„BABEȘ-BOLYAI" UNIVERSITY
CLUJ-NAPOCA
FACULTY OF HISTORY AND PHILOSOPHY
DOCTORAL SCHOOL OF
INTERNATIONAL RELATIONS AND SECURITY STUDIES

PH.D. THESIS
SUMMARY

Ph.D. supervisor:
Professor Adrian Liviu Ivan, Ph.D.

Ph.D. student:
Sorin Gurzău

Cluj-Napoca
2021

„BABEȘ-BOLYAI" UNIVERSITY
CLUJ-NAPOCA
FACULTY OF HISTORY AND PHILOSOPHY
DOCTORAL SCHOOL OF
INTERNATIONAL RELATIONS AND SECURITY STUDIES

Cybersecurity in the XXI Century.
Sustainability in Business Intelligence

Ph.D. supervisor:
Professor Adrian Liviu Ivan, Ph.D.

Ph.D. student:
Sorin Gurzău

2021

CONTENTS

KEY-WORDS: Cyber Security, Governance, International Relations, Cyber Diplomacy, Critical Infrastructures, Cyber Defense Strategies, European Union, North Atlantic Treaty Organization, Business Intelligence, Competitive Intelligence, Cyber Intelligence, Precautionary Principle, Ethics, Public Health Globalization, Romanian Health System, „Swiss Cheese" Model, „The Troika of Errors", COVID-19

INTRODUCTION

ARGUMENT AND MOTIVATION

Because of the extensive digitalization, the massive online connection of the global population and the possession of fixed and mobile electronic devices, the developed technologies belonging to the fourth and subsequent fifth industrial revolution have generated, besides advantages, a series of negative consequences, including those regarding cyber security, thus cyber-attacks becoming a real danger for the business environment as well. Indeed, there is information coming from the global business environment, which places cyber-attacks in the top ten most likely risks and with the greatest impact (WEF 2020*c*. 60-63).

Regarding the undisputed importance of technology worldwide, cyber governance is becoming an imperative desideratum, while a public-private partnership can score significantly in the field of cyber security. On the other hand, in the context of the cyber governance gap, the discrepancy between its own and/or partners' cybersecurity targets and the development of technology demands the business environment to make additional and vital efforts for sustainability in *Business Intelligence*. From the perspective of cyber security, the major involvement of information technology in all fields of activity produces the continuous and rapid change of the status of national and international security, especially in the case of critical infrastructures (energy systems, transport, health, water supply), with possible impact on interstate relations (WEF 2020*c*. 65). The identification of critical points and vulnerabilities in achieving cyber security, but also of its control points are integral parts of *Business Intelligence* and can be assimilated to the precautionary principle, which proves its usefulness here too, not only in the public health where it was stated and applied.

In such context, this thesis opens a very current topic of study, namely cyber security and the customization of sustainability aspects in *Business Intelligence*.

The motivation for choosing this theme is found not only in the current evolution of the phenomenon of relatively marked cyber insecurity but also in the already classic one of security in general. Worldwide, the state of security today is still characterized by sufficient vulnerabilities, complex and not always known causality, with more or less violent manifestations in different sectors. This situation occurred as a result of cumulative pressure,

over time, of multiple factors: political, economic, financial, social, cultural, biological, religious, demographic, military - which influenced the safety climate of states and citizens.

Regardless of the form of funding, public or private, the healthcare system is a business: it sells services, holds, analyzes, and transmits data at the national (horizontal and vertical/hierarchical) and international level to European and global organizations and partners of research projects. It is obvious that in this context, health diplomacy and the general principles of ethics, and in particular of medical ethics, acquire an even more important role, especially when cybersecurity breaches create opportunities for "fake news" with a defined purpose of manipulation, in extreme medical situations, such as epidemics.

OBJECTIVES

The present research aims to contribute to the analysis of cyber security aspects especially at the organizational/institutional level and at the same time to offer the openness to finding new, modern solutions that ensure sustainability in *Business Intelligence*.

The main objective of the research is both to approach the topic of cybersecurity from a multidisciplinary perspective and to be able to continue the debate and networking on this issue, which is fundamental for both national security and regional and international security, all the more so as no entity alone can eliminate or reduce cyber insecurity.

We start from the **hypothesis** that three important domains/sectors (hereinafter referred to as targets), apparently independent, interfere in generating cyber insecurity (vulnerabilities and threats) or in generating cyber security (resilience) at the organizational, societal, and finally international level. These targets are international relations/diplomacy, political decision-making/governance, and business environment/*Business Intelligence*/critical infrastructures.

We have chosen a critical infrastructure as a case study of cyber security in the sustainability of *Business Intelligence*, that of health services, in particular the health services system in Romania. The digitization of the medical system (e-Health) as a requirement for storing, processing, and transmitting data allows the assumption that if there is cybersecurity there is data security, a correct analysis within the Business Intelligence process allowing measures and strategies as an integral part of the overall security strategy.

With the intent to answer these questions and achieve the goal of the research, we have set ourselves the following **objectives**:

1. Placing cybersecurity in the current context of an overall security

2. Assessment of risks/hazards/vulnerabilities in cybersecurity at the individual, organizational, state, and global level
3. Analysis of *Business, Competitive, Market,* and *Cyber Intelligence* positioning in the functionality of critical infrastructures
4. Integration/association of target areas in achieving cybersecurity and sustainability in *Business Intelligence.*

RESEARCH METHODOLOGY AND STRATEGY

This Ph.D. thesis is the result of inductive research carried out in three directions centered on cyber security. Two important but intertwined stages were the basis of the research, namely the documentation by going through/revising/systematizing the specialized literature and analyses – the case study.

• *Review and systematization of the specialized literature*

The specialized literature in the areas of interest (target) of the research is rich, our interest is directed especially towards publications and other types of national and international sources from after 2000 until the first half of 2021. The presentation of the general concepts and their evolution started from the works (books and articles) of the well-known, classical authors of each field present especially in Chapters 1 and 3 of the elaborated thesis. The paper contains over 300 bibliographic references, out of which a smaller number deals with the subject of cyber security in the health service systems and much fewer than of *Business Intelligence* in the same sector, the systematic concern for them being recent, and the specialized literature poorer.

• *Analyses and case study*

We have included in the thesis some personal analyses on four topics that connect cybersecurity, *Business Intelligence*, supranational organizations and political-military alliances, international relations, health systems, and public health. These analyses were based on the collection of data from official sources (reports, notes, press statements of governments/government agencies/ministries, and their representatives, international bodies, and professional organizations). Part of the information was taken from online/media sources and here we refer to new information/points of view, as yet unsystematized.

The analysis of cyber security issues and the role of *Business Intelligence* in the Romanian healthcare system was based on the adaptation of two established analysis models ("Swiss Cheese" and "The Troika of Errors"), used in various fields, but not for cyber

security issues in the health sector or the combination of cyber security–*Business Intelligence* in Romania.

The inductive approach was also chosen for the case study, in which we opted for the qualitative method. In this regard, a questionnaire was created that was self-administered by the persons who agreed to answer the questions formulated. The results were interpreted descriptively.

The doctoral thesis was structured in five chapters, as follows:

Chapter 1 - GLOBAL SECURITY IN THE XXI CENTURY starts from the presentation of theoretical aspects that focus on the evolution of the concept and security environment that support the classification of cyber security and the challenges at its address as current priorities.

In the context of the continuous upward trend of the globalization process, the migration of attention to the spectrum of insecurity from the military dimension more towards the economic, political, social, and environmental dimensions have shown that the growing threats can no longer be mastered strictly within the national framework. After the Cold War, the concept of security has taken a different approach, while international and supranational policies had a better-defined role, like other types of actors besides the state ones have intervened (Chifu 2009. 1-18), by far the most important role in reformulating the concept of security being owned by the Copenhagen School. The need for cooperation and action to preserve collective security in all its dimensions, closely interconnected, has become even more evident, and the intervention of security institutions and organizations (EU, NATO, UN) more than salutary (Burke *et al.* 2016. 64-79). The dynamics and multidimensionality of security issues have increased attention towards human security. Placing human security at the heart of the international security agenda was officially recognized in the early ‘90s in the United Nations Human Development Report, which states that "security has symbolized protection against threats such as diseases, hunger, unemployment, crime, social conflict, political repression and environmental risks" (United Nations Development Program 1994. 22) affecting, in fact, all levels of society with consecutive expansion in international relations. The change in the hierarchy of security threats in the XXI century brought in the spotlight the threats to the functioning of the economic system, the proliferation of weapons of mass destruction, climate changes,

international terrorism, population migration, diseases with epidemic/pandemic evolution, and last but not least cyber crimes, which have become truly fearsome by their frequency and magnitude. In the contemporary security environment, the binder between terrorism and crisis or war situations is the very cyberspace as a bridge between the state, the political sector, the business sector, and the terrorist organizational structures.

Cyberization is currently considered a consequence of computerization and cybernetization (Ma 2016. 1-9), leading to the emergence of cyber power and its migration to non-state actors, as a new dimension of power in the XXI century (Nye 2010. 1-19). With certainty, the occurrence of the Internet offered unlimited possibilities for communication and knowledge and opened up, albeit initially seemingly insignificant, the problem of cybersecurity and then the associated hyper-securitization of cyberspace (Hansen–Nissenbaum 2009. 1164). Challenges for cybersecurity, including cyber warfare, are a reality, and the most accurate actions to combat them are essential for all sectors and areas of activity. The main problem of the vulnerability of information systems, however, is related to the business environment and espionage, despite the general impression given by the specter of a major cyber incident at the level of critical infrastructures. E-health is a bridge that connects a sector of critical importance, that of health services, with the digital world, and cannot currently be separated from the Internet of Things, which has become an important focal point for public health as a defining component of human security and, implicitly, of general security. The issue of securing cyberspace has appeared on the EU's political agenda and is perceived as a growing threat towards citizens, governments, and businesses in its Member States. In this respect, the EU is an actor of cybersecurity securitization, even though there are differentiated tasks at the Union’s level in the consensus of the collective effort to address cybersecurity (Christou 2018. 278-301). It is precisely in the context of the above that the EU together with NATO has been forced to radically rethink their common approach regarding the protection of information networks.

Last but not least, we have found that governance and cyber diplomacy, as new branches of the core areas, have an overwhelming role in achieving optimal solutions for sustainable general governance acts. As a particular result of the multinational impact of cybercrimes, the need for an international consensus on cybersecurity is implied, by requiring an agreement of the legal framework, which must necessarily be continued with implementation and an operational consensus. While cybersecurity addresses issues closely related to sovereignty, cybersecurity management at the national or international level

involves a multitude of issues and requires different types of areas of expertise aligned in a communication and cooperation relationship.

CYBERSECURITY AND STRATEGIES TO DEFEND THE KEY ENTITIES are presented in **Chapter 2**.

The protection of critical infrastructures against cyber-attacks has been an acute problem over time, proportional to the probability of a cyber-attack, with the European Union and the US adopting important initiatives in the field of critical infrastructures' cybersecurity that are currently practically already or are on the verge of becoming critical information infrastructures, all being of vital importance. Investigations conducted at the European level have revealed that the fourth cybercrime threat was the one considered about attacks that distort or even undermine the internal functions of one or more critical infrastructures (EUROPOL 2019. 23). Massive cyber-attacks on critical infrastructures have already a rich track record, the best known since Estonia (2007) and the extensive WannaCry (2017-2019) declared by Europol of an unprecedented level, all the more since only a few countries have not been affected by the attack (EUROPOL 2017. 30). Regarding the cybercrime-type actions in Romania, during 2019 low-complexity attacks were recorded that addressed mostly the health services sector, highlighting the vulnerability and lack of concern for ensuring minimum cyber protection measures in the medical system (SRI 2020a).

The threats to cyber security required the development of the new security strategy in the field, so that at the level of the European Union, with the support of the European Union Agency for Cybersecurity, the process of revising Directive (EU) 2016/1148, known as the NIS Directive, was initiated, and the proposal for the NIS Directive 2.0 was launched. The integration of the European and global dimensions of cybersecurity lies with cyber diplomacy, which plays an important role in the ability to respond directly to current threats and to substantiate better cooperation in the actions against future threats. In this context, the EU has built the cybersecurity strategy of its infrastructures based on defense and cyber diplomacy in positioning itself as a peace defender (Cîrnu 2019. 35-40) based on the precautionary principle, with a real potential to defuse conflicts in cyberspace.

Taking as a starting point the evolving presentation of the cyber security strategy of the European Union, we analyzed based on several defined criteria the national cybersecurity strategies in force during 2015-2021 in Romania, Germany, France, Belgium,

and Estonia. It resulted that Romania and Germany are focused on establishing and promoting the role of public-private partnerships and the safe use of communication and information tactics by citizens, private organizations, and authorities in the cyber environment. On the other hand, France aims to ensure the safety of the business environment and the sustainability of cyberspace. Specifically, international cooperation and strengthening competencies are mentioned in the strategies of Romania, Estonia, Germany, and France, and last but not least the protection of critical infrastructures (essential services) are specified in the strategies of Romania, France, Germany, and Belgium.

The last subchapter on the impact of actions to maintain the international security of cyberspace is intended to discuss the role of powers and elites in the era of globalization, in particular of NATO, for which we have argued the classification as an elite. According to Burke, global political reality requires new approaches to security, based on a better ethical view of what security truly means (Burke *et al.* 2016. 64-79). In the context of contemporary global threats, we set out to analyze the (ethical) principle according to which "all security actors have the responsibility to create security for all" as the US and NATO consider for the achievement of global security. Is the elite position at risk by the vulnerability of cybersecurity? The data presented show that NATO's cyber-attacks and cyber security are a sensitive topic highlighted in the official reports of the organization and of some governmental institutions since 1998, the type and conception of a cyber attack representing a direct threat to their position, due to the asymmetrical problems generated. Among the long-term decisions on cybersecurity that NATO member states took at the Warsaw Summit in 2016 was the recognition of cyberspace as the fifth area of armed conflict in which NATO will be operational, in addition to the other areas: air, sea, land or space. Also, as part of strengthening joined cooperation and challenges, in February 2016, NATO signed a technical agreement with the EU on cyber defense cooperation.

We chose to treat in **Chapter 3 - THE BUSINESS INTELLIGENCE - CYBER SECURITY RELATIONSHIP** in which *Business Intelligence* is a key factor in the development of organizational performance, both in private and public law entities.

Integrated into society and its institutions, the business environment has besides financial interest also ethical and political perspectives, having a strong influence in decision-making and determining the way companies decide to manage their activities (Freeman–Burton 2019. 1). Unlike *Business Intelligence*, *Business Analytics* involves the use of statistical procedures in data analysis that are also the basis of the predictive models

that substantiate the decision management, thus being a complement to the *Business Intelligence* process. Several studies consider that four elements integrate the areas of *Business Intelligence*, *Business Analytics*, and organizational performance management: competence, documentation, visualization, and work culture, but the elements that integrate *Business Intelligence* and *Business Analytics* are software programs and data management, elements also present in the public sector for performance management, electronic governance being complementary (Yahaya *et al.* 2019. 292-298).

After 2000, information began to appear on the aspects of data collection in *Business Intelligence*, which raises the issue of ethical operation. Unlike *Business Intelligence*, extraction of data from the external environment of the organization, which is the specific framework of *Competitive Intelligence*, allows predictive analysis, which is becoming increasingly important in the *Business Intelligence* process and as a result, the use of *Competitive Intelligence* in the business environment appears as a necessary extension of *Business Intelligence*, both depending on the qualification of the human factor. Naturally, the question arises when does *Competitive Intelligence* turn towards industrial espionage? Industrial espionage can be framed as a form of commercial data extraction, and the boundary between *Competitive Intelligence* and industrial espionage can sometimes be blurred, easily leaving room for diversion to espionage in a voluntary or non-voluntary manner, but certainly facilitated by the wide access to advanced information and communication technology. It is not to be neglected the fact that there are known involvements of states in industrial espionage, and also the involvement of private companies in the industrial espionage actions of governments (Crane 2005. 233-240). Another type of intelligence related to the business environment, in fact, a component of the business, is *Market Intelligence*, which also refers to the collection and analysis of information from the external environment of a company but which, unlike *Competitive Intelligence*, investigates more broadly, in an integrated approach, and the results obtained have long-term implications, with an obvious feature of complementarity with *Competitive Intelligence* (Jamil 2013. 465-469). We noted in our approach that the security of cyberspace and the correctness of the information collected are completed and correlated with cyber intelligence that refers to the collection, analysis, and interpretation of digital data in and through cyberspace, representing threats, transformed or not into risks that become strategic information in the business environment. In this way, cyber intelligence becomes an

important part of creating safe cyberspace and in the sustainability of *Business Intelligence* (Moore 2020. 1-14).

As technology has now become an integral part of the health sector, healthcare organizations must integrate appropriate *Business Intelligence* systems into their operations (Ashrafi *et al.* 2014. 117-130). We have identified common *Business Intelligence* and *Business Analytics* tools within organizations and those found in research activities, and we have seen that the specific tools of *Business Intelligence* are entirely common as stages in research. Unlike *Business Intelligence*, *Business Analytics* is much more suitable for conducting the research itself (prognosis, predictive modeling) than for evaluating the project performance.

Deepening the application of international laws from the point of view of ethics in the health systems is all the more important because at the intersection of cybersecurity and medical research is the human subject. The existence of so many common elements of *Business Intelligence* and *Business Analytics* between organizations and research draws, even more, attention to the aspects of professional ethics, confidentiality, precaution, and social responsibility. Cybersecurity is not optional if aspects of ethics in health and research are taken into account, but is a prerequisite for the application of the principles of medical ethics, first of all of the confidentiality, and is thus the preamble to compliance with data protection legislation. Cybersecurity thus operates on the precautionary principle, applied in the field of public health.

In **Chapter 4** we intended to outline **THE INTERNATIONAL CIRCUMSTANCES DURING THE COVID-19 PANDEMIC (1 JANUARY 2020 – 31 MARCH 2021).**

On 31 December 2019, the Health Authorities in China reported to the World Health Organization several cases of viral pneumonia of unknown origin in Wuhan, Hubei province. Due to the rapid spread of the disease, the WHO declared the phenomenon as a pandemic on 11 March 2020 (European Centre for Disease Prevention and Control - ECDC 2020. 1-10). A year apart, the WHO made public the Report of the international team of specialists who could not specify the exact source of the epidemic in Wuhan, that is of the pandemic, respectively. The unpredictable evolution of the health crisis caused by the COVID-19 pandemic has raised questions from the very initial stage regarding the global governance related to it because the measures that have been implemented by many governments have practically violated the principles of health diplomacy through unilateral

decisions. The pandemic shows that public health problems can no longer be maintained strictly at the national level, the rapid spread of the disease falling within the context of globalization, with undesirable implications for the economic, social, and even political dimensions of security (Jora 2020. 119).

The personal analysis on the principle of multilateralism in the actions of states and of the WHO, the UN, and NATO during the COVID-19 pandemic highlighted that the translation of multilateralism into the situation of health crisis produced was accepted by the WHO member states in May 2020 by adopting the Resolution on the collective response to COVID-19, and highlighting the leading role of the WHO in the crisis management. Another common issue of the UN, and the WHO relates to the issue of global security with a direct focus on the health domain, technical expertise, and last but not least, financial resources influencing the efforts to rebuild high-performance health service systems. The third common issue noted in the statements of the two organizations is related to their funding problems in the context of the COVID-19 pandemic and solidarity actions. The actions of the WHO and China have initiated diplomatic disputes, economic losses, trade-type tensions, and a climate of mutual mistrust as a whole, worldwide. The WHO has lost credibility, and its multinational funding has been the subject of intense debate in mid-April 2020 when the US Administration announced a temporary halt to funding for the WHO (later resumed). The allegations against the WHO, as a partisan of the Chinese model of addressing the COVID-19 epidemic, could be framed as a continuation of China's hard-type securing process, started by the US during the Trump Administration (LARICS 2020). Also based on multilateralism, NATO was confronted with the need to reinterpret Article 5 of the Treaty, possibly inapplicable due to the general equal vulnerability of civilians and military personnel, but NATO has acted permanently so that "this health crisis does not become a security crisis" (NATO 2021*a*) (NATO 2021*b*).

The development of COVID-19 vaccines has meant a fierce battle between Russia, the USA, the United Kingdom, and China (although developed after the Russian Sputnik vaccine, the Chinese CoronaVac vaccine was the first in the world to be used nationally) not only to obtain vaccines and concerning their effectiveness but also to the way (even the priority) in which the countries of the world will have access to the necessary doses, generating, at least in the first phase, the nationalism of vaccination. Even though the European Union has also partially joined this trend, the COVID-19 vaccination campaign started in all EU countries simultaneously on December 27, 2020, in the spirit of European

solidarity (Consiliul Uniunii Europene 2020). The opposite of vaccination nationalism is the multilateral initiative COVAX, managed in a public-private partnership, that has relied on equitable access to the vaccine of low- and middle-income countries, but has raised the issue of their use as a strategic foreign policy tool and the acquisition of international influence (Ameyaw-Brobbey 2021) by strengthening relations and geopolitical domination, examples of which are China and Russia. As for Romania's policy concerning the COVID-19 pandemic, it has closely followed the model of the European Union, being, in addition, the first Member State to manage the EU's strategic reserve of medical equipment. Also, Romania was the first NATO member state to use the Alliance's Strategic Transport Capability, bringing to the country means in the fight to combat the pandemic.

The issue of cybersecurity, since the beginning of the pandemic, has highlighted several ethical, legal, and even technical aspects regarding the huge volume of data collected and their security/confidentiality, as well as cyber espionage. We have formulated in the previous chapters the hypothesis that the precautionary principle in public health overlaps with cybersecurity in terms of measures and actions to identify and prevent vulnerabilities causing insecurity. Since its onset, the COVID-19 pandemic has been accompanied by an exodus of true and false information (infodemic), with the involvement of state actors, largely supported by social networks that quickly generated measures to combat and prevent the phenomenon of "fake news" (China and Russia were directly accused). The COVID-19 pandemic has caused the intensification of fears induced by the avalanche of online information (cyberchondriosis), known to have an impact on public health (Starcevič *et al.* 2020. 53-61). As for the intensification of state-type cyber espionage, it targeted not only the competitive research for the treatment, but also for the creation of the vaccine (Fidler 2020*b*), a fact illustrated in early December 2020 when the European Medicines Agency was the victim of a cyberattack targeting the Pfizer vaccine, its production, and subsequent distribution not being affected (CERT-RO 2020*a*).

The evolution of the COVID-19 pandemic has proved without any doubt that informational systems/information have a central role in the reaction of national governments and international organizations, their policy and decisions are based on data analysis and prognoses. The relationship between *Business Intelligence* and COVID-19 pandemic was analyzed by Paul Grill who found that the problem of large databases in *Business Intelligence* is actually the lack of them and which, together with an amount of correct data collected lead to completely wrong data regarding the parameters used to

monitor the pandemic (confirmed cases, total deaths, total cured people), the analysis of incomplete or wrong data leading obviously to the increase in the probability that the measures will also be wrong. The implementation of *Business Intelligence* in the management of the pandemic crisis must be based on reliable data, only in this way, the *Business Intelligence* would have a significant contribution in supporting the organizations involved in the health crisis, not only from a medical perspective but also from the business environment perspective (Grill 2020).

Chapter 5 - PERSONAL CONTRIBUTIONS. CYBERSECURITY AND *BUSINESS INTELLIGENCE* IN HEALTHCARE SERVICES AND HEALTH GLOBALIZATION brings to attention the globalization of public health and international health governance, as well as health diplomacy, as a preamble to analyze the role of cybersecurity in the functionality of health service systems as core units of global public health. Including the theme of public health in the external policies of states (Katz *et al.* 2011. 517-520) and its governance is supported by a multitude of events carried out and recorded especially in the last hundred years which have highlighted the fact that in the context of globalization and the development of global governance it is inherent for independent states to enter in partnerships in which to cooperate not only with each other but also with non-state actors (Kickbush–Buss 2011. 601-610). Concerning the many risks imposed to global public health, associated with infectious diseases, international trade in opium and alcohol, occupational hazards, and transboundary pollution (Fidler 2001. 844-845), Sophie Harman stated that "international health governance is an emerging domain combining public health, medical sociology, health economics, international law, anthropology, political science and international relations" (Harman 2017. 1-2). Thus, threats to global health have created a trend that brings to attention the current and effective involvement of health diplomacy, a pioneering domain, and a new branch in the theory and practice of international relations (Jora 2020. 113) along with the management of national health systems to maintain general safety. The growing importance of the health-safety nexus (hybrid threat) reflects political responsibility and the implications of the two articulations between health and safety – securitization of health and medicalization of security (Nunes 2012. 151-152). Romania is an active part of international agreements, networks, and specific organizations, being involved in diplomatic efforts to protect global health. Studying the history of the Romanian health services system we found that its

significant change and modernization occurred after 1990 due to the emergence in the health legislation of the right of private healthcare providers to operate. On the other hand, the Romanian healthcare system has faced malfunctions of the health card and the electronic health file, as well as episodes of cyber-attacks, officially announced since 2012 (WannaCry or others resulting in payments for partial or total database recovery). The security of health data is strictly regulated by the EU Directive 95/46/EC, and per The Romanian Intelligence Service's competencies in the field of national security, and the mission of the National Cyberint Center being the protection of critical infrastructures that includes the health system. Our case study on cyber security issues and the role of *Business Intelligence* in the Romanian healthcare system started from the hypothesis that, as a consequence of active and system errors, cyber security is affected and leads to events with a negative impact upon healthcare. The use of the "Swiss Cheese" model (Reason 2000. 768-770) in the analysis has highlighted vulnerabilities in terms of cybersecurity. The analysis of vulnerabilities, risks, and cyber insecurity events are part of the general risk management in the organization and are an integral part of *Business Intelligence*, while the management of errors is extensively substantiated by the "Troika of Errors" (Helmreich *et al.* 1999. 19–32). The brief foray into the Romanian healthcare system is the qualitative part of our research and presents the opinions on cyber security and *Business Intelligence* in achieving the performance and sustainability of a number (smaller than expected) of people with managerial responsibilities in the health services sector in Romania. The results showed not only partial knowledge and awareness of the issues under discussion but also a lacunar implementation, especially in the public health system, *Business Intelligence,* and of the measures specific to cyber security.

CONCLUSIONS

The particular placement of cybersecurity in the current context of general security in the XXI century is determined by the upward trend of cyberization when practically the increasingly pronounced addiction towards cyberspace transcends in all fields of activity and has irretrievably altered the classical environment of security. In practice, the military, political, economic, societal, and environmental dimensions can no longer be separated from cybersecurity, which is now becoming the equivalent of a common denominator of all these. Whether we refer to the relations between states, non-state structures, or supranational organizations (possibly affected by the transformation of cyberspace into a space of power

through information holding, capacity of deterrence, defense or attack, and resilience), governance and paradoxical to the business environment, these "target" areas are contributors to both endangering and generating security. We do not consider it excessive to affirm that cyber diplomacy is becoming an essential issue for the foreign policy of the XXI century, which cumulatively targets human rights, security, and economic policy. The ”voice” and the joint action are essentially an obvious necessity for the security of cyberspace, despite the reluctance that still exists from the perspective of sovereignty and, implicitly, of the national strategies.

The multitude of threats materialized with cyber-attacks upon state structures, **critical infrastructures**, or even private operational organizations of some critical infrastructures and their consequences were defining in the securitization of cyberspace and led to the formulation of national or common cyber defense strategies (e.g. the European Union) and which subsequently, after implementation, were subjected to up-dating according to the new threats and need for increased vigilance. Again, it is necessary to mention the role of diplomacy in finding common measures of action, avoiding disputes, and achieving the goal of maintaining cybersecurity without, however, erasing the differences imposed by the principle of national sovereignty (an aspect resulting from our analysis of the national cybersecurity strategies in five Member States of the European Union. It cannot be excluded that if the critical infrastructures and critical informational infrastructures have suffered from various cyber threats (e.g. energy, transport, telecommunications, military systems), areas less targeted in the past have become new targets, namely the health service systems (see the WannaCry attack) or the central water supply systems (the triad quantity-quality-cybersecurity) in which the processes computerization has evolved extremely fast.

The assessment of risks/hazards/vulnerabilities in cybersecurity at the individual, organizational, state, and global levels shows that neither powers nor elites have been bypassed by the sensitive issue of cybersecurity. Even **NATO**, which has been argued in the thesis that it is an elite, has been among the cyber-attacked structures since the late '90s under the circumstances in which the US became an important player in the fight against international terrorism. Our analysis highlighted the existence of vulnerabilities and exposure to direct threats generating asymmetries in the case of powers/elites. Paraphrasing Article 16, paragraph 2 of the Romanian Constitution "no one is above the law" we can state in the context of our analysis that "no one is above cyber vulnerabilities and threats".

The integration of *Business Intelligence* systems into the systemic management supported primarily by the risks culture as part of the organizational culture (**one of the many situations generating vulnerabilities**) can lead to an efficient process of good governance. In the field of health, *Business Intelligence* solutions are based on an important volume of data ("big data" collected, stored, analyzed, reported, and transferred) towards which there is no doubt that they have and will have the potential of a positive impact on the role of basic units for the national and global public health. **The health system in Romania**, as well as those in the Member States of the European Union and not only, operates with cyber-vulnerable tools and here we refer to the health card and the electronic health file with a role in streamlining the service, but with frequent malfunctions and problems related to the confidentiality of sensitive data.

Overall, the analysis of ***Business Intelligence* positioning in the functionality** of critical infrastructures (including the health systems) of public law shows rather a modest and fractured implementation, unlike the private sector where *Market* and *Cyber Intelligence* are competitively associated and operational. Among the potential benefits represented by *Business Intelligence*, as well as by the other types of *intelligence* mentioned in the health sector, data consolidation and protection (for example, personal data, economic data) seem to come first. In other words, *Business Intelligence* as an integrative method, *Competitive Intelligence* as a method with a constructive potential, *cyber intelligence* as an insurance method coexists and operates in a synergistic relationship. Certainly, the complementarity between informatics security and the *Business Intelligence* process in organizational sustainability can define the role of public and private organizations in the national cybersecurity strategies. On the other hand, however, the responsibilities of the private sector's organizations regarding the protection of critical infrastructures and critical informational infrastructures cannot be excluded from the process of collective securitization.

Under what circumstances are organizations/companies in any field of activity more vulnerable? The international conjuncture during the COVID-19 pandemic (January 1, 2020 – March 31, 2021) that we analyzed in our thesis has brought to attention, at an exponential magnitude, a phenomenon previously present, namely the infodemic, this time with incomparably more severe consequences because it concerns the global public health (Romania was no exception to the aggravation of the infodemic). In parallel with the infodemic, the COVID-19 pandemic has generated the resurgence of cyberchondriosis, associated with the increase in the state of uncertainty and fear of disease, a phenomenon that can be considered

similar to terrorism. From the cybersecurity point of view, the COVID-19 pandemic has once again shown the known malfunctions and vulnerabilities of healthcare systems, but also several ethical, legal, and even technical aspects regarding the resulting metadata and their security/confidentiality. As a whole, cybersecurity and *Business Intelligence* would provide an effective framework for understanding the phenomenon and would provide more pertinent ways out of the pandemic.

The tendency to the isolation of the EU member states, the lack of cooperation, in the first phase motivated by the sovereignty, while worldwide, the at least suspicious actions and measures of the WHO regarding China at the onset of the pandemic, have disrupted the international climate through the vehement contestation emerged from the US and other countries. In the context of global health and safety, another aspect of the pandemic, namely the vaccination campaign, has once again upset the international situation through the so-called geopolitics of vaccination, as a result of the COVEX initiative, although overall, the WHO has had a significant contribution in terms of health diplomacy by promoting the principle of multilateralism.

In particular, **the analysis of the Romanian health system** has highlighted that the current type of management, the outdated structure, still-vitalized and poorly reshuffled, determine that the obvious, existing, serious, and dangerous problems, for which there is a precedent to be at the origin of the causality of the security breaches. The applicability of *Business* and *Competitive Intelligence* is practically non-existent in the state sector, which as much as it is budgeted, shows that for the most part the system is not sufficiently motivated for analysis and performance. Seemingly underfunded, the use of available funds is directed towards the medical act and significantly important departments (patient databases, electronic equipment, devices, high-performance equipment or medical facilities, as a whole being susceptible to cyber-attacks, which have even happened and which as shown, can cause severe disruptions or irreparable consequences for whose functionality cybersecurity would be also the key in the sustainability of *Business Intelligence*.

Is the Romanian health services system ready to confront the reality of cyber insecurity? The analysis of cybersecurity issues and the marking of the role of *Business Intelligence* in the Romanian healthcare system was done with the help of the "Swiss Cheese" model in which we included 6 specific defensive barriers. The model has demonstrated that for the public health system there are vulnerabilities in terms of cybersecurity, which by "aligning" the active errors have resulted and can still result in adverse events. However, many healthcare

organizations do not apply sustainable error management practices, supported by a *business* analysis and which, like other *intelligence* components in the health services sector, are conditioned by cybersecurity. **The investigation carried out on security and *Business Intelligence* in the opinion and practice of persons with administrative decision-making power in the Romanian health system** highlighted that although important, cyber security is not considered a priority and that *Business Intelligence* seems to be still a field foreign to the respondents. As it concerns a competitive environment, however, the upward trend of implementing high-performance risk management systems, including cybernetic ones, has emerged in the private health system and, as a result, cyber security is considered a *business* problem, which also needs a *business* solution.

Our analysis outlines that **the targets (domains) are vulnerable and decisively affected by cyber insecurity. Integration/association of international relations, governance of the business environment/critical infrastructures in achieving cyber security and sustainability in *Business Intelligence*** is real and present. None of these targets could be nominated in the security context of the XXI century as dominant or subordinate, their fluidity and interchangeable dynamics being continuous, while cybersecurity is the key and junctional element in the relationship of these three targets. Certainly, we can identify the binders between these targets and cybersecurity, these being, in our opinion, the principles of ethics (leading to transparency and openness) and the precautionary principle. Taken over by the public health in the field of environmental protection, the precautionary principle (sometimes regarded with reluctance by a part of the scientific community) implemented within limits to maintain the progress is superposable to both international relations and governance, *business* environment, and *Business Intelligence*.

Reducing the angle of cyber insecurity in the XXI century can only be based on error management and collaboration. The relationship between prevention, identification/annihilation, and mitigation/elimination of risks and threats involves the transfer of the "lesson learned" in the sense that any higher age leads to basic prevention, and the di ribution of experience is the fir ep of external collaboration. In this regard, one of the objectives is to develop cybercrime deterrence capabilities in all countries and to maintain cooperation to reduce risks.

In what direction will the cybersecurity - *Business Intelligence* relationship evolve? Clearly, in the context of accepting cyberspace as a space of power, the "defense-attack-resilience" cybersecurity paradigm will be hardly predictable. The development of society and

the need for performance will include *Business Intelligence* in the current practice, seconded by *Competitive, Market,* and *Cyber Intelligence*. The connection of cybersecurity with *Bussines Intelligence* is not one-sided, this relationship is concretely mutual, and cyber security due to its transnational character is no longer optional in any field. The analysis of vulnerabilities, risks, and cyber insecurity events is part of the general risks management in any domain and con itutes an integral part of *Business Intelligence*.

The novelty elements of the research presented in the introductory chapter of the thesis have materialized, as it results from the present conclusions formulated, in the personal contributions to a very current topic of udy, namely cyber security and the cu omization of su ainability aspects in *Business Intelligence*, which will open research directions with an innovative character in the field of cooperation between the academic environment, the private and public sector businesses. At the same time, the possibility of continuing to develop this theme, which is fundamental both for national security and for regional and international security, is all the more important because, as ated in the thesis, no entity alone can eliminate or reduce cyber insecurity.

BIBLIOGRAPHY (selective)

AMEYAW-BROBBEY, Thomas (2021): COVID-19 Vaccination: A Real Te of Sovereign Equality and Friendship. Global Policy Journal. https://www.globalpolicyjournal.com/blog/03/02/2021/covid-19-vaccination-real-te -sovereign-equality-and-friendship.

ASHRAFI, Noushin et al. (2014): The Impact of Business Intelligence on Healthcare Delivery in the USA. Interdisciplinary Journal of Information, Knowledge, and Management. Vol. 9. pp. 117-130. https://doi.org/10.28945/1993.

BURKE, Anthony *et al.* (2016): An Ethics of Global Security. Journal of Global Security Studies. Vol. 1. Issue 1. pp. 64-79. https://doi.org/10.1093/jogss/ogv004.

CENTRUL NAȚIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ - CERT-RO (2020 a): Știrile săptămânii din cybersecurity (10.12.2020). Disponibil la: https://cert.ro/cite e/ irile-saptamanii-10-12-2020. Accesat la 4 martie 2021.

CHIFU, Iulian (2009): Societal Security. An agenda for the Ea ern Europe. Corpus ID: 199402475. pp. 1-18. Disponibil la: http://www.cpc-ew.ro/pdfs/societal_security.pdf. Accesat 5 mai 2020.

CHRISTOU, George (2018): The Collective Securitisation of Cyberspace in the European Union. We European Politics. Vol. 42. Issue 2: The European Union, Security Governance and Collective Securitisation. pp. 278-301. https://doi.org/10.1080/01402382.2018.1510195.

CÎRNU, Elena Carmen (2019): Cyber Diplomacy, Strategic In rument in Foreign Affairs Policy. Romanian Cyber Security Journal. ROCYS. Spring 2019. Vol. 1. Issue 1. pp. 35-40. https://rocys.ici.ro/documents/spring2019/article_5.pdf.

CONSILIUL UNIUNII EUROPENE (2020): Combaterea dezinformării. Disponibil la: https://www.consilium.europa.eu/ro/policies/coronavirus/fighting-disinformation/. Accesat la 7 mai 2021.

CRANE, Andrew (2005): In the Company of Spies: When Competitive Intelligence Gathering Becomes Indu rial Espionage. Business Horizons. Vol. 48. pp. 233-240. https://doi.org/10.1016/j.bushor.2004.11.005.

ENISA (2020b): Prevention is the Cyber Defence for Hospitals. https://www.enisa.europa.eu/news/enisa-news/prevention-is-the-cyberdefence-for-hospitals. Accesat la 10 mar. 2020.

ENISA (2020c): Sectoral / Thematic Threat Analysis. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-cybersecurity-research. Accesat la 5 decembrie 2020.

EUROPEAN CENTRE FOR DISEASE PREVENTION AND CONTROL - ECDC (2020): Clu er of Pneumonia Cases Caused by a Novel Coronavirus, Wuhan, China. pp. 1-10.Disponibil la: https://www.ecdc.europa.eu/sites/default/files/documents/Risk%20assessment%20-%20pneumonia%20Wuhan%20China%2017%20Jan%202020.pdf.

EUROPOL (2017): Internet Organized Crime Threat Assessment (IOCTA) 2017. Disponibil la: https://www.europol.europa.eu/activities-services/main-reports/internet-organised -crime-threat-assessment-iocta-2017. Accesat la 14 aug.2018.

EUROPOL (2019): Internet Organized Crime Threat Assessment (IOCTA) 2019. Disponibil la: https://www.europol.europa.eu/activities-services/main-reports/internet-organised -crime-threat-assessment-iocta-2019 . Accesat la 12 febr.2020.

FAZAL, Tanisha M. (2020): Health Diplomacy in Pandemical Times. Cambridge University Press. International Organization. Vol. 74. Issue S1. pp. E78 - E97. https://doi.org/10.1017/S0020818320000326. Accesat la 13 aprilie 2021.

FIDLER, David (2001): The Globalization of Public Health: The Fir 100 Years of International Health Diplomacy. Bulletin of the World Health Organization. Vol. 79. Issue 9. Geneva. pp. 842-849. Print version ISSN 0042-9686. https://www.who.int/bulletin/archives/79(9)842.pdf

FIDLER, David (2020 b): Cybersecurity in the Time of COVID-19. Digital and Cyberspace Policy Program. Council on Foreign Relations. https://www.cfr.org/blog /cybersecurity-time-covid-19. Accesat la 5 decembrie 2020.

FREEMAN, Edward–Burton, Joseph (2019): Should Businesses Fight for Democracy? MIT Sloan Management Review. Disponibil la: https://sloanreview.mit.edu/article/business-in-society/.

GRILL, Paul (2020): Business Intelligence and the COVID-19 Pandemic. InfoSol Blog. Disponibil la: https://infosolblog.com/business-intelligence-and-the-covid-19-pandemic/. Accesat la 30 martie 2021.

HANSEN, Lene–Nissenbaum, Helen (2009): Digital Disa er, Cyber Security, and the Copenhagen School. International Studies Quarterly. Vol. 53. Issue 4. pp. 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x.

HARMAN, Sophie (2017): International Health Governance. Oxford Bibliographies. Disponibil la: https://www.oxfordbibliographies.com/view/document/obo-9780199743292/obo-9780199743292-0140.xml. Accesat la 2 mai 2019.

HELMREICH, Robert L. et al. (1999): The Evolution of Crew Resource Management Training in Commercial Aviation. The International Journal of Aviation Psychology. Vol. 9. pp. 19–32. http://dx.doi.org/10.1207/s15327108ijap0901_2.

JAMIL, George. (2013): Approaching Market Intelligence Concept through a Case Analysis: Continuous Knowledge for Marketing Strategic Management and its Complementarity to

Competitive Intelligence. Procedia Technology 9. pp. 463-472, http://dx.doi.org/10.1016/j.protcy.2013.12.051.

JORA, Lucian (2020): Considerations Regarding the Global Need for a "Health Diplomacy". Romanian Review of Political Sciences and International Relations. Vol. XVII. Issue 2. pp. 114–121. https://acad.ro/bdar/rapInt2021/12fil/2In StPolRelIntern_Raport.pdf. Accesat la 17 martie 2021.

KATZ, Rebecca et al. (2011): Defining Health Diplomacy: Changing Demands in the Era of Globalization. Milbank Q. Vol. 89. Issue 3. pp. 503-523. https://doi.org/10.1111/j.1468-0009.2011.00637.x.

KICKBUSCH, Ilona–Buss, Paulo (2011): Global Health Diplomacy and Peace. Infectious Disease Clinics of North America. Vol. 25. Issue 3. pp. 601-610. https://doi.org/10.1016/j.idc.2011.05.006.

LARICS.RO (2020): Donald Trump, Organizația Mondială a Sănătății și securizarea hard a Chinei. Începutul unui nou Război Rece. Disponibil la: https://larics.ro/donald-trump-organizatia-mondiala-a-sanatatii-si-securizarea-hard-a-chinei-inceputul-unui-nou-razboi-rece/. Accesat la 9 noiembrie 2020.

MA, Jianhua et al. (2016): Perspectives on Cyber Science and Technology for Cyberization and Cyber-Enabled Worlds. 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), Auckland, New Zealand. pp. 1-9, https://doi.org/10.1109/DASC-PICom-DataCom-CyberSciTec.2016.17.

MOORE, Richard (2020): Cyber Intelligence-Driven Risk: How to Build and Use Cyber Intelligence for Business Risk Decisions. ©2021 John Wiley & Sons, Inc. (P)2021 Gildan Media. ISBN: 978-1-119-67684-3. pp. 1-192. https://www.wiley.com/en-us/Cyber+Intelligence+Driven+Risk%3A+How+to+Build+and+Use+Cyber+Intelligence+for+Business+Risk+Decisions-p-9781119676843.

NATO (2021 a): Joint Press Point by NATO Secretary-General Jens Stoltenberg, US Secretary of State Antony Blinken, and US Secretary of Defense Lloyd J. Au in III. Disponibil la: https://www.nato.int/cps/en/natohq/opinions_183061.htm. Accesat la 15 mai 2021.

NATO (2021 b): NATO's Response to Hybrid Threats. Disponibil la: https://www.nato.int/cps/en/natohq/topics_156338.htm. Accesat la 7 aprilie 2021.

NUNES, João (2012): Health, Politics and Security. e-cadernos CES (online). pp. 142-164. Disponibil la: http://dx.doi.org/10.4000/eces.989.

NYE, Joseph (2010): Cyber Power. Belfer Center for Science and International Affairs, Harvard Kennedy School. pp. 1-19. Disponibil la: http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf. Accesat la 6 septembrie 2020.

REASON, James (2000): Education and Debate. Human Error: Models and Management. British Medical Journal. Vol. 320. pp. 768-770. REASON, James (2000): Education and Debate. Human Error: Models and Management. *British Medical Journal*. Vol. 320. pp. 768-770. https://dx.doi.org/10.1136%2Fbmj.320.7237.768.

SERVICIUL ROMÂN DE INFORMAȚII – SRI (2020 a): Amenințarea cibernetică în 2019. Evaluare și perspective de evoluție. Buletin Cyberint seme rul I 2020. https://www.sri.ro/assets/files/publicatii/buletin-cyber-sem-1-2020.pdf. Accesat la 5 augu 2020.

STARCEVIČ, Vladan et al. (2020): Cyberchondria in the Time of the COVID-19 Pandemic. Human Behaviour & Emerging Technologies 2020. pp. 53–61. https://doi.org/10.1002/hbe2.233.

UNITED NATIONS DEVELOPMENT PROGRAM (1994): Human Development Report 1994: New Dimensions of Human Security. pp. 1-137. Disponibil la: https://doi.org/10.18356/87e94501-en.

WEF - WORLD ECONOMIC FORUM (2020 c): The Global Risk Report 2020. Disponibil la: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf. Accesat la 5 septembrie 2020.

YAHAYA, Jamaiah et al. (2019): The Implementation of Business Intelligence and Analytics Integration for Organizational Performance Management: A Case Study in Public Sector. International Journal of Advanced Computer Science and Applications. Vol. 10. Issue 11. pp. 292-298. http://dx.doi.org/10.14569/IJACSA.2019.0101140.