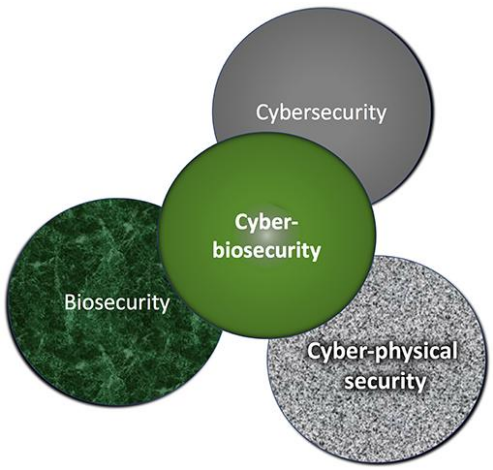
Kostadin Rangelov Bakov

CYBERBIOSECURITY AS AN ELEMENT OF THE NATIONAL SECURITY SYSTEM

ABSTRACT

for obtaining the degree of Doctor of Philosophy

Field of higher education: 9. Security and Defense,
Professional direction: 9.1 National Security,
Doctoral Programme National Security



PhD Supervisors: Prof. Dr. Ilia Iliev, Assoc. Prof. Dr. Ivan Stanchev

Plovdiv, 2025

The dissertation was discussed at a meeting of the "Department of Political Science and National Security" at the Faculty of Economic and Social Sciences of "Paisii Hilendarski" University of Plovdiv, held on 27.06.2025, at which it was decided to direct it for public defense.

The dissertation is 221 pages long and contains an introduction, six chapters, conclusion and references.

A total number of 69 tables and 63 figures are included. The bibliography includes 35 sources in Cyrillic and 160 in Latin.

On the subject of the dissertation three author publications are presented in English.

Materials related to the forthcoming public defense are available in the "Academic Staff Development and Doctoral Studies" of the "Paisii Hilendarski" University of Plovdiv, as follows as well as in the Central University Library.

The public defense of the dissertation is scheduled for 19.09.2025 at 11.00 a.m. at the Paisii Hilendarski University, Plovdiv, 24 Tsar Asen Street, "Compass" Hall, at meeting of the Scientific Jury composed of:

Prof. Dr. Sc. Nikolay Marinov Nikolov – Paisii Hilendarski University of Plovdiv

Assoc. Prof. Dr. Nina Dimitrova Dimcheva – Paisii Hilendarski University of Plovdiv

Prof. Dr. Sc. Ilin Alexandrov Savov – Trakia University, Stara Zagora

Prof. Dr. Georgi Vasilev Kamarashev – University of Veliko Tarnovo, Veliko Tarnovo

Assoc. Prof. Dr. Sc. Petar Gospodinov Marinov – "G. S. Rakovski" Military Academy, Sofia

Author: Kostadin Rangelov Bakov

Title: Cyberbiosecurity as an element of the national security system

TABLE OF CONTENTS

ABBREVIATIONS USED

GMO – Genetically Modified Organisms

DNA – deoxyribonucleic acid

EEA – European Economic Area

EC – European Commission

EU – European Union

GMO – Living Modified Organisms

ICT – Information and Communication Technologies

IT – Information Technology

CBD – Convention on Biological Diversity

BWC – Biological and Toxin Weapons Convention

CWC – Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction

CT – Quantum dot

ICPD – International Plant Protection Convention

NS – National Security

OPCW – Organisation for the Prohibition of Chemical Weapons

UN – United Nations

RCT – Randomised Controlled Trial

RNA – ribonucleic acids

USA – United States of America

SSCRS – Strategic Security Resources Assessment and Control System

USSR – Union of Soviet Socialist Republics

SPS – World Trade Organisation Agreement on the Application of Sanitary and Phytosanitary Measures

WTO – World Trade Organization

FBI – Federal Bureau of Investigation

HIV – acquired immune response syndrome

CDC – Circulating Cancer Cells

AAAS – American Association for the Advancement of Science

AI – Artificial Intelligence

AHL – acyl-homoserine lactones

ASSURED – affordable, sensitive, specific, user-friendly, robust and rapid, equipment-free, deliverable

BCG – BCG vaccine

INTRODUCTION

Cyberbiosecurity is an emerging field at the intersection of cybersecurity and biosecurity. The goal of cyberbiosecurity has been described as addressing "the potential or actual malicious destruction, misuse, or exploitation of valuable information, processes, and materials at the interface of the life sciences and digital worlds". Cyberbiosecurity is part of a system of measures that collectively aim to safeguard the bioeconomy.

A number of publications over the past decade have highlighted the complexity of the enterprise we call "cyberbiosecurity" and the concerns about its security, stability, and resilience. These include the security of personal genomic data, as foreign companies that have acquired all or part of U.S. companies or contracted for genomic or health data services provide access to sensitive personal information; the continued vulnerability of electronic health records and healthcare systems to DNA sequencing controls through DNA-encoded malware; the vulnerability of the synthetic biology supply chain; the cyber compromise of large biopharmaceutical industries; and high-level studies that systematically examine U.S. biodefense programs and capabilities.

The most vivid demonstration of the introduction of a system of rules for cyberbiosecurity is the Coronavirus-19 pandemic. The relevance of the topic of biosecurity and cyberbiosecurity is driven on the one hand by the evolution of terrorism and interstate conflict showing a trend towards increased terrorist attacks using biological weapons, and on the other by the significant scientific advances in the last 30 years of molecular biology and molecular biotechnology that have led to the possibility of almost unhindered use of molecular biology techniques and methods in routine laboratories. Additionally, there are still unresolved issues relating to the risks of infectious diseases being deliberately transmitted across borders in the face of migration pressures and the implementation of the doctrine of free movement of people and goods around the world.

The authorities responsible for national security must be prepared to respond adequately to the dynamic changes in the international situation.

One of the main areas of focusing academic efforts should be the task of developing strategies, principles, rules, algorithms and methodologies that will lay the foundations for a concept of cyberbiosecurity on the territory of Bulgaria as a member of the EU.

At the moment, there is no doctrine, concept and programmes for cyberbiosecurity at national level. On the proposed topic of the dissertation, there are no known scientific publications and developments by other Bulgarian authors dealing in detail with the aspects of cyberbiosecurity in the context of sharing sensitive databases.

On the basis of the above circumstances, we can formulate the research problem that this thesis addresses: the NS system lacks an element responsible for biosecurity and cyberbiosecurity. Also, there is no structure functionally responsible for the protection of biosecurity and cyberbiosecurity, as well as no concept for its provision.

The object of study is *cyberbiosecurity as an element of the national security system.*

The subject of study is the *legal and technical aspects of cyberbiosecurity as a combination of knowledge and skills in three different areas – national security, information technology and molecular biotechnology, which need to be coordinated with the security and operational and investigative aspects.*

***The aim** of this dissertation is to **create a concept for cyberbiosecurity protection in the Republic of Bulgaria**.*

*In order to achieve the stated goal, the following **research tasks** are identified to be completed in the process of research:*

1. To analyze the current state of cyberbiosecurity and its place in the national security system.

2. To study biological weapons and carry out their classification through the prism of scientific achievements in the field of molecular biotechnology.

3. Identify the dangers and threats and determine the level of risk in cyberbioattacks.

4. To systematize the obtained results and propose a model of a cyberbiosecurity concept.

5. Determine guidelines for the development and improvement of counter-cyberbioattack activities.

6. To analyze the effectiveness of applying rapid methods for disease diagnosis as a risk factor for biosecurity.

Research hypothesis:

Based on the established absence of a concept, doctrine and programs for cyberbiosecurity in Bulgaria, as well as considering the increasing interconnectedness of information systems with biomedical and biotechnology data, the hypothesis is formulated that the development and implementation of an integrated model for cyberbiosecurity, covering legal, technical and organizational aspects, will significantly increase the resilience of the national security of the Republic of Bulgaria against cyberbioattacks and will minimize the risks arising from the sharing of sensitive databases in the context of membership in the European Union (EU). This model should include a strategy for countering biological weapons, systematization of threats and risks, as well as guidelines for the development and improvement of activities for the prevention and response to cyberbioattacks.

Theoretical and methodological basis of the study

The theoretical and methodological basis of the research are the conceptual foundations of the *systems approach; management theory, conflict theory; theory and practice of biosensor creation, theoretical foundations of molecular biotechnology.*

National, institutional and educational normative documents, encyclopedic and reference literature, educational and methodological materials have been used in the dissertation research.

Research methodology

In the course of the research for the solution of the research tasks a complex of:

- **Theoretical methods**: analysis and synthesis of the general characteristics of cybersecurity, requiring an interdisciplinary approach of the planned research.

- **Empirical methods**: environmental monitoring to detect the risks in the protection and transfer of sensitive biological data, survey of different population groups to consider the individual and societal risk in the transfer and storage of sensitive biological databases, expert assessment of the feasibility of biosensors and techniques for rapid diagnosis of potential agents of biological threat to the population.

- **Statistical methods**: various methods for processing, summarising and analysing sensitive biological databases have been used to process, summarise and analyse the results.

For greater focus, specificity and depth of development, the following **limitations** have been assumed in the research process:

1. A detailed survey of sources that investigate specific biosensor and diagnostic test patterns to detect potential biological threats.

2. The activities of other countermeasure actors as part of the national security system are not the subject of this study.

3. The time scope of the study is 2022-2025.

4. The spatial (territorial) scope includes the territory of the Republic of Bulgaria in terms of surveys and international environment when comparing and analyzing data conducted in an international environment.

5 Regulatory base is up-to-date as of 01.01.2025.

Research methodology:

During the **first (preparatory) stage of the study** (2020-2022), the research problem is analyzed in terms of the technical and technological level in the two main areas – information technology and molecular biotechnology (biosensors). The key characteristics of the two dynamically developing fields of science and technology in an interdisciplinary area are revealed. The subject and object, aims and objectives of the study are defined, and the working hypothesis is formulated.

In the **second (main) stage** (2023-2024), the conceptual foundations of a platform for building a cyberbiosecurity system are developed. Simultaneously, adjustments are made to the research methodology, precise strategies are formulated for the scientific investigation of new biosensors, and the application of a suite of existing instrumentation and biosensors to conduct biomonitoring.

In the **third (final) stage** (2025), the results are summarized and the main conclusions and recommendations presented in the dissertation are formulated.

The credibility and validity of the dissertation results are ensured by the logic of the research and by the applied conceptual and theoretical-methodological basis.

Significance of the results

The scientific novelty *of the research consists in revealing the interrelations between biosecurity, cyberbiosecurity and the international security environment, constructing a model of cyberbiosecurity as an element of the national security system.*

The theoretical significance of the research lies in the solution of the scientific task – *formulation of a concept of cyberbiosecurity.*

The practical significance of the research lies in proposing a system of devices and biosensors that can be used to conduct rapid analysis of the agents of a potential bioterrorist attack.

CHAPTER ONE: NATIONAL SECURITY AND ITS RESOURCING

1.1. General overview

Chapter One discusses the nature of national security with an emphasis on the factors that influence its level. It examines the importance of information resources and the state of ecosystems in protecting national security. In the modern world with the development of the technological revolution, artificial intelligence and molecular biotechnology, it is necessary to examine the concept of national security through the prism of problem solving with an interdisciplinary approach.

National security (NS) is the priority of every country, regardless of its polity, political system and economic status. For its provision it is necessary to allocate the necessary resources – human, financial, technical, legal. One of the key issues in maximising the effectiveness of NS activities is to strike a balance between the capabilities of the state and the assessment of the level of protection required.

Achieving a balance between the necessity and availability of strategic resources in the state is a basic prerequisite for its national security situation. Finding this balance in practice is mainly done through each country's budget. This prerequisite in itself includes the subjective factor, which can be broadly defined by the interaction of economic processes and the political governance of the country. Each country's budget is a function of trade-offs between the level of the country's economy and the level of political maturity of the society.

The state is still the most important factor in providing NS. This circumstance also gives rise to the fact that the redelegation of its authority over the resourcing and operations of critical infrastructure is untenable and generates unwarranted risks in terms of the present moment.

1.2. Information as a strategic resource and its control

In the era of the global world that is currently being transformed information is a key factor for the security of both states and the individual.

According to the definition of prof. Stoyan Denchev (2019), "Information, in all the variety in which it manifests itself, is a valuable resource, just like financial, material and human resources. Generally speaking, the concept of information resources can be expressed as follows: all available resources of a system and their transformation into usable information. Other authors, detailing the above definition, give the following definition: "Information resources are all the physical and logical components of an information processing system, such as computers, programs, data, information, operating systems, communication links, systems and programmers, program analysts, operators and managers".

In the context of the dynamic development of the world in general and the development of technology in particular, the definition of information resources must also be seen through the lens of AI. According to Hristo Chaushev (2024), AI is emerging as a significant transformative force in social media, improving the creation of personalised content and increasing user engagement.

1.3. Resources in the context of the global environmental crisis and complex risk

Natural resources underpin the functioning of the economy and their availability and the ways in which they are used determine the quality of human life. Raw materials such as fuels, minerals and metals, but also food, soil, water, air, biomass and ecosystems are limited. The great danger posed by the exploitation of natural resources is linked to factors such as economic development, population growth and urbanisation, and the increasing exploitation of ecosystem resources.

Ecosystem services are an interdisciplinary field of science between ecology and economics. Ecosystems are life-support systems that are providers of ecosystem services and economic benefits.

The main conclusion that emerges is that there is an almost complete overlap between the parts of the planetary ecosystem possessing a high risk of ecological catastrophe and the modern regions with the largest populations in the world.

All planetary resources are finite, commensurate with the existence of the planet and the solar system itself. The resources themselves don't matter if our civilization disappears for a variety of reasons – there simply won't be anyone to consume the resources, to convert the material and energetic nature of the planetary environment into suitable ones for survival and development. Contemporary realities in human society's attitude to natural resource potential show a rigid, heavy-handed and unjustified traditionalism.

1.4. Key Problems in the Functioning of the Strategic Security Resource Assessment and Control System (SSRACS)

The Strategic Security Resources Assessment and Control System surveys the nation's human, economic, financial, technological, and information resources and includes the following basic assessment principles:

- Balance between the needs of the security system and the capabilities of the country;
- Efficiency and effectiveness;
- Satisfaction of required operational capabilities.

The most effective use of financial resources is through the implementation of a long-term concept and strategy, not simply through funding in each individual project. Financing the modernization of countries' industrial and technological bases has the greatest impact on the security of societies. There is a need for certainty about the overall impact of decisions on the implementation of projects to develop and deploy high-tech solutions in promising industries. There is also a need for effective technology risk management. High-tech solutions can have both positive and negative

impacts on the development of individual countries and the world as a whole. While professing the principle of competitiveness, societies today are developing technologically ahead of their time and at a much slower pace socially, despite the proclaimed principle of humanity. The anticipatory development of modern technologies in the digital society implies their use both for the positive development of society and for imposing the will of a part of the peoples' society over the rest to the detriment and subjugation of the latter. Recent technological advances in the two fastest growing fields, information technology and molecular biotechnology, offer for the first time in human history the possibility of being used uncontrollably by different groups of people, even by individuals. This fact puts the security of society as a whole in an entirely new situation. Therefore, we cannot afford to consider the prerequisites for the emergence of a security risk for society, for individual states and for alliances of states fragmented by sectors and industries. Today, it is increasingly imperative to apply an integrated approach to building the system for assessing and controlling strategic security resources, with cybersecurity, biosecurity and cyberbiosecurity at the centre of this system, as unifying the entire activity of individual societies through the introduction of high-tech processes into use. They are at the intersection of the problems of scarcity of raw materials and energy, on the one hand, and environmental catastrophes, particularly in certain regions.

Conclusions from chapter one:

The world today is changing at high speed. The development of the process of globalisation has opposed the development of the nation state especially in the emerging confrontation of the world hegemons. The recent events after the Covid-19 pandemic and the conflict between Russia and Ukraine on the one hand, and technological progress in all fields of science on the other, digitalization as a process and the advent of AI have clearly shown that individuals and communities seek and expect security, in all its dimensions, most now within the nation state. The situation is similar for migration processes, climate change and environmental crises. A new doctrine of national security needs to be put in place, including cybersecurity and biosecurity in the new international relations.

CHAPTER TWO: CURRENT LEGAL ISSUES IN THE REGULATION OF BIOTHREAT ASSESSMENT AND PROTECTION PROCESSES

2.1. Legal acts concerning protection against biological threats

In contemporary terms, biological threats can be illustrated as a spectrum that includes intentional disease outbreaks, emerging infectious diseases on the one hand, and natural disease outbreaks on the other.

General criteria have been defined for different biological agents, including pathogens, to classify them according to their degree of hazard, and these are grouped into three categories, as outlined below.

Category A includes high-priority agents, such as organisms that pose a national security risk to countries because they can spread or transmit easily from person to person; result in high mortality rates and have the potential for major public health impact; can cause public panic and social disruption; and require special public health preparedness actions.

Such agents/diseases include Anthrax (*Bacillus anthracis*); Botulism (*Clostridium botulinum* toxin); Plague (Yersinia pestis); Smallpox (*Variola vera*); Tularemia (*Francisella tularensis*); Viral hemorrhagic fevers including Filoviruses (Ebola, Marburg) and Arenaviruses (Lassa, Machupo).

Category B includes agents that are moderately easy to spread; result in moderate levels of morbidity and low levels of mortality; and require specific improvements in diagnostic capacity of laboratories and enhanced disease surveillance.

Category B includes the following agents/diseases: Brucellosis (*Brucella* species); Epsilon toxin from *Clostridium perfringens*; Food safety threats (salmonellosis), Melioidosis (*Burkholderia pseudomallei*); Psittacosis (*Chlamydia psittaci*); Q fever (*Coxiella burnetii*); Ricin toxin from *Ricinus communis* (castor bean); Staphylococcal enterotoxin B; Typhoid fever (*Rickettsia prowazekii*); Viral encephalitis (alphaviruses such as Eastern equine encephalitis, Venezuelan equine encephalitis and Western equine encephalitis; Water safety threats (*Vibrio cholerae, Cryptosporidium parvum*).

Category C includes emerging pathogens that could be designed for mass spread in the future because of their availability; ease of production and spread; and potential for high morbidity and

mortality and major health impact. Category C includes emerging infectious diseases such as Nipah virus and hantavirus.

New infectious agents are continually being discovered in nature for which no treatment and prophylaxis have yet been developed.

Special attention should also be paid to genetically modified organisms (micro-organisms, plants and animals), also known as "chimeric organisms", artificially created through various genetic manipulations. Scientific advances have even made it possible to synthetically construct genetic material (genome) to be incorporated into host micro-organisms, and to achieve the recovery of extinct pathogens such as the smallpox virus that causes smallpox by using molecular biological methods to synthesize DNA. On the other hand, advances in molecular biology can also be used to create entirely new pathogens that have never existed in nature, whose pathogenic properties are not known to medical science and have no real experience of causing epidemics. They are also called superpathogens, in which characteristics of two or more pathogens are combined.

2.2. Current biological research and its implications for human biosecurity

In the current context, rapid scientific and technological progress is being made in a number of fields, which has implications for the blurring of technological barriers to the acquisition and use of biological weapons. Technologies with the potential to mitigate global catastrophic biological risks, e.g. genomic sensing, extracellular diagnostics, synthetic vaccinology, are evolving. While these technologies should not be seen as panaceas, they can be a critical part of the response to severe pandemics and global catastrophic biological risks.

At the same time, there are known examples of research undertaken with potential dual-use applications. The potential dual-use nature of certain technologies does not serve as a pretext for restricting scientific exchange and technology transfer, especially for developing countries. An important aspect of the issue is capacity building, including on the training of scientists and laboratory personnel in biosafety, biosecurity and laboratory diagnostics programmes.

Of particular relevance to modern bioresearch is the practice of other legal instruments and international organizations. For example, the experience of the implementation of the mandate of the Scientific Advisory Board of the Organisation for the Prohibition of Chemical Weapons (OPCW) and the WHO Meeting of Experts on the Science and Technology Foresight Process, including risk management of molecular biology research in general and its application in high-tech industries.

Conclusions of Chapter 2: The review of the legal framework shows the need to update and synchronise the legislation of the Republic of Bulgaria through the prism of cybersecurity and biosecurity.

CHAPTER THREE: BIOSECURITY AND THE PUBLIC HEALTH ETHICS POSED BY BIOLOGICAL THREATS

3.1. General overview

The use of biological agents as weapons of war or terror has its roots in antiquity, beginning with the use of pathogens to kill horses, which were vital resources in the age of direct combat. There are also concerns about bioterrorism these days, such as the widespread discovery of letters sent containing *Bacillus anthracis* through the United States Postal Service in the fall of 2001. As a result of this bio-attack, five of the twenty-two people who were infected died. The so-called Ameritrax attacks were crucial in raising the national security system's attention to the threat of bioterrorism.

Events preceding the anthrax attacks also helped shape thinking and actions toward bioterrorism. For example, in 1984 a series of salad bars in Dallas, Oregon of the US were infected with salmonella by followers of the Bhagwan Shree Rajneesh movement (later known as Osho). These occultists aimed to rig county elections by making potential voters contagiously ill so that they could not appear at the polls on election day. In the mid-1990s, the poison gas sarin attacks on the Tokyo subway by the Aum Shinrikyo cult killed twelve people and injured hundreds. Attackers have also attempted a series of biological attacks over the years, primarily in subway stations, although none of these earlier efforts were successful.

Concerns about the orchestration of bioterrorist attacks are heightened by the expansion of life sciences research that can be used with "dual-use" capabilities. Here, useful research has the potential to be misused by malicious actors with a variety of nefarious agendas, including those with expertise in biological weapons. Unlike overt biological weapons research, which is conducted by a variety of organizations (e.g., in the past, Soviet bioweapons programs operated undetected for decades to produce biological weapons for some countries in the former Union of Soviet Socialist Republics (USSR), dual-use research is typical especially for countries with few financial resources that cannot develop a nuclear weapons program). The aforementioned research with biological objects is also intended for noble purposes, such as the treatment of genetic diseases and hard-to-treat illnesses.

It is a real possibility that biotechnology, as the industry of the future in the 21st century, could be used to produce biological weapons and as an alternative to solve significant problems of mankind, from finding cures for incurable diseases to active components for disease prevention, including pandemics, to obtaining new materials to replace petroleum-based products. It all depends on the objectives of the research programmes, on the one hand, and on the scientific potential of the laboratories concerned. In this context, we could describe **biosecurity as policies and actions designed to prevent the development or emergence of serious biological threats or mitigate their consequences – deliberate biological weapons, pandemics, emerging infectious diseases or the result of accidents caused by the activities of large laboratory complexes.**

This chapter analyzes the information gathered through the lens of the potential applications of biotechnology for bioterrorism purposes and focuses on nation-state responses to deliberate biological threats. The principles and challenges associated with examining potential biotechnology threats for bioterrorism purposes have significant overlap with the broader set of biological threats.

Chapter Three Conclusions:

Events such as the anthrax attacks in 2001 and preceding incidents such as the salmonella outbreak in the US, and the Tokyo poison gas attacks, highlight that bioterrorism is a growing threat, accompanied by increased concerns about the consequences of biological attacks.

Biosecurity policies, dual-use research and the development of biotechnology pose new challenges to national security and public health. The classification of biological threats is based on principles of freedom, security, justice, and utility that have imposed new ethical norms in response to the situation. There is a need to balance the protection of public health with the individual rights of citizens, especially in the context of biological attacks and pandemics.

The potential for misuse of biotechnology has necessitated the introduction of new rules and policies to ensure the safety of the public, the prevention of biological threats and the promotion of ethical practices in research. Stakeholders must work together to cover gaps in legislation and prevent possible attacks based on biological agents, while preserving the priorities of security, freedom and justice.

In the context of preventing, preparing for, and responding to biological threats, the ethical issues that arise before, during, and after a crisis are critical to securing public health and national security. According to Directive (EU) 2017/541, various acts that may lead to serious consequences must be classified as terrorist offences. Ethical dilemmas highlight the need to balance scientific freedom and public safety.

Pre-crisis preparations include assessing the risks associated with research on dual-use items that could lead to potentially devastating pandemics. Conducting such research presents scientists with dilemmas about safety and public health benefits. Organisations should seek to fund research that minimises the risk of biological threats.

In the event of a bioterrorist attack, the allocation of scarce resources also creates conflicts between principles of equity and efficiency. There is a need to establish clear priorities in resource allocation that take into account both saving lives and maintaining the social fabric of society. Issues

of procedural fairness and public participation in decision-making on these issues are equally important but also complex.

Public engagement in the formulation of preparedness strategies can build trust, but at the same time risks giving away information that could be used by deliberate adversaries. The public must be actively involved in the creation of biological threat prevention and response plans, taking into account both the ethical and practical aspects of these processes.

In the face of a biological threat, ethical norms become key to organizing adequate safety and public health measures. In times of crisis, it is important that responses to bioterrorism attacks are based on principles of fairness, transparency and rapid communication. Developed countries have a moral obligation to help weaker nations, while obligations to contain the spread of epidemics also play a role in global safety.

Communication in epidemics must be transparent to maintain public trust, and coercive public health measures must be proportionate and the need for them can be justified. Isolation of infected persons is acceptable, while quarantine of potentially exposed persons is rarely justified and may lead to loss of confidence. The development of new therapeutic agents must be carried out with attention to ethical standards, and randomised controlled trials (RCTs) raise particular debates in the context of public trust and participant safety.

Once the crisis is contained, the recovery platform must vote to support affected communities by providing needed resources and infrastructure renovation. The fundamental principles of equity and reciprocity must guide recovery efforts that benefit not only affected communities but also global safety.

Ethical standards in responding to biological threats require balanced governance between public health and security, with a clear legal and regulatory framework to guide decision-making at all stages of preparation, response and recovery.

Ethical issues related to biosecurity and bioterrorism require careful consideration and a balance between scientific freedom, public health, efficiency and fairness to ensure the safety and resilience of society in the face of biological threats.

CHAPTER FOUR: CYBERBIOSECURITY TO PROTECT THE BIOECONOMY

4.1. General overview

The bioeconomy and related biotechnologies offer new technological solutions to many of the health and resource challenges facing the world. Modern biotechnology can increase the supply and environmental sustainability of food, feed and fibre production, improve water quality, provide renewable energy, improve animal and human health and help maintain biodiversity by detecting invasive species.

The definition of the bioeconomy has been subject to numerous academic interpretations and definitions, especially in the last 10 years. Bauer et al. in 2018 proposed the following interpretation of the term “Bioeconomy” in the form of a classification of activities:

1. “Let firms innovate at their own pace”: the Bioeconomy follows business-led innovation, especially in the agribusiness industry, providing growth and sustainability;

2. “Energy is the key issue”;

3. “The Bioeconomy as an Endless Frontier”: Simply replacing resources will not be enough to manage global problems; new knowledge and R&D are required, especially in the chemical industry;

4. “Green Intervention Agenda”: Bioeconomy through public policy interventions (research, targets, demand-driven policies, finance) to transform industrial and economic structures as the market alone cannot cope.

For greater precision in the terminology used, we can cite two definitions of the term “Bioeconomy” given by international forums:

“The bioeconomy includes those parts of the economy that use renewable biological resources from land and sea – such as crops, forests, fish, animals and micro-organisms – to produce food, materials and energy. This is an essential alternative to the dangers and limitations of our current fossil-based economy and could be considered the next wave in our economic development. It offers great opportunities for innovation, jobs and growth and as such will help to re-industrialise Europe.”

The European Commission (EC) gives the following interpretation of the bioeconomy: “In broad economic terms, the bioeconomy refers to the set of economic activities related to the invention, development, production and use of biological products and processes. The application of biotechnology to primary production, health and industry can lead to an emerging ‘bioeconomy’ in which biotechnology contributes a significant share of economic output. The bioeconomy in 2030 is likely to include three elements: advanced knowledge of genes and complex cellular processes, renewable biomass, and the integration of biotechnology applications across sectors”.

4.2. Introduction of the term “cyberbiosecurity”

The term “cyberbiosecurity” includes information and research from the two scientific fields of cybersecurity and biosecurity and can be defined as a hybrid scientific field with broad applications. Initially, some authors defined the term as “the understanding of vulnerabilities to unwanted surveillance, intrusion, and malicious and harmful activities that may occur in or at the interfaces of biological and medical sciences, cyber-, cyber-physical, and infrastructure systems and supply chains, and the development and implementation of measures to prevent, protect against, mitigate, investigate, and identify such threats that relate to security, competitiveness, and resilience.” They stress that this is an initial definition that is still to be developed.

Simply put, from its inception, biosecurity has focused primarily on reducing the risks associated with the misuse of various branches of biological science that can cause harm to humans, animals, plants, and the environment through the creation, production, and intentional or accidental release of infectious disease agents or their byproducts (e.g., toxins). Cybersecurity is a separate field that focuses primarily on the security of information technology-based systems, from personal computers and communication devices to large infrastructures and networks. Only until the last few years has the overlap between ‘cyber’ and ‘biosecurity’ not been realised. After analysing the data on the development of the two fields separately, we can conclude that the two fields need to work together and will not be effective in the development of modern technology if they work separately. An additional incentive to combine cybersecurity and biosecurity is the deepening interdisciplinary approach in modern science.

Cyberbiosecurity actually started with thinking about a particular set of problems that modern branches of biological science face along with the rest of the natural sciences. The creation of a unifying scientific field, the elaboration of its taxonomy and the identification of a way forward are realized with the extension of an interdisciplinary approach to research and innovation.

Other publications in recent years also highlight the complexity of the endeavour we call “cyberbiosecurity” and concerns about security, stability and sustainability. These include the security of personal genomic data when foreign companies that have purchased all or a portion of U.S. companies or contracted for genomic or health data services and provide access to sensitive personal information; the continued vulnerability of electronic health records and health care systems imposing

controls on DNA sequencing through DNA-encoded malware; the vulnerability of the synthetic biology materials supply chain, the cyber compromise of large industrial biopharmaceutical The Dark Net may also be involved as it interacts with life sciences activities with potential dual use, and has access to biopharmaceutical research, development, intellectual property and products and compromises the integrity of critical life and health science and to cyber supported technologies and infrastructures. Due to the development of bioinformatics as an essential part of modern molecular biotechnology, the security of synthetic DNA can also be included. It is clear that this rapidly expanding interdisciplinary scientific field does need a universally accepted definition, common tasks and defined boundaries for best assessment, focused development and impact.

4.3. Analysis of cyberbiosecurity systems in biotechnology industries

With the development of molecular biotechnology, we can add another dimension to cyberbiosecurity and take an approach that we believe should be included with the aspects of cyberbiosecurity already discussed earlier. The biopharmaceutical industry itself has its own significant shares and investments in the research, development, manufacture and sale of vaccines, therapeutics and prophylactics for the global market. At the same time, experts increasingly recognize that biotechnology production itself is potentially vulnerable to unwanted or illegal activities that could lead to harmful outcomes. These can include intellectual property theft, supply chain disruption, manipulation of bioprocess development and bioproduction, cyberattacks on key IT components and cyber-physical interfaces, corruption of critical data, and manipulation of security systems and infrastructure on which security and safety depend. In providing the results of an analysis of the potential threat of biotechnology industry failure, users (the owners and managers of biotechnology industries) are not satisfied with generalizations or esoteric approximations (not accepted by formal science) in reports on the security vulnerabilities of biotechnology enterprises, but demand a comprehensive, detailed analysis that can be applied in practice to the specific case or specific biotechnology industries.

In implementing a thorough, comprehensive analysis of an existing biotechnology enterprise, it is necessary to identify security gaps and vulnerabilities, make recommendations regarding them, and lay the groundwork for more specific and comprehensive measures to be taken, whether or not they exist or need to be developed and validated. A systems analysis approach has now been developed which is designed to assess the current state of security, determine what would be an acceptable security state and provide guidance and recommendations to bring the enterprise from its current state to the desired state.

What is very important from the cybersecurity problem analysis performed is that a rigorous examination of any biotechnology enterprise can lead to the identification and characterization of individual vulnerabilities, gaps, deficiencies, and opportunities for which affordable solutions can be applied or new ones can be developed, tested, and implemented. Of interest in the future, as a subject of cyberbiosecurity, are detailed studies on how genomics can be compromised as it relates to molecular biotechnology in modern biomanufacturing. The plausible scenarios of cyber attacks and what the effects could be are known.

Our analysis of such information shows that biomanufacturing enterprises can benefit from comprehensive, multidisciplinary analyses to identify security vulnerabilities, leading to solutions to mitigate or address them. This in turn turns necessitates the prospect of developing and validating a set of methods or protocols that could be used by enterprise personnel or external service providers to support individual small biotechnology enterprises to the large biopharmaceutical industry. For example, implementing such an analysis for a probiotics of a small or starter company is comparable to a cybersecurity analysis for a world-leading insulin company.

Guidelines or standards can then be developed, established, and adopted to ensure consistency and quality of the analysis performed, the credentials of the personnel doing it, and the quality and effectiveness of the measures taken. Because biotechnology production requires highly intelligent approaches, the implementation of bio-attacks requires at least the same level of preparation on the part of adversaries who might design and execute sophisticated attacks. However, relatively simple methods and practices are likely to raise the bar significantly to reduce risk. Finally, combining

analyses of this kind can be used as the basis for informed investments in research, development, testing, and assessment to address the most troubling current and future threats.

4.4. Cyberbiosecurity perspectives

Many other sections of informatics as a science appear critical to life and biomedical technology in particular. These additional applications are naturally included within the training to achieve cyberbiosecurity. These include not only, personalized genomics and medical technology, 3-D printing of critical personalized medical devices, and medical laboratory and surgical robotics. A broader system is needed. Cyberbiosecurity could be expanded to include cyber-biosystems in agriculture and farm-to-table food production, processing and delivery systems, as well as in natural resource and environmental management. Direct and organised engagement – biosecurity and cyber-security communities, for relevant life sciences sectors – should take place. Academia, industry, government or non-profit organisations (including experts on policy, regulatory and legal issues) need to start communicating and drawing on each other's expertise, harmoniously identifying and developing priorities and opportunities, and identifying 'next steps'. There is now a great opportunity to propose a common structure and a common language. Finally, while the definition and creation of cyberbiosecurity is taking place, it is necessary to follow national or international strategies to harmonize the emerging discipline and promote its importance, success and sustainability.

4.5. Biosensors and potential application in implementing biosecurity prevention

In ensuring cybersecurity of clinical research with human genetic material, it is necessary to use instrumentation and analysis methods that ensure high speed of analysis and reliability of result under "field conditions". One possible solution is the use of biosensors.

As defined by the International Union of Pure and Applied Chemistry (IUPAC), a biosensor is 'a self-contained integrated device that is capable of providing specific equipment for quantitative or analytical readout of reaction results using a biological recognition element (biochemical receptor) that is in direct spatial contact with a transducer'. In general, biosensors are designed to translate physical, chemical or biological events into measurable signals. In this respect, the design of any biosensor is characterised by several components: 1) biomolecules (enzymes, proteins, nucleic acids, aptamers, antibodies, organelles, microorganisms or cell receptors) responsible for selectivity to the target analyte; 2) a transducer (optical, electrochemical, piezoelectric, mechanical, or thermal) that converts the biosensing event proportional to the concentration of the target analyte into a quantifiable electrical signal, and 3) an electronic system including an amplifier, processor, and display that will further process the signal into a user-friendly visualization.

A successful biosensor must have at least some of the following useful features:

1. The enzyme must exhibit high specificity of enzyme response for the purpose of the assays, be stable under normal storage conditions, and show good stability of results over a large number of assays (i.e., significantly greater than 100).

2. The enzymatic reaction must be able to be run over a wide range of physical parameters such as agitation, pH and temperature, which would ensure the independence and reliability of the assay being performed and would allow samples to be analysed with minimal pre-processing. If the reaction involves cofactors or coenzymes, these should also, if possible, be co-immobilised with the enzyme.

3. The result of the reaction carried out should be accurate, precise, reproducible and linear within the useful analytical range, without dilution or concentration. It must also be free from electrical noise. It must meet the following requirements:

a/ Linearity: The maximum linear region of the sensor calibration curve. The linearity of the sensor shall be high for the detection of high substrate concentrations.

b/ Sensitivity: The value of the sensor response per unit substrate concentration shall cover a wide range and be able to discriminate very minute differences in substrate concentration.

c/ Selectivity: A maximum of low interference from co-existing chemicals is a prerequisite for obtaining the correct result.

d/ Response time: The time required to obtain a result should be as short as possible.

4. If the biosensor is to be used for invasive monitoring in clinical situations, the probe should be small and biocompatible, without toxic or antigenic effects. If it is to be used in bioreactors, it should be sterilizable by autoclaving, but currently the enzymes in biosensors cannot withstand such radical treatment with high temperature and humidity. Under any circumstances, the biosensor should not be susceptible to clogging or proteolysis.

5. The entire biosensor kit should be inexpensive, small, portable, and capable of use by laypersons in the particular field to ensure its mass application.

6. There must be a market for the biosensor. Clearly, developing a biosensor is of little value if other factors (e.g., government subsidies, continued employment of skilled analysts, or poor customer acceptance) encourage the use of traditional assay methods and inhibit the decentralization of laboratory testing.

4.5.1. Application of biosensors by protein detection

The development of sensitive, easy to use and inexpensive biosensors for protein detection is a must as protein detection is of great interest for diagnostic applications in various fields. The main reason is that proteins are the most conserved molecules of living organisms along with nucleic acids and are also readily available for extraction from various diagnostic materials. In fact, many diseases can be related to the higher/lower presence of a protein or to the reporting of their different isomeric forms, as is the case for example with iso-enzymes. Many paper sensors have been developed using different strategies. The main format used in paper nanobiosensors to detect proteins is sandwich analysis based on antibody pairing (immuno-sandwich formation), as discussed below.

For example, lateral fluidic biosensors are paper-based devices that enable low-cost and rapid diagnostics with good robustness, specificity, sensitivity, and low detection limits. The use of nanoparticles as labels plays an important role in the design and fabrication of lateral flow strip. The choice of nanoparticles and the corresponding detection method directly influence the performance of these devices. Various nanomaterials (e.g., gold nanoparticles, carbon nanotubes, quantum dots, phosphor and latex bead conversion technologies, etc.) have been discovered and are being applied in practice in lateral fluidic biosensors. Various detection methods (colorimetric, fluorescence, electrochemical, magnetic, etc.) and signal amplification strategies (providing secondary reactions or modifying the lateral flux band architecture, as well as the use of devices such as smartphones to read the result of lateral flux bands have also been developed. A similar mechanism of improving the function of a lateral biosensor was proposed by Choi et al. (2010), combining two types of gold nanoparticles of different sizes in the same sandwich to detect Troponin I with a detection limit of 10 pg mL^{-1}in serum samples of myocardial infarction patients.

4.5.2 Application of biosensors in nucleic acid detection

The detection of nucleic acids is used for genetic tests, but also for the detection of pathogens producing these molecules extremely important in diagnostics. The samples used are usually pre-amplified using PCR (Polymerase Chain Reaction) or isothermal techniques so that there is a sufficient amount of DNA to be detected, or the samples are synthetic DNA sequences. In addition, the binding of the DNA sequences to the paper usually occurs through the use of a protein pair, such as biotin-avidin or antigen-antibody, which bridges the DNA and the paper.

Even when no nanoparticles are involved in the experiment, it is worth mentioning because the scientists designed a paper strip that is capable of DNA amplification using a rotating circle amplification (RCA) technique, another isothermal alternative to PCR. The scientists have taken advantage of and shown that poly(N-isopropylacrylamide) microgels linked to DNA oligonucleotides are compatible with enzymatic reactions. Briefly, they could detect up to 100 pM of a DNA target that was used as a template for a DNA ligase to bind a capture sequence to a primer sequence. The new

DNA molecule is further amplified by RCA, which generates extremely long ssDNA that can be detected using complementary DNA functionalized with fluorescent dye.

4.5.3. Cell-based devices

Paper devices that integrate cells either as receptors to indirectly detect proteins or other species, or to directly detect them, have also been developed. It should be noted that most of the cells cannot pass intact through the pores of the membranes used, but they can be attached to the surface of the paper.

Li et al. (2017) developed an LFA to detect whole cell antigens of Pseudomonas aeruginosa and Staphylococcus aureus based on the use of gold nanocups functionalized with specific antibodies as labels. The authors obtained detection of a range of bacterial lineages within 500-5000 CFU mL^{-1}; furthermore, in this work they describe the fabrication of a compact portable device that converts the color intensity of gold nanoparticles into a quantitative voltage reading proportional to the bacterial concentration in the sample.

Liu et al (2019) developed a strip-aptamer-gold nanoparticle biosensor to detect circulating cancer cells, reaching a detection limit of 4000 Ramos cells with the naked eye and 800 Ramos cells with a portable strip reader within 15 min. In addition, the cells were also detected in human blood samples.

A strip flow biosensor based on a gold nanoparticle immunosandwich was developed to detect Salmonella typhi in human serum. The LoD reached by the authors was 1.14 105 cfu mL1 within 15 min, which is better than dot blot immunoassay.

Some other interesting biosensors, although not using any nano materials, but due to their interesting innovation are also described. The first work, done by Struss, describes the development of a portable filter-paper based strip biosensor for the detection of signaling molecules sensitive to bacterial quorum sensing, N-acyl-homoserine lactones (AHLs). They reached a LoD of 10 nM AHL and they could also successfully use the device for physiological samples. They briefly dried the genetically modified bacterial cells on a strip of filter paper using beta-galactosidase as a reporter protein. The saliva samples are applied to the tape.

4.5.4. Application of biosensors for infectious disease detection

In the fight against infectious diseases, it is often important to make an accurate and timely diagnosis in order to make an informed decision on the treatment plan. A prompt and accurate diagnosis allows clinicians to prescribe the correct medical treatment and greatly improves the patient's prognosis overall. In particular, when it comes to infectious diseases, timely diagnosis is even more important and can reduce or prevent further infection in the patient population.

Although there are many effective methods to detect pathogenic agents, such as culturing in selective media, microscopy, genomic amplification (e.g. PCR) and immunoassay (e.g. ELISA), each of these approaches has its own drawbacks and is less applicable in resource-limited settings where infectious diseases are more prevalent. Other diagnostic methods such as polymerase chain reaction (PCR) and enzyme-linked immunosorbent assay (ELISA) are more efficient in terms of time and scope, but have several disadvantages. Immunoassays can be successfully used to detect infectious diseases if the correct antibody-antigen interaction is determined, but are difficult to develop and use for the detection of pathogens with high levels of epitope mutation (e.g. in the highly variable bacterial and viral genome). Due to the listed drawbacks, the need for the development of innovative methods for rapid and reliable diagnostics is growing tremendously.

While each biosensor is characterized by several advantages and disadvantages based on the target application, their design typically includes high ligand specificity and selectivity, high throughput capacity, dynamic range, rapid detection, ease of design and operation, cost-effectiveness, and low power requirements.

Chapter Four Conclusions:

Biomarkers associated with the detection of disease states can serve as indicators of human diseases. Clinical diagnosis of diseases can greatly benefit from the timely and accurate detection of biomarkers, which has been the subject of extensive research. For example, because of the specificity of antibody and antigen recognition, electrochemical immunosensors can accurately detect multiple biomarkers of disease, including proteins, antigens, and enzymes. Different types of electrochemical immunosensors have been constructed. The focus of applications of these immunosensors is on the ability to detect cancer, Alzheimer's disease, the new coronavirus pneumonia, and other diseases. Future trends in electrochemical immunosensors are related to achieving lower detection limits, improving electrode modification capabilities, and developing compositions. All biosensors are now also coupled with SMART devices, enabling results to be shared in different directions. Here the need to protect on the one hand the personal health data of each person, on the other hand the protection of the data from misuse in their collection, processing and inclusion in large databases is very clearly demonstrated. The need for the development of specialised protocols in the field of cyberbiosecurity clearly emerges. The demonstration of an interdisciplinary approach in addressing the issue at hand to ensure the protection of this sensitive data requires a concerted effort to work together by national institutions responsible for protecting national security.

CHAPTER FIVE: RESULTS OF EMPIRICAL STUDIES

Two separate studies have been conducted within this dissertation, one related to the aft microbiome, the second divided as two sub-studies related to the preparedness of young professionals and professionals in the fields of cybersecurity, cyberbiosecurity, and countering cyberbioattacks. As a final result, the conducted research confirms the need to develop a **model for the application** of methodologies to synchronize physical security, cybersecurity and biosecurity as an element of national security.

The empirical research conducted is an important part of developing the concept of cyberbiosecurity and its implementation in practice. In the research analyses the following data has been obtained:

1. **Data on** the level of awareness of specialists of disaster and emergency structures and population protection in the field of cybersecurity and biosecurity.

2. **Data on** currently available cyber and bio incident response protocols.

3. **Data on the** level of awareness of institutions relevant to the problem of synchronization of physical and cyberbiosecurity.

4. **Data on** the level of safety through the lens of cyberbiosecurity, obtained by conducting a study on the health status of the human microbiome by analyzing biological material – breast milk and feces of children up to one year of age.

5. **Data on the** level of safety through the lens of cyberbiosecurity, obtained as an indirect result of the analysis of genetic material from breast milk and feces of a child up to one year of age.

6. **Development** of specific requirements for the methodology of interaction of physical and cyberbiosecurity in relation to the dynamics of the relationship between public and private entities with different objects of activity.

At the time of conducting the research related to the young experts and specialists of the structures for countering threats in the field of cybersecurity and biosecurity, it is clear that the field is underdeveloped and with the exception of the dissertation of Dr. Peter Tsvetanov from 2021 on *"Preparedness of hospitals for active treatment for medical provision of victims of radiological terrorism"*, defended at Medical University Sofia, no similar research has been done so far. For the purpose of the survey, two separate questionnaires were constructed, taking into account the specificity of the respondents' profile, and for individual questions we used the model already

developed in Dr Tsvetanov's thesis (see ANNEX 1 **Young Specialists** Survey and ANNEX 2 **Specialists** Survey).

Methodological limitations of the study

This study was conducted using an online survey form created and distributed via the **LimeSurvey** platform between April and May 2024. Despite the advantages of this method – speed of data registration, access to a wider audience and automated processing – there are a number of methodological limitations that should be considered when interpreting the results:

1. **Representativeness issues:** the use of an online survey results in only a selection of participants, allowing mainly people with internet access and digital literacy to participate. This creates a risk of sample skewing relative to the general population. In this particular study, this can be noted through the way the surveys were distributed through so-called gatekeepers in view of the sensitivity of the data recorded and the specificity of the two questionnaires. The survey thus conducted can be thought of not so much in terms of its **representativeness but in terms of its precedence.** In selecting respondents, we were guided not so much by adherence to the principles of forming a representative sample in which participants would have taken part on the basis of random selection, as by the principles underlying the formation of a **convenience sample** designed to focus the research among a particular group with a particular occupational and socio-demographic profile. Part of the shortcomings of the study are also related to the fact that it **is geographically limited to the territory of the city of Sofia. This limits the possibility of generalizing the data and the results obtained.**
2. **Data quality.** In this particular case, this manifested itself in the form of data returns – in the Young Professionals Survey 1, a total of 216 surveys were received, of which 152 were partially completed and 64 were fully completed. For Survey 2 Professionals, the total number of surveys received was 124, of which 72 were partially completed and 52 were fully completed. In the course of the analysis of the surveys, only the fully completed surveys were statistically processed, the results of which will be presented in the presentation.
3. **Limited control over the completion process:** the researcher has no ability to control the environment in which the survey is completed, nor to ensure that the respondent has completed it independently and objectively. In this particular case, we relied heavily on gatekeepers through whose internal channels the surveys were distributed, hence the motivation for completion by the respondents given the internal institutional dynamics between department heads and experts in those departments, both in the national security and health care systems.
4. **Technical limitations:** while LimeSurvey offers various options to control and filter responses, in the absence of registration or one-time links, the possibility of duplicate or false responses cannot be completely ruled out.
5. **Limitations of open-ended questions:** Open-ended questions are often left unfilled or contain too short and uninformative answers, making subsequent qualitative analysis difficult. In this case, in both surveys, the open-ended questions, after the initial data analysis and coding in SPSS ver. 27, required further processing of the open-ended questions and their typing so that they could be graphically summarised and analysed more easily.

Despite these limitations, the online survey via LimeSurvey was preferred in view of its easy accessibility and the possibility to reach a wider range of respondents in a short period of time.

5.1. Results of Survey No. 1 Young Professionals (Survey on the Awareness and Preparation of Young Professionals and Students in the Event of a Cyberattack, Bioterrorism Attack and Cyberbioattack (ID 448767))

Key findings

Based on the data summarized, the following summary conclusions can be drawn:

1. Working with biological toxins: Most respondents have not worked in a field where biological toxins can be obtained. The main biohazards encountered are bacteria and viruses.
2. Knowledge of bioterrorism and cyberbioterrorism: Most respondents know what bioterrorism and cyberbioterrorism are. However, a significant proportion do not feel prepared to give first aid in the event of a bioterrorist attack.
3. Preparation and instructions: A large proportion of respondents do not have instructions on what to do in the event of a bioterrorist attack or cyber-attack at the institutions where they work. Personal protective equipment is also lacking in many institutions.
4. Training and periodicity: Most respondents felt that periodic training on disaster response and bioterrorism attacks is necessary. The preferred period for such training is one year.
5. Cyber attacks: Very few respondents had received training on how to respond to a cyber-attack. Most do not have cyber-attack instructions and cannot operate cyber-attack assessment equipment.
6. Demographics: Most respondents were female, the highest proportion of young professionals under 25 years of age, and most respondents had one year of work experience in their field of expertise, which is consistent with the demographic profile derived.

Based on the survey data, the top risks that stand out can be typified into several categories and sub-categories:

1. Biological toxins:
    - Bacteria and viruses: The most common workplace biohazards.
    - Acids, chemicals and chemical substances: Also pose a significant risk.
2. Lack of preparation and instruction:
    - Inadequate preparation for bioterrorist attacks: Many respondents do not feel prepared to give first aid in a bioterrorist attack.
    - Lack of Instructions and Personal Protective Equipment: Many institutions lack instructions for action and personal protective equipment.
3. Cyber attacks:
    - Inadequate preparation for cyber attacks: Very few respondents had received training on what to do in the event of a cyber attack.
    - Lack of instructions and equipment to assess a cyber attack: Most respondents do not have instructions on what to do in case of a cyber attack and cannot handle equipment to assess a cyber attack.
4. The harms of a cybera ttack:
    - Personal data leakage: the most commonly cited harm in sensitive data compromise.
    - Psychological trauma and financial abuse: also a significant risk.

These risks point to the need to improve training and instructions for dealing with bioterrorism and cyberattacks, as well as to conduct periodic disaster response training. Based on the risks identified, several suggestions can be made for prevention:

To reduce the risks associated with bioterrorism, cyberbioterrorism and biological toxins, we can take the following measures:

1. Improving knowledge and training

- Conduct regular training and workshops for staff on bioterrorism and cyberbioterrorism. This includes theoretical and practical sessions.
- Information material: Dissemination of information material explaining the risks and how to respond to bioterrorism and cyber attacks.

2. Development and implementation of instructions

- Instructions for action: Develop detailed instructions for dealing with bioterrorist attacks and cyber-attacks. These instructions should be available to all employees.
- Simulations and exercises: Conduct simulations and exercises that role-play hypothetical bioterrorism and cyber-attack scenarios. This will help staff prepare for real situations.

3. Provide personal protective equipment

- Personal Protective Equipment: Provide personal protective equipment for all employees who may be exposed to biological toxins. This includes masks, gloves, protective clothing, etc.
- Instructions for use: Training of personnel on how to properly use personal protective equipment.

4. Improving infrastructure and technology

- Biological contamination assessment: Provide instrumentation and methodology to assess biological contamination. Staff training on how to use this equipment.
- Cybersecurity: Implement cybersecurity systems that protect the institution’s sensitive data. Staff training on how to respond to a cyber attack.

5. Periodic checks and updates

- Periodic Checks: Conduct periodic checks on the institution's preparedness to respond to bioterrorism attacks and cyberattacks.
- Instructional Updates: Regularly update operational instructions and training materials to reflect new threats and technologies.

6. Creation of specialized teams

- Dedicated Teams: Establish dedicated teams of trained professionals to respond to bioterrorism and cyber attacks. These teams should be available 24/7.

7. Raising awareness

- Awareness campaigns: Conduct awareness campaigns among employees and the public on the risks of bioterrorism and cyber attacks.

These measures will help to significantly reduce the risks and increase the preparedness of institutions and staff to respond to disaster situations.

5.2. Results of Survey No. 2 Professionals (Cybersecurity, Biosecurity and Cyber Security Awareness and Training Survey (ID 427823))

Key findings

Based on the survey and the data presented, several generalizations can be made:

1. Lack of knowledge and training on bioterrorism and cyberbioterrorism

- Knowledge of health damage: 73.08% of respondents do not know what health damage can be caused when sensitive data is misused.
- First Aid Preparation: 87.50% of respondents do not feel prepared to give first aid in case of a bioterrorism attack or biotoxin incident.

2. Lack of instructions and personal protective equipment in institutions

- Bioterrorism Instructions: 78.85% of the respondents do not have any instructions to act in case of a bioterrorist attack in the institution where they work.
- Personal protective equipment: 71.15% of the respondents do not have personal protective equipment in the institution to protect themselves in case of a bioterrorist attack or accidental incident.

3. Lack of training on cyber attacks

- Training for cyber attacks: 65.38% of the respondents have not received any training for dealing with cyber attacks.
- Instructions for dealing with cyber attacks: 61.54% of the respondents do not have instructions for dealing with cyber attacks in the institution where they work.

4. Harm of cyber attack

- Leakage of personal data: 34.62% of respondents mentioned leakage of personal data as the main harm in case of cyber attack.
- Psychological trauma: 13.46% of respondents cited psychological trauma as the primary harm.
- Financial abuse and loss: 21.15% of respondents cited financial abuse and loss as the primary harm.

These risks underscore the need to improve staff knowledge and training, develop and implement bioterrorism and cyberattack response instructions, provide personal protective equipment, and conduct regular training and workshops. This will help to significantly reduce risks and increase preparedness for disaster response.

The results of the survey of experts also revealed significant gaps in knowledge and preparation for bioterrorism and cyber attacks. Most respondents have not worked in a biohazard environment, and the main incidents they are familiar with include incidents in research laboratories, nuclear accidents, and unauthorized disposal of biological waste. However, a significant proportion of respondents were unaware of the health harms that can be caused by the misuse of sensitive data, with the main harms including psychological trauma and changes in diagnosis and treatment.

Bioterrorism preparation and instructions are inadequate. Most respondents have not received training on what to do in the event of bioterrorism and do not have instructions on what to do in the institutions where they work. Personal protective equipment is also lacking in many institutions. In addition, most respondents believe that providing medical assistance to people who have suffered a bioterrorist attack poses a risk to their health, and many do not feel prepared to provide first aid in such incidents.

Cyber attacks also pose a significant risk, with very few respondents having received training on what to do in the event of a cyber-attack. Most do not have instructions on what to do in the event of a cyber-attack and are unable to operate cyber-attack assessment equipment. The main harms of a cyberattack include personal data leakage, psychological trauma, and financial abuse.

Recommendations to reduce risks

To reduce the risks associated with bioterrorism and cyberattacks, it is necessary to improve staff knowledge and training through regular training and workshops. The development and implementation of detailed instructions for dealing with bioterrorism and cyber-attacks is essential. Providing personal protective equipment to all staff and improving the infrastructure and technology for assessing bio-contamination and cyber security are also important measures. Conducting periodic

reviews and updates of instructions, establishing dedicated teams of trained professionals, and raising awareness among employees and the public will help to significantly reduce risks and increase disaster response preparedness.

5.3. Results from Survey 3: Breast milk microbiome testing as an example of sensitive data analysis with medical relevance

The sharing and use of sensitive data by living people poses significant challenges when considering ethical, legal and societal issues. In the EU, the General Data Protection Regulation (GDPR) aims to protect EU citizens from privacy and data breaches in today's data-driven society by establishing rules for the processing and movement of personal data. However, the GDPR leaves room for national derogations, and this has allowed for some consistency to be maintained in the legal landscape within the European Economic Area (EEA), adversely impacting the practice of clinical and scientific research

Research involving health information faces significant challenges, risks and limitations in terms of patient confidentiality. Studies in recent years have shown that many patients do not feel comfortable when all of their health data is shared, even if key identifiers are removed. One sensitive element of health information relates to newborn data. Breastfeeding newborns in the first months after birth is the environmentally friendly way for them to survive and adjust to the lifestyle. The data that have been obtained from research studies in various aspects on breast milk, breastfeeding and the health status of the child and mother are an important element of the concept of vital prosperity of the human population as a whole. Increasingly, the model of personalized data correlated to the social and ecological gical environment is being applied, which requires very careful collection, processing, storage and use of these personal data. In order to check the level of awareness on the one hand, and the level of potential threat of misuse of the collected personal data on the other, we conducted surveys among breastfeeding mothers as part of a scientific study on the profile of the breast milk microbiome correlated to child health.

In our study, due to time and funding constraints, we surveyed and analyzed data from a laboratory study on one of the key parameters of breast milk, the presence of beneficial microorganisms in the microbiome of the breast milk samples examined. Designing an appropriate survey is a key point in biomedical research. The survey we conducted enabled us to assess the attitudes and feasibility of many participants' participation as breast milk donors for the study we conducted in parallel. As a result of the examination of the breast milk microbiome and the results we obtained, which we related to the information from the prepared survey, gave us the conviction of intellectual property protection in the face of the developed breast milk examination protocol for the detection of a state of dysbiosis. The developed protocol refers to the development of a specific in vitro quantification method for the rapid prediction of dysbiosis in infants up to 1 year of age, whereby the ability to control the human microbiome is achieved, the method, according to the description, taking into account, on the one hand, general indicators such as age and sex and, on the other hand, specific indicators of human health. The proposed method is based on the processing of data from analyses of the diversity and proportion of microorganisms in the intestinal tract and other body fluids (saliva, breast milk, faeces), the amount of metabolites used as biomarkers and the consideration of the level of enzymatic activity of enzymes used as biomarkers, allowing to take into account individual characteristics of people. The method is based on in vitro analysis of the gut microbiota balance in children from one to twelve months of age and prediction of its recovery in established dysbiosis by calculating correlation coefficients between key indicators divided into three main groups:

1. Correlation between the composition and quantity of microorganisms in breast milk and in the child's stool;

2. Correlation between the enzyme profile and activity of enzymes responsible for the absorption and metabolism of milk components (lactose, lipids, oligosaccharides, proteins) in breast milk and stool samples of the child;

3. Correlation between the amount of metabolites derived from the metabolism of the major components of breast milk by the microbiota in breast milk and in the child's faeces.

There are three key aspects to keep in mind regarding the publication of sensitive health data in an anonymous mode. First, the precise definition of the term is quite difficult. Terminology differs across EU Member States. For example, in the UK, data that is 'linked-anonymised' or 'pseudonymised' may be considered 'anonymous' if the data controller does not have access to the linking key. Second, when it comes to data or biosamples relating to patients, it is uncertain how effectively they can be anonymised. Furthermore, if anonymised, there is a concern that some of their research value may be diminished. Third, complete (unlinked) anonymity prevents the donor from exercising their right to withdraw consent and makes it impossible to return research results or incidental findings to them.

CHAPTER SIX: DATA ANALYSIS IN SYNCHRONISING PHYSICAL SECURITY AND CYBER SECURITY IN DIGITAL SOCIETIES

6.1. General overview

The intertwining of digital technologies and the physical world ushers in an era where security is no longer limited to the cyber domain or the physical domain, but encompasses both. This requires a re-evaluation of security paradigms, highlighting the importance of synchronised strategies to protect our increasingly digital societies. The importance of this issue lies in its relevance to national security, economic stability and the protection of individual rights and freedoms. Blurring the lines between physical and digital processes, understanding and implementing integrated security measures is paramount.

The threat landscape in digital societies is characterized by its complexity and dynamism as adversary states continuously exploit the interconnections between the physical and cyber realms. Cyber-physical systems, such as electrical grids, transportation networks, and healthcare, are becoming prime targets for cyberbioterrorist attacks, demonstrating the potential of cyberattacks to cause physical consequences. This evolving landscape highlights the need for a unified approach to security that encompasses both cyber and physical vulnerabilities.

Synchronization between physical security and cybersecurity is critical to preventing, responding to, and mitigating security incidents. Inconsistent efforts can lead to gaps in security postures, making it easier for threats to penetrate defenses. A synchronized approach ensures that security measures are consistent, intelligence is shared across domains, and incident responses are quick and effective. This holistic perspective is essential to strengthen defences against complex threats that exploit the link between the physical and digital worlds.

Digital societies are characterized by their dependence on information and communication technologies for everyday functions, from governance and commerce to social interaction and entertainment. This dependence creates a cyber-physical environment that is integral to the functioning of society, but also introduces vulnerabilities. Protecting this world requires a nuanced understanding of how digital and physical security intersect and impact each other, necessitating strategies that are adaptive and flexible and forward looking.

Emerging technologies such as AI , the Internet of Things (IoT) and blockchain are playing a key role in shaping the security landscape. While these technologies offer innovative solutions to improve security, they also introduce new vulnerabilities and attack vectors. The dual purpose of emerging technologies underscores the importance of incorporating technology-centric security strategies that attempt to both leverage these innovations for protection and mitigate the risks they pose.

The synchronisation between physical security and cyber security also presents policy and governance challenges. Developing and implementing policies that address both areas requires coordination between a wide range of stakeholders, including government agencies, private sectors and civil society. Furthermore, the global nature of cyber threats requires international cooperation, further complicating governance efforts. Addressing these challenges is critical to establishing effective and sustainable security frameworks.

The economic implications of synchronized security strategies are significant. Cybersecurity incidents can have direct financial consequences, such as response and recovery costs, as well as indirect consequences, such as loss of consumer trust and damage to brand reputation. Conversely, effective synchronization can improve economic stability by protecting critical infrastructure, ensuring the reliability of digital transactions, and building trust in digital ecosystems.

Integrating physical and cyber security measures also raises social and ethical issues. Issues such as privacy concerns, surveillance and potential misuse of technology need to be carefully considered. Here we can present a real-life example that does not seem to concern the use and potential misuse of sensitive personal data. Tattoos and permanent makeup are widespread worldwide, yet there is considerably little published research regarding the health risks associated with them. Their increasing popularity has led to an increase in reports of subsequent infections. Tattooing can be seen as an example of a health risk (infections, psychological problems) on the one hand, and an iconic and social risk (the unregulated import, distribution and use of inks and other tattooing supplies) on the other. Although inks are injected into the human body, they do not usually require strict compliance with specific safety requirements, unlike other substances (e.g. drugs, implants, etc.). Inherently, this process constitutes an injury to the skin, which can result in superficial and internal infections, systemic inflammatory processes, eczema, psoriasis, lichen planus, photodermatitis, etc. Injuries sustained by breaching the epidermal barrier of the skin during tattooing represent a "gateway" for microbial pathogens that can subsequently cause local wound infection. In some cases, adverse reactions may occur immediately after the procedure, but prolonged infectious processes may also occur, as pathogens from the coloured pigments can enter the bloodstream via the dermis circulatory system. Due to these facts, the ink ingredients are considered as the main source for health risk. Whereas decades ago only natural dye products were used (one of the most common is an extract from the plant Lawsonia inermis), inks of uncertain origin and content are now widely used, as there are still no uniform international standards for their production. The tattoo inks available on the market are complex mixtures containing over 100 compounds of pigments, solvents, thickeners, preservatives and other impurities. The lack of a clear description also poses serious health risks, although information on the exact list of ingredients should be provided by each manufacturer. Tattooists and beauticians buy inks freely most often directly from suppliers or via the internet, which creates additional problems. The fact that many inks are transported and stored in reusable containers is also a serious concern. This process poses an additional risk of contamination (e.g. with staphylococci, streptococci, etc.). Results of scientific studies have reported the presence of both aerobic and anaerobic bacteria in commercial tattoo inks and permanent make-up stored under aerobic and anaerobic conditions. This means that even factory-sealed inks may contain anaerobic bacteria, which are known to thrive in low-oxygen environments (such as the dermal layer of the skin) together with aerobic bacteria. It is reasonable to assume that contaminated inks can cause infection by both types of bacteria.

On the other hand, there is a social and economic risk through the use of tattoo studios, which are essentially commercial activities. In a very cursory survey, there is a lack of serious control in our country both over the import of inks and supplies and over the activities of tattoo parlours in terms of compliance with the hygienic conditions for intervention in the human body.

Balancing the need to ensure the protection of individual rights and freedoms is a complex challenge that requires thoughtful approaches that respect ethical principles and social values.

Building resilience in digital societies requires a commitment to continuous exploration, innovation and collaboration. This includes not only developing technical solutions, but also creating a culture that recognizes security among people and organizations. Education and awareness are key components of this effort, as is the creation of partnerships across sectors and borders.

The synchronization between physical security and cybersecurity in digital societies is not only a technical problem, but a multifaceted challenge that intersects with politics, economics, society, and ethics. Addressing this challenge requires a holistic and integrated approach that recognizes the complexity of the threat landscape and leverages collaboration and innovation to build resilient defenses. As digital societies continue to evolve, the importance of synchronized security strategies will only grow, underscoring the need for continued research, dialogue, and action in this critical area.

Proposal for a new concept of the interaction between physical and cyber security

The convergence of physical security and cyber security in digital societies marks a significant paradigm shift in the approach to protecting our interconnected world. The importance of this topic cannot be overstated as it directly affects national security, economic stability and the safety and security of individuals. This increasing reliance on digital technologies has blurred the lines between physical and cyberspace, creating a complex landscape in which threats can cross these domains and have profound consequences. This academic research highlights the need for a synchronized approach to security, integrating physical and cyber strategies to address the multifaceted nature of modern threats. Such an integrated approach is not only useful, but also essential to reducing risks and increasing resilience in the face of complex and evolving threats.

The integration of AI and machine learning (ML) technologies into security systems is an example of the innovative strategies used to predict and counter threats. These technologies have the potential to revolutionize security practices by providing predictive capabilities, thereby shifting the paradigm from reactive to proactive security mechanisms. The case studies cited above, such as the Stuxnet worm attack and the Mirai botnet exploit, illustrate the concrete implications of cyber-physical threats and the critical need for a healthy synchronization between physical and cyber security measures. Such incidents serve as a reminder of the inherent vulnerabilities in our interconnected systems and the potential for catastrophic consequences if these vulnerabilities are not addressed appropriately.

The challenges associated with aligning physical security and cyber security are numerous and include technological, organisational and cultural aspects. Overcoming these challenges requires a concerted effort to foster interdisciplinary collaboration, integrate advanced technologies, and overcome complex regulatory environments. The paper shows that while technological solutions are indispensable, the human factor plays a key role in the effectiveness of security measures. In particular, education and training emerge as key components in cultivating a security-conscious culture that recognizes the interconnected nature of threats and the importance of integrated security practices.

Regulatory and compliance pressures further complicate the synchronization process, requiring flexibility and adaptability in security obligations to meet legal requirements. that at the same time effectively protect against threats. GDPR in the EU serves as a prime example of how regulatory frameworks are shaping security practices, requiring organizations to adopt comprehensive approaches that span physical and digital security. These regulations underscore the importance of synchronization not only to protect data and infrastructure, but also to ensure compliance with more stringent legal requirements.

The future of security in digital societies is inextricably linked to efforts to anticipate, adapt and mitigate the risks posed by the changing threat landscape. This requires continued research, investment in emerging technologies, and international cooperation to develop and implement effective synchronization strategies. A survey of cloud trends and forecasts reveals a clear consensus among experts on the growing importance of synchronization between physical security and cybersecurity. The integration of AI and IoT technologies, the focus on resilience and recovery strategies, and the emphasis on insider threats highlight the dynamic nature of security challenges and the innovative approaches developed in response.

The merging of physical and cyber security within digital societies marks a decisive shift in the approach to protecting critical infrastructure, data and assets. This integration is driven by the growing interconnection between physical facilities and cyber networks, resulting in the emergence of cyber-physical systems (CPS). CPSs are integral to the operation of critical infrastructure, including electrical grids, transportation, and healthcare, highlighting the importance of a unified approach to security. The authors argue that the interconnected nature of these systems makes them vulnerable to a wide range of attacks, necessitating synchronized security strategies that address both cyber and physical threats.

The complexity of the threat landscape in digital societies is further elaborated by Kitchin and Dodge (2014), who discuss how the digitization of physical transactions creates new vulnerabilities.

They highlight that traditional security measures designed to deal with physical or cyber threats in isolation are no longer sufficient. The need for integrated approaches to security is highlighted by Alcaraz and Zeadally (2015), who present an in-depth analysis of the challenges and solutions to protect industrial control systems from cyber-physical attacks. Their research highlights the criticality of synchronizing physical security and cybersecurity to protect against sophisticated attacks that can have catastrophic physical consequences.

The challenge of synchronizing physical security and cybersecurity strategies is explored by Collier et al. (2016), who propose a strategic framework for achieving effective integration. This framework highlights the importance of organizational coordination, intelligence sharing, and effective response strategies. Similarly, Zhu and Basar (2011a; 2011b) address the operational challenges of synchronization, including the need for compatible technology platforms and communication protocols across domains. These studies highlight the difficulty of achieving synchronization, but also the potential benefits of a single security posture.

The policy and governance dimensions of physical and cybersecurity synchronization are explored by Dunn-Cavelty and Suter (2009), who analyze the implications for national security policy and politics. They argue that effective synchronization requires not only technical solutions, but also policy frameworks that facilitate collaboration among government agencies, private sectors, and international partners.

From an economic perspective, Anderson and Moore (2006) present a general analysis of the costs and benefits associated with implementing synchronized security measures. They highlight the potential for significant economic impact, including preventing harmful breaches, protecting critical infrastructure, and improving user confidence in digital systems. This economic perspective is essential for understanding the wider implications of security strategies and justifying investment in synchronised security measures.

The role of technological innovation in facilitating the synchronisation of physical and cyber security is a key theme in the literature. Demirkan et al. (2020) discuss the potential of blockchain technology to improve security in cyber-physical systems by providing a secure and transparent mechanism for access management and control. Mitchell and Chen (2014) explore the use of AI to detect and respond to security threats in the physical and cyber domains, illustrating how technology can bridge the gap between traditionally separate domains.

Practical applications of synchronized security strategies are highlighted through case studies. Krotofil et al. (2015) present a case study on the security of industrial control systems, demonstrating how physical security measures can be integrated into cybersecurity defenses to protect against sabotage and espionage. These real-world examples provide valuable insight into the challenges and successes of implementing synchronized approaches to security.

The societal implications of synchronised security measures are discussed by Dunn-Cavelty and Leese (2018) who consider the impact on privacy and civil liberties. They warn that the integration of physical and cyber surveillance technologies can lead to invasive monitoring that raises ethical concerns. However, they also note that carefully designed security measures can improve public safety without compromising individual rights, stressing the use of a balanced approach.

The importance of international cooperation in achieving effective alignment between physical security and cyber security is highlighted by Nye (2016). He argues that cyber threats cross national borders, requiring concerted efforts to develop and implement security strategies that are effective at the global level. This perspective underscores the need for international norms and agreements that facilitate cooperation in protecting cyber-physical systems.

Looking forward, the literature suggests several areas for future research, including the development of improved threat detection algorithms, the exploration of new governance models, and the assessment of the long-term economic impacts of synchronized security strategies. Researchers such as Radanliev et al. (2020a; 2020b) suggest a focus on integrating emerging technologies such as IoT and smart infrastructure within a security framework. These future directions emphasize the continued evolution of the field and the need for continuous innovation and collaboration.

The literature review highlights the critical importance of synchronizing physical security and cybersecurity in digital societies. The growing interconnectedness between the physical and digital realms presents unique challenges, but also opportunities for developing comprehensive security strategies. The works reviewed collectively underscore the need for integrated approaches that address the complexity of the threat landscape that organization and technology integration evoke and the implications for policy, governance, and society.

Synchronizing physical security and cybersecurity in digital societies is a critical and complex endeavor that requires an interdisciplinary approach leveraging the latest technological advances and fostering a culture of security awareness. The importance of this topic stems from its direct impact on the protection of critical infrastructure, economic interests and the well-being of people in an increasingly digital world. As digital societies continue to evolve, integrating physical and cyber security will become even more important to address the complex and interconnected threats of the future. This academic research not only highlights the current realities and challenges of synchronization, but also underscores the need for innovative, integrated strategies for navigating the complexities of the digital age. The way forward requires collaboration, innovation and a firm commitment to improving security in all its dimensions, ensuring a safer and more sustainable digital society for the future.

Conclusions to chapter six

In today's world, where technology and the Internet play an ever-increasing role in our daily lives, cyberbiosecurity is emerging as a critical aspect of national security. This dissertation has examined the various dimensions of cyberbiosecurity, including the threats, vulnerabilities, and necessary protection measures. The analysis showed that biological systems and data are subject to increasing risks from cyberattacks that can have serious implications for public health, the economy, and social stability.

The main findings of the study underline the need for an integrated approach to cyberbiosecurity that includes both technical and organisational measures. It is important that countries develop and implement strategies to protect critical infrastructure, invest in training and awareness-raising among the population, and promote international cooperation in the fight against cyber threats.

The survey conducted among professionals in various fields such as security, cybersecurity and clinical laboratories also showed worrying results. The results of the survey revealed a low level of preparedness to protect sensitive biomedical data and a lack of preparedness to respond to bioterrorism threats. This highlights the need for immediate action to improve the capacity and preparedness of these key sectors.

KEY FINDINGS AND RECCOMENDATIONS

Based on the analysis and findings of the study, I propose the following specific measures to improve cybersecurity:

1. Legislative initiatives: Develop and adopt new laws and regulations that address the specific needs of cyberbiosecurity. These regulations should include strict requirements for the protection of biomedical data and incident response procedures. Particular attention should be paid to the IIA 2 regulation, which introduces mandatory standards for the security and confidentiality of medical information.

2. Training and awareness-raising: Conduct regular training and seminars for health care and laboratory staff on cybersecurity best practices. Trainings should include topics such as recognizing phishing attacks, password management, and use of encryption.

3. Invest in technology: Invest in advanced cybersecurity technologies, including intrusion detection systems (IDS), intrusion prevention systems (IPS), and network traffic monitoring tools. These technologies should be deployed in critical infrastructures and continuously updated.

4. International cooperation. Participation in international forums and initiatives for the exchange of information and good practices in the field of cyberbiosecurity. Establishment of partnerships with other countries and organizations for joint projects and research.

5. Organisation of regular simulations and exercises on response to cyber-attacks and bioterrorist threats. These exercises will help institutions identify weaknesses in their systems and develop effective action plans.

6. Public-Private Partnerships. Supporting public-private partnerships between government agencies, academic institutions, and the private sector to develop innovative cyberbiosecurity solutions and technologies

7. Monitoring and Auditing. Introduction of regular monitoring and auditing of cybersecurity systems in healthcare institutions and laboratories. This will help in early detection of vulnerabilities and timely remediation.

8. Dedicated protection for research centres with genetically modified organisms (GMOs). These centres should be equipped with specific measures to protect their databases and experimental results, as the potential consequences of compromising this information could be particularly serious.

Trends in the development of contemporary threats clearly outline the need for a strategic and integrated approach to cyberbiosecurity as an integral component of national security. Based on the research and analysis conducted, I offer the following recommendations for improving policies and practices in this area:

1. **Expanded involvement of the private sector and IT companies in cybersecurity:**

The private sector, including biotechnology companies, IT firms, and cloud service providers, owns a significant portion of critical infrastructure and biological databases. Therefore:

- Adoption of legislative requirements for compatibility with cyberbiosecurity standards (e.g. ISO/IEC 27001 with extensions for handling biodata).
- Encourage public-private partnerships between public institutions, academia and private companies to develop innovative biosensors, cryptographic algorithms and other technological solutions in the field of biosecurity.
- Establish secure mechanisms and protocols for incident reporting and information sharing between the public and private sectors.

2. **Regional cooperation in South East Europe:**

Cyber and biothreats are often cross-border in nature. This requires a coordinated effort between countries in the region through:

- Establishment of a regional coordination platform (e.g. a Balkan Cybersecurity Group under the auspices of ENISA or another international organisation).
- Organising joint exercises and simulations involving health, military and IT structures.
- Exchange of best practices and experts, creation of a regional database of competent specialists in the field.
- Development of a harmonised regulatory framework for biological data protection, control and uniform standards for the private sector.

In conclusion, the sustainable development of national security in the context of digitalisation and biotechnological progress is unthinkable without adequate cyberbiosecurity measures. The implementation of the above recommendations will contribute to the development of a more effective, adaptive and sustainable system of national and regional defence against modern hybrid threats. Cyberbiosecurity cannot be ignored as part of national security. It requires sustained effort and adaptability to address new challenges and ensure the protection of vital biological systems and data.

Only through coordinated action and sustainable policies can we ensure the safety and well-being of our society in the digital age.

CONCLUSIONS:

1. Legislative initiatives: Develop and adopt new laws and regulations to address the specific needs of cyber biosecurity. These regulations should include strict requirements for the protection of biomedical data and incident response procedures. Particular attention should be paid to the MIS 2 regulation, which introduces mandatory standards for security and confidentiality of medical information.

2. Training and awareness raising: Conduct regular training and seminars for employees in healthcare institutions and laboratories on best practices for cybersecurity. Training should include topics such as recognizing phishing attacks, password management, and using encryption.

3. Technology Investments: Invest in advanced cybersecurity technologies, including intrusion detection systems (IDS), intrusion prevention systems (IPS), and network traffic monitoring tools. These technologies should be deployed in critical infrastructures and constantly updated.

4. International cooperation: Participation in international forums and initiatives for the exchange of information and good practices in the field of cyberbiosecurity. Creation of partnerships with other countries and organizations for joint projects and research.

5. Simulations and exercises: Organizing regular simulations and exercises to respond to cyberattacks and bioterrorism threats. These exercises will help institutions identify weaknesses in their systems and develop effective action plans.

6. Public-Private Partnerships: Promote public-private partnerships between government agencies, academic institutions, and the private sector to develop innovative cybersecurity solutions and technologies.

7. Monitoring and auditing: Implementing regular monitoring and auditing of cybersecurity systems in healthcare institutions and laboratories will help in early detection of vulnerabilities and their timely remediation.

8. Specialized protection for GMO research centers: Special attention should be paid to research centers working with genetically modified organisms (GMOs). These centers must be equipped with specific measures to protect their databases and experimental results, as the potential consequences of compromising this information can be particularly serious.

SCIENTIFIC CONTRIBUTIONS

Based on the dissertation developed, the following scientific and applied contributions can be derived:

1. A model for combining physical security with cybersecurity and biosecurity in implementing permanent control of institutions and companies working with sensitive data is proposed.
2. A model is proposed for an interdisciplinary approach in upgrading the activities in providing cyberbiosecurity in the vector of sensitive personal data – processing of large data sets with sensitive information – regulation of storage and access to sensitive large databases.
3. A concept for an interdisciplinary approach to developing a protocol of events to provide the necessary cyberbiosecurity when dealing with sensitive data of people concerning their health status is proposed.

Cyberbiosecurity cannot be ignored as part of national security. It requires constant effort and adaptability to address new challenges and ensure the protection of vital biological systems and data. Only through coordinated action and sustainable policies can we ensure the safety and well-being of our society in the digital age.

PUBLICATIONS RELATED TO THE DISSERTATION

1. Bakov,K.,THE NEW REALITIES IN SYNCHRONIZING PHYSICAL SECURITY AND CYBERSECURITY IN DIGITALSOCIETIES , Scientific journal "Security and Defense" – National Military University "Vasil Levski," Year III, Issue 1, 2024.

2. Mollova-Doshkova, D., Bakov, K., Iliev, I., The Art of Asking and Analyzing Sensitive Questions in Breast Milk Microbiome Research, Acta Microbiol. Bulg., приета за публикуване в издание 40(2) за 2024г. (Q4) .

3. Bakova, D., Yaneva, A., Harizanova, S., Shopova, D., Mihaylova, A., Kasnakova, P., Bakov K. & Iliev, I. (2025). Monitoring Health Risks Associated with Body Modifications (Tattoos and Permanent Makeup): A Systematic Review. Cosmetics, 12(1), 8. (Q2)

PARTICIPATION IN SCIENTIFIC FORUMS WITH PRESENTED RESULTS FROM THE DISSERTATION

1. Bakov, K., New Realities in Synchronizing Physical Security and Cybersecurity in Digital Societies, report, Conference "Revolutions and Evolutions," Paisii Hilendarski University of Plovdiv, March 5-7, 2024, participation;

2. Iliev I., and Bakov K., The Green Economy – Challenges and Examples of Interdisciplinary Solutions, report, International Scientific Conference "The Interdisciplinary Approach in the Applied Field of Economic and Social Sciences";

3. Bakov, K., Financing of terrorist organizations through cryptocurrencies, report, International Scientific Conference "Interdisciplinary Approach in the Applied Field of Economic and Social Sciences";

4. Bakov, K., Social and Emotional Education in the Context of Physical Security in the Learning Environment, report, National Conference "Social and Emotional Learning in Teacher Training" (November 26-29, 2023).

5. Daniela Mollova, Kostadin Bakov, Miroslav Zhekov, Ilia Iliev, Potential for the development of biosensors for the analysis of sensitive parameters in the study of the breast milk microbiome, II National scientific conference Physics-Engineering-Technology, 27-28 November 2024, Plovdiv, Bulgaria, poster D-8, p. 71.

BIBLIOGRAPHY CITED IN THE ABSTRACT

1. Денчев, С. (2019). *Информация и сигурност*, Академично издателство „За буквите“ .ISBN 978-619-185-369-4
2. Чаушев, Х. (Декември 2024). Генеративен AI и съдържание в социалните медии – комуникационни предизвикателства в сферата на сигурността. *Сигурност и отбрана*(2), 179-187. https://doi.org/10.70265/YVKC6923

3. Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection, 8*, 53-66. https://doi.org/10.1016/j.ijcip.2014.12.002

4. Anderson, R., & Moore, T. (2006, October 27). The economics of information security. *Science, 314* (5799), 610-613. DOI: 10.1126/science.1130992. Retrieved from: https://www.cl.cam.ac.uk/~rja14/Papers/sciecon2.pdf

5. Collier, Z. A., Panwar, M., Ganin, A. A., Kott, A., Linkov, I. (2016). Security Metrics in Industrial Control Systems. In: Colbert, E., Kott, A. (eds) *Cyber-security of SCADA and Other Industrial Control Systems*. Advances in Information Security, vol 66 (pp. 167–185). Springer, Advances in Information Security, vol 66 (pp. 167–185). Springer, Cham. https://doi.org/10.1007/978-3-319-32125-7_9

6. Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics*, 7(2), 189–208. https://doi.org/10.1080/23270012.2020.1731721

7. Dunn-Cavelty, M., & Suter, M. (2009, December). Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection*, *2*(4), 179-187. https://doi.org/10.1016/j.ijcip.2009.08.006

8. Kitchin, R., & Dodge, M. (2014). *Code/space: Software and everyday life*. Massachusetts: MIT Press.

9. Krotofil, M., Larsen, J., & Gollmann, D. (2015, April). The process matters: Ensuring data veracity in cyber-physical systems. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security* (pp. 133-144). https://doi.org/10.1145/2714576.2714599

10. Li, Z., Chen, H., & Wang, P. (2019). Lateral flow assay ruler for quantitative and rapid point-of-care testing. *Analyst, 144*(10), 3314-3322.

11. Liu, H.; Ge, J.; Ma, E.; Yang, L. Advanced biomaterials for biosensor and theranostics. In Biomaterials in Translational Medicine, 1st ed.; Yang, L., Bhaduri, S.,Webster, T., Eds.; Academic Press: Cambridge, MA, USA, 2019; pp. 213–255.

12. Mitchell, R., & Chen, R. (2014). Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems. *IEEE Transactions on Dependable and Secure Computing*, *12*(1), 16-30. DOI: 10.1109/TDSC.2014.2312327

13. Nye Jr, J. S. (2016). Deterrence and dissuasion in cyberspace. *International security, 41(3)*, 44-71. https://doi.org/10.1162/ISEC_a_00266

14. Radanliev, P., De Roure, D. C., Nurse, J. R., Mantilla Montalvo, R., Cannady, S., Santos, O., ... & Maple, C. (2020a). Future developments in standardisation of cyber risk in the Internet of Things (IoT). *SN Applied Sciences*, *2*, 1-16. https://doi.org/10.1007/s42452-019-1931-0

15. Radanliev, P., De Roure, D., Page, K., Nurse, J. R., Mantilla Montalvo, R., Santos, O., ... & Burnap, P. (2020b). Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains. *Cybersecurity*, *3*, 1-21. https://doi.org/10.1186/s42400-020-00052-8

16. Zhu, Q., & Basar, T. (2011a, April). Towards a unifying security framework for cyber-physical systems. In Proceedings of the workshop on the foundations of dependable and secure cyber-physical systems (FDSCPS-11) (pp. 47-50). Retrieved from: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=b860375d2d89142f9b26870411f7ec7e0b56568a

17. Zhu, Q., & Başar, T. (2011b, December). Robust and resilient control design for cyber-physical systems with an application to power systems. In *2011 50th IEEE Conference on Decision and Control and European Control Conference* (pp. 4066-4071). IEEE. DOI: 10.1109/CDC.2011.6161031