”MIHAI VITEAZUL” NATIONAL INTELLIGENCE ACADEMY

INTELLIGENCE AND SECURITY DOCTORAL SCHOOL

SUMMARY OF THE DOCTORAL THESIS

DOCTORAL SUPERVISOR

Professor PhD

Ioan DEAC

PhD CANDIDATE

Research assistant

Cristian CONDRUȚ

BUCHAREST, 2025

”MIHAI VITEAZUL” NATIONAL INTELLIGENCE ACADEMY

INTELLIGENCE AND SECURITY DOCTORAL SCHOOL

SUMMARY OF THE DOCTORAL THESIS

EDUCATIONAL MODEL FOR THE TRAINING OF THE CYBERINTELLIGENCE ANALYST IN THE FIELD OF INTELLIGENCE AND NATIONAL SECURITY

DOCTORAL SUPERVISOR

Professor PhD

Ioan DEAC

PhD CANDIDATE

Research assistant

Cristian CONDRUȚ

BUCHAREST, 2025

TABLE OF CONTENTS

INTRODUCTION

The increased capacity to dissimulate and anonymize intelligence activities, the low risks of exposure of the personnel within intelligence organizations, the possibility of dynamizing the period of an intelligence activity, are just some of the important advantages of operations carried out in the cyber environment, compared to those carried out in the conventional environments of intelligence and security confrontations. The 2007 cyber attacks in Estonia, the 2008 cyber attacks in Georgia, the 2010 disabling of the uranium enrichment facilities in Iran through the use of the STUXNET worm application, the cyber attacks on the U.S. Democratic National Committee, carried out on the sidelines of the 2016 presidential elections, or the espionage and cyber sabotage activities of the Russian Federation in the context of the war of aggression launched in 2022 against Ukraine, are just a few relevant examples to illustrate the importance of cyberspace for intelligence and security organizations.

In all these examples, at least two elements stand out as the common denominator: 1) cyberspace is a confrontational environment for intelligence and security organizations, given that for all the examples presented the involvement of intelligence and security organizations was either associated or attributed; 2) certain activities performed in the cyber environment are carried out by the personnel of intelligence and security organizations. In this context, regardless of whether we refer to offensive or defensive cyber activities, the success of the missions is also dependent on the competence of the human resources involved, beyond the technical tools and other types of organizational resources. This aspect emphasizes the increasingly compelling need for a cybersecurity and intelligence and security education, in order to train the necessary competences of the cyberintelligence specialist in intelligence and national security organizations, so that they can fulfill their missions.

Although there are numerous initiatives, curricula and strategies for the education and training of cybersecurity specialists[1], the number of those that include elements related to cyberintelligence is extremely low and not adapted to the training of specialists in intelligence

[1] As shown in *Comparative Analysis of Strategic Cyber Security Focus Areas - United Kingdom, Estonia, Romania* (Condruț 2023).

and security organizations[1]. The negative impact of this element is even higher when we notice that within intelligence and security organizations, there is not just one type of specialist who simultaneously carries out activities to collect, process, and analyze intelligence. In this context, the need to train the cyberintelligence specialist in intelligence and security organizations must be tailored to the type of activity they perform. As far as we are concerned, we have tailored our research interest to the cyberintelligence analyst in the intelligence and national security field, considering that the activity performed by this type of specialist is the one that most integrates and capitalizes on the knowledge acquired at the level of an organization from this domain.

Thus, we **question** *the need to configure a model for the training of the cyberintelligence analyst in the intelligence and security field in order for them to have the necessary competences to identify, prevent and counter threats from the cyber environment*, taking into consideration the need for cybersecurity education in intelligence and national security organizations and the role and responsibility of the cyberintelligence analyst in the intelligence and national security field.

We believe that the solution to our research problem consists of developing an educational model suitable for this type of specialist and connecting both current professional practice and existing academic debates by applying *the scientific method.* Thus, the **goal** of our research will be to *configure an educational model for the training of the cyberintelligence analyst for the intelligence and national security field, which contains educational competences, learning objectives and educational content, a model achieved by applying scientific research methods.*

In order to achieve the goal of our research, we aimed to carry out scientific research activities divided into 4 successive stages. We aimed to solve **the first stage** of the doctoral research by achieving **objective 1** of the research: *identify and rank the most important defining strategic elements of cybersecurity at the national and European level, including from the perspective of the interaction between cybersecurity and national security*. In order to achieve **objective 1**, we will select a number of national cybersecurity strategies, whose content we will analyze through a mixed approach, using the MAXQDA software. We will present results

[1] See *Chapter 6*.

on the prevalence of priority strategic cybersecurity dimensions in the context of our research: *cyber threat assessment, national security,* and *cybersecurity education*.

The results obtained in **stage 1** will be useful for presenting the results obtained in **stage 2**, which involved achieving the following two scientific research objectives:

- **Objective 2 –** *Configure a set of cybersecurity and intelligence competences necessary for the cyberintelligence analyst in intelligence and national security by analyzing the interactions between intelligence and cybersecurity.*
- **Objective 3 –** *Validate and prioritize the cybersecurity and intelligence competences needed by the cyberintelligence analyst in intelligence and national security.*

In order to achieve **objective 2**, we will select a series of analytical cybersecurity reports, the content of which we will analyze through a mixed approach using the MAXQDA software. The results of the content analysis will be used to shape an extensive set of cybersecurity knowledge, skills, and abilities, reported to the *NICE Framework* (i.e., the cybersecurity occupational competency framework developed by NIST USA).

In order to achieve **objective 3**, we will present how we applied the sociological survey method by using the questionnaire technique and consulted national and international experts in intelligence, national security, cybersecurity and cyberintelligence to assess the set of competences obtained by achieving **objective 2**. We will present the results of the sociological survey by using descriptive statistical parameters, thus obtaining a validated set of competences. The priority subset of cyberintelligence analysis competences in intelligence and national security will be achieved by interpreting several descriptive statistical parameters.

The results obtained by achieving **objective 3** of **stage 2** will be useful for presenting the results obtained in **stage 3**, which involves achieving the following two scientific research objectives:

- **Objective 4 –** *Configure a model of a tool for the pedagogical assessment of the priority competences necessary for the cyberintelligence analyst in the intelligence and national security field, which could be used in an educational intervention.*
- **Objective 5 –** *Configure a model to train the priority competences necessary for the cyberintelligence analyst in the intelligence and national security field, which could be used in an educational intervention.*

In order to achieve **objective 4,** we will present how we applied the content analysis method and the questionnaire technique by consulting national and international experts in intelligence, national security, cybersecurity and cyberintelligence, so as to determine the best methods of pedagogical assessment of priority competences. Applying the content analysis method will take into account elements specific to educational sciences and to assessment theory and methodology. To be able to configure the assessment tool itself, we will develop learning objectives that correspond to the set of priority cyberintelligence analysis competences and are structured in typologies of assessment items, based both on the results of the content analysis and on the elements extracted from the assessment theory and methodology.

In order to achieve **objective 5**, we will present the way in which, starting from the learning objectives defined in an argumentative manner in the activities performed to achieve objective 4, one can develop educational content that can be implemented directly within the training processes of cyberintelligence analysis in intelligence and national security.

The results we obtained in **stages 2** and **3** will be useful for presenting the results obtained in **stage 4**, which involves achieving the following two scientific research objectives:

- **Objective 6 –** *Test the effectiveness of a cyberintelligence analysis educational intervention by measuring the priority competences needed by future specialists in this field.*
- **Objective 7 –** *Test cyber resilience as a factor of progress of the educational intervention.*

In order to achieve **objective 6** and **objective 7**, we will carry out a pedagogical experiment in a quasi-experimental design with a non-equivalent control group. The experimental sample will consist of future intelligence analysts – students of the *Security and Intelligence Studies* Bachelor's degree program within "Mihai Viteazul" National Intelligence Academy (ANIMV). The methodology of the pedagogical experiment will be presented in the paper.

Although by completing stages 1 – 4 we will achieve the goal of our research, we also aim to complete stage 5, which involves achieving **objective 8**: *carry out a comparative analysis between the set of competences needed by the cyberintelligence analyst in intelligence and national security and the existing sets of competences in university study programs that train cybersecurity experts and intelligence analysts.* We will select study programs that teach cybersecurity and intelligence analysis competences from the European Union and compare competences, learning outcomes and educational content associated with these with our validated set of cyberintelligence analysis competences in intelligence and security. Such an approach will allow us to highlight the current situation of the university's educational offer intended for the training of intelligence analysis and cybersecurity competences in comparison with the results we have obtained in **stages 1 – 4**.

CONTEXTUALIZATION AND THEORETICAL BACKGROUND OF THE CYBERINTELLIGENCE ANALYSIS

In order to achieve the **goal** of our doctoral research - *configuring an educational model for the training of the cyberintelligence analyst for the intelligence and national security field, which contains educational competences, learning objectives and educational content, a model achieved by applying scientific research methods* - we conducted a theoretical investigation of the main elements that can contribute to the empirical substantiation of educational and training approaches for cyberintelligence analysts in intelligence and security organizations. This theoretical investigation is presented in detail in Chapter 1 of the PhD thesis and involved the following activities: 1) investigating the field of cyberintelligence analysis, considering the intersection of the fields of intelligence and cybersecurity, for which we have deepened theoretical elements from security studies, intelligence studies and the field of cybersecurity; 2) the argumentation of the education and training approaches in this field, in particular with reference to occupational and competence frameworks specific to intelligence and cybersecurity and to the theories and approaches specific to educational sciences; 3) the capitalization of the experience drawn from scientific works in the field of our research topic - the education and training of cyberintelligence analysts in intelligence and security - by extracting the premises used in empirical research.

Regarding the analysis of *cyberintelligence*, as a field at the intersection of intelligence and cybersecurity, we obtained that: 1) cybersecurity is a multidisciplinary field that requires technical and non-technical approaches; 2) the securitization of the cybersecurity field is justified in the current security context and thus the national security discourse that captures elements of cybersecurity acquires greater importance from the perspective of scientific research; 3) cyberintelligence analysis in intelligence and security organizations is at the intersection of intelligence analysis and cybersecurity, and there is a need for systematization of the training of specialists in order to successfully fulfill the missions of intelligence and security organizations.

Regarding the foundations of training and assessment in cyberintelligence analysis, we noted the useful elements for the presentation of the research conducted in order to achieve objectives 2 and 3: 1) the need for scientific research on the standardization of education and training of *cyberintelligence* analyst in *intelligence* and security, 2) the occupational and competency frameworks in intelligence and cybersecurity; 3) the specific standard of the intelligence analyst occupation in the COR; 4) the NICE Framework of competencies in cybersecurity and intelligence NICE Framework. We have also clarified the concepts of knowledge, skills, abilities, competency and learning objective, which served as the basis for our methodological approaches to the research. Last but not least, we have established the theoretical elements specific to the theory and methodology of instruction and assessment, which we have used to base our research to achieve objectives 4, 5, 6, 7 and 8.

In terms of scientific research experience carried out to identify ways to educate and train the *cyberintelligence analyst* in *intelligence* and security, we have succeeded in: 1) highlighting the extensive use of the *NICE Framework* in the investigated research works, both for the configuration of cybersecurity competence sets and for comparative analysis with other occupational and competence frameworks; 2) investigating the main methodological approaches carried out in the field of our research topic, sociological survey and experiment emerging as suitable tools in these contexts; 3) reflecting the link between individual cyber resilience and learning, these being useful in the experimental stage of our research.

Chapter 1 is the one in which we contextualized and theoretically grounded the field of *cyberintelligence* analysis, managing to argue for the existence of cyberintelligence analysis as a distinct professional field within intelligence and national security organizations and for the need for education and training of specialists in this field. We also emphasized how education and training in the field can be effectively accomplished, which led our discussion toward occupational and competency frameworks, clarifications of concepts central to our research, and toward training and assessment theory and methodology. All of these elements formed the basis of our empirical research, and from this point on, our paper presented how we carried out these activities, the results obtained and the interpretations made.

CONFIGURING TRAINING AND ASSESSMENT MODELS IN CYBERINTELLIGENCE ANALYSIS IN INTELLIGENCE AND SECURITY

Chapters 2, 3 and 4 of the paper have been devoted to the configuration and presentation of the training and assessment models used in cyberintelligence analysis specific to the intelligence and security domain.

In **Chapter 2** we set out to fulfill the **objective 1** of our research - *identify and rank the most important defining strategic elements of cybersecurity at the national and European level, including from the perspective of the interaction between cybersecurity and national security* - specific to **first stage** of our research. We aimed at: 1) presenting the results and interpretations obtained as a result of a qualitative content analysis applied to four national cybersecurity strategies; 2) analyzing and explaining the main elements of the existing strategic framework at the European Union level in the field of cybersecurity and cybersecurity education.

To analyze the content of the four national cybersecurity strategies, we used the content analysis method, developing defining strategic categories and dimensions, and used the MAXQDA2022 software application. The applied research methodology led us to the following major findings:

- States attach increasing importance to the areas of *governance* and *preparedness and resilience*, considering, on the one hand, the need for state institutions to assume the role of national coordinator in the field and, on the other hand, the need to ensure a good response capability to major cybersecurity incidents. We also found the areas of national *risk management*, *legislation and regulation*, and *capacity, capability and awareness* to be important for states, given that they have a direct impact on the whole society, including when referring to the involvement of relevant societal actors, and that they represent the most important basis for *governance* and *preparedness and resilience*. In terms of our priority strategic dimensions - *cyber threat assessment*, *national security* and *cybersecurity education* - we were able to show that their ranking is extremely high in national cybersecurity strategies. All the countries analyzed base their strategic arguments and objectives on cybersecurity threat assessments while emphasizing the impact on national security.

- Cybersecurity education is being addressed in all the countries analyzed through measures aimed at strengthening efforts in this area, such as the development of cybersecurity curriculum frameworks, occupational and competency frameworks or the development of cybersecurity curricula. We have identified strategic planning as the most important strategic dimension within the area of *capability, capacity and awareness*, which includes cybersecurity education. This affirms States' commitment to developing cybersecurity education and training initiatives.

In the context of the explanatory analysis of the main elements of the existing EU policy framework for cybersecurity and cybersecurity education, we obtained the following results:

- Cyber security at EU level is addressed in relation to all existing societal domains. However, given our research interest, we have chosen to prioritize the security and defense domain, where the role of cyberintelligence is very well articulated and is important in all phases of CSDP operations and missions. *Strategic Compass* also mentions the need to develop intelligence analysis and cyberintelligence capabilities, which also supports the synergy between the two. It is important to note that a large part of the results obtained in the content analysis phase of the national cybersecurity strategies were reflected in the CSDP documents, which proves a good strategic convergence between the state actors analyzed (i.e. U.S.A., UK, Spain and Romania) and the EU.
- The EU has a strong strategic support for cybersecurity education and a multitude of institutional actors involved in such endeavors, such as ENISA, EDA, ECCC and ESDC. Beyond the objective of bridging the gap between the existing needs in the labor market and the supply of cybersecurity skills training, we have noted the synergy between ENISA and ESDC in creating cybersecurity courses tailored to the ECSF. This demonstrates the ability to integrate cyber security into security and defense specific training approaches. We also note the high level of ambition of the *Cyber Skills Academy* by integrating the institutional capacities of ECCC, ENISA and ESDC. We also note the affirmation of the need to link the ECSF with the ESCO, which could generate important opportunities for the creation of university curricula at Member State level. However, we also note a lack of EU strategic level concern for

cyberintelligence analysis in *intelligence* and security, which leads to the need for awareness of this need.

The results that we obtained as a result of analyzing the content of the national cybersecurity strategies are the argument and support for the next stage of the research - analyzing the content of the analytical cybersecurity reports. Thus, we argued the choice of analytical cybersecurity reports for the realization of the next stage of the research, capitalizing on the following elements presented in **Chapter 2**: 1) quantitative results relevant to the strategic dimensions of *threat assessment* and *national security*; 2) qualitative assessments of the analyzed cybersecurity strategies, where the strategic cybersecurity discourse includes analytical cybersecurity sections. Also, the analysis of the way that cybersecurity education is reflected at national and European level shows that our orientation towards the instrument of occupational and competency frameworks is correct, this being an important topic on the strategic agenda, and that the synergy between cybersecurity and intelligence is supported at the strategic level, especially in relation to the EU's security and defense policy.

In **Chapter 3,** we capitalized on the results obtained and interpreted in **Chapter 2**, fulfilling the following scientific research objectives, specific to **second stage** of our research:

- **Objective 2** – *Configure a set of cybersecurity and intelligence competences necessary for the cyberintelligence analyst in intelligence and national security by analyzing the interactions between intelligence and cybersecurity.*
- **Objective 3** – *Validate and prioritize the cybersecurity and intelligence competences needed by the cyberintelligence analyst in intelligence and national security.*

To achieve research objectives 2 and 3 we applied the following elements of scientific research methodology: 1) for objective 2 we used the qualitative content analysis method for the analysis of analytical reports on cybersecurity and a tailor made procedure for exploiting the results of this analysis and the *NICE Framework*; 2) for objective 3 we used the sociological survey method by involving 44 experts from organizations working in the fields of cybersecurity, intelligence, national security and cyberintelligence. The main results we obtained led to the fulfillment of the two research objectives related to cyberintelligence analysis competence sets in intelligence and national security, as follows:

- Related to Objective 2 - We configured the initial set of cyberintelligence analysis competences in intelligence and security by conducting a content analysis of cybersecurity analytic reports, which revealed that these information products represent a combination of factual and methodological elements specific to both intelligence and cybersecurity analysis. Although the obtained result may be considered trivial, its value lies, on the one hand, in its assumption through a scientific research approach, non-existent in the literature, and, on the other hand, in its use as an intermediate element in a phased doctoral research design. We used this result to extract the keywords needed to effectively configure our initial competence set, making use of the existing knowledge, skills and abilities of the *NICE Framework*. We also ensured the appropriateness of our set of competencies in relation to others existing in the *NICE Framework* and in the literature and thus completed our research approach specific to objective 2.

- Related to Objective 3 - By applying the sociological survey method, we succeeded in validating 91.5% of the competences existing in the initial set, realized as a result of the achievement of objective 2. The result is remarkable, considering that the validation resulted from the consultation of 44 experts in cybersecurity, intelligence, national security, and cyberintelligence at the national and international levels. We also consider the result obtained by classifying the validated competences into the typologies presented by Borum and Sanders as extremely important, as it clearly defines the orientation of our set towards the connection between analytical and technical competences, facilitated by contextual, organizational and communication competences. Out of the validated competencies, 8 emerged as priorities for the cyberintelligence analyst in intelligence and security. This result substantiates the approaches to fulfill our research objectives 4, 5, 6 and 7.

In **Chapter 4,** we capitalized on the results obtained and interpreted in **Chapter 3**, leading to the fulfillment of the following scientific research objectives, specific to the **third stage** of our research:

- **Objective 4 –** *Configure a model of a tool for the pedagogical assessment of the priority competences necessary for the cyberintelligence analyst in the intelligence and national security field, which could be used in an educational intervention.*
- **Objective 5 –** *Configure a model to train the priority competences necessary for the cyberintelligence analyst in the intelligence and national security field, which could be used in an educational intervention.*

In order to achieve objective 4 and 5 we applied the following research methodology: 1) content analysis of the answers collected by applying the questionnaire technique to 18 experts working in organizations in the field of cybersecurity, intelligence, national security and cyberintelligence, contributing to the achievement of objective 4; 2) the procedure of configuring the models of tools for assessment and training of priority skills of cyberintelligence analysis in intelligence and security, which allows the achievement of the two research objectives. By corroborating all the results obtained as a result of conducting the content analysis, we obtained that our assessment instrument should be administered in **written form** and predominantly **test practical aspects of cyberintelligence analysis in intelligence and security** and **use written test and writing analytical materials as assessment methods**. As a result of the content analysis, we have obtained a generic version of a pedagogical assessment tool, which: 1) builds on the results of our content analysis; 2) creates the framework for testing all the priority competences of cyberintelligence analysis; 3) ensures the possibility of application in real educational approaches, given the possibility of standardization and low resource consumption. Based on the results of the content analysis, the model of the pedagogical assessment tool was configured in the form of a written test with items valuable for cyberintelligence analytic practice, while also respecting the requirements of assessment theory and methodology. We configured learning objectives, justified the choice of assessment item types, including drawing on the opinions of experts in cyberintelligence, cybersecurity, national security and intelligence, generated items and ways of scoring them, and verified the compliance of our tool with the quality criteria for assessment tests. We emphasize the importance of configuring the learning objectives starting from the prioritized cyberintelligence analysis competencies in intelligence and security and respecting the elements of the cognitive process dimension of *Bloom's Taxonomy*. These objectives represent the most important outcome of Chapter 4 as they have proven their usefulness also in the process of configuring the pedagogical training model of cyberintelligence priority analysis skills. It is important to note that this model respects the elements captured in the training theory and methodology and that it was created with reference to theoretical and practical elements specific to the fields of cybersecurity, intelligence, and security. It is also relevant in the context that both models have been created for use in real pedagogical formative and evaluative contexts, a point that we have elaborated in Chapter 5.

VERIFYING THE EFFECTIVENESS OF THE PEDAGOGICAL MODEL OF CYBERINTELLIGENCE ANALYSIS IN INTELLIGENCE AND SECURITY

In **Chapter 5**, we experimentally verified the results presented in **Chapter 3** (i.e. priority cyberintelligence analysis competences) and in **Chapter 4** (i.e. assessment tool model and pedagogical training model of priority cyberintelligence analysis competences), fulfilling the **fourth stage** of our research, which involved achieving the following two scientific research objectives:

- **Objective 6 –** *Test the effectiveness of a cyberintelligence analysis educational intervention by measuring the priority competences needed by future specialists in this field.*
- **Objective 7 –** *Test cyber resilience as a factor of progress of the educational intervention.*

To meet these objectives, we conducted a pedagogical experiment in a quasi-experimental design with a non-equivalent control group, involving students in the undergraduate program *Security and Intelligence Studies* at ANIMV. To fulfill the research objectives, we set out to test the following hypotheses:

- **Hypothesis 1** (Hyp1) – *A cyberintelligence educational intervention applied to future intelligence and national security analysts will lead to higher assessment scores when jointly assessed with other future intelligence and security analysts who have not received the same educational intervention.*
- **Hypothesis 2** (Hyp2) – *An exposure to an adverse cyber event during the cyberintelligence educational intervention applied to future intelligence and national security analysts will lead to higher assessment scores when assessed jointly with other future intelligence and security analysts who have been given the same educational intervention but have not been exposed to the adverse cyber event.*

- **Hypothesis 3** (Hyp3) – *A cyberintelligence educational intervention applied to future intelligence and national security analysts will result in higher scores on the assessment administered 6 months after the intervention than on the assessment administered before the intervention.*

Based on the three hypotheses of our research, which involved the application of educational interventions, we distinguished the following needs: 1) the need for an educational intervention that does not involve the simulation of an adverse cybersecurity event; 2) the need for an educational intervention that involves the simulation of an adverse cybersecurity event. Thus, we defined three experimental groups: 1) a control experimental group, which receives no intervention; 2) an experimental group that receives an educational intervention without an adverse cybersecurity event; 3) an experimental group that receives an educational intervention with an adverse cybersecurity event. Thus, we considered as the only independent variable (IV) the group, *IV-group*, with the following three levels: 1) for the group allocated to the educational intervention without an adverse cybersecurity event, the level labeled *intervention*; 2) for the group allocated to the educational intervention with an adverse cybersecurity event, the level labeled *event*; 3) for the control group, the level labeled *control*. In addition, the verification of *Hyp1* and *Hyp2*, in comparison with the verification of *Hyp3*, involved the configuration of different variables:

- For the testing of *Hyp1* and *Hyp2*, we considered it appropriate to apply the model pedagogical assessment tool *(i.e.,* result of scientific research objective 4), both before and immediately after the educational interventions. We thus utilized a design in which we obtained paired values for each participant in our study, both before the proposed educational interventions (*i.e.,* to be referred as ***pre-test score***) and after them (*i.e.**,** **post-test score***). Given the mathematical arguments for using the ANCOVA inferential statistical method, we considered the post-test score as our dependent variable (DV) and the pre-test score as our covariate variable (i.e., CoV – has effect on DV). In addition to ANCOVA, we also used the Holm-Bonferroni post-hoc test for *Hyp1* and *Hyp2*.
- For the testing of Hyp3, we did not intend to modify our experimental design, but to extend it with a further stage, which involved retesting participants approximately 6 months after the completion of the educational intervention, again using the model pedagogical assessment tool obtained by fulfilling objective 4 in Chapter 4. We thus checked whether the participants in the educational intervention (*i.e.,* set up by the fulfillment of objective 5 in Chapter 5) had formed cyberintelligence analysis competences in intelligence and security that

can be proven in the medium and long term, not just in the short term. The score obtained on the retest (i.e., which we have labeled the ***retest score***) represents one of the levels of the dependent variable *DV-score,* along with the pre-test score and the post-test score. Therefore, the moments of test administration, corresponding to the pre-test, post-test, and retest scores, will be considered as levels of an independent and nominal variable (*IV-time*): 1) *pre-test*; 2) *post-test*; 3) *retest*. For testing *Hyp3,* we used mixed-factor ANOVA, Holm-Bonferroni post-hoc test, and simplified effects.

For the verification of *Hyp1 and Hyp2*, we analyzed data collected as a result of the participation of 34 students enrolled in the first year of undergraduate studies in *Security and Intelligence Studies* at ANIMV. By applying ANCOVA and *Holm-Bonferroni* tests, we obtained statistical significance for the comparisons between: 1) *control* and *intervention* group, obtaining that the *intervention group* had on average a result of 14.288 points higher than the *control group* on the result obtained in the *post-intervention test* (i.e., *post-test score*); 2) *control* and *event* group, obtaining that the *event group* had on average a result of 20,328 points higher than the *control group* on the result obtained in the post-intervention test (i.e., *post-test score*). These results led us to validate Hyp1. We were also unable to obtain statistical significance for the difference in the means of the post-test scores for the *intervention-event* pair, which led to the invalidation of *Hyp2*. The statistical test applied to verify *Hyp1 and Hyp2* has a statistical power of 0.98. Regarding the verification of *Hyp3*, we obtained statistical significance for the differences between the *pre-test* and *post-test* values for the groups: 1) *event*, this group obtaining mean scores 12 points higher at 6 months after the closure of the intervention, compared to the pre-intervention testing time; 2) *intervention*, this group obtaining mean scores 14 53 8 points at 6 months after the closure of the intervention compared to the time of pre-intervention testing. Thus, we also validated *Hyp3*, with a statistical power of 0.88. In the last part of *Chapter 5*, we made interpretations on the results obtained, which aimed at: 1) arguing the importance of the results, in relation to the occupational standard of the information analyst in Romania; 2) highlighting the validity and efficiency of our pedagogical model; 3) ways in which our experimental design could be improved, given the decision to invalidate Hyp3.

At the end of *Chapter 5*, we have reached the aim of our research to configure an educational model of cyberintelligence analyst training for the field of intelligence and national security, which contains educational competences, learning objectives, *and educational contents, a model realized by applying scientific research methods*. We also believe that we have provided a solution to our research problem – the need to model the training of the cyberintelligence analyst in the field of intelligence and security in order to have the necessary competencies to know, prevent, *and counter threats from the cyber environment*.

CHECKING THE OPTIMALITY OF EUROPEAN STUDY PROGRAMS FOR THE TRAINING OF CYBERINTELLIGENCE ANALYSTS IN INTELLIGENCE AND SECURITY

In **Chapter 6**, we conducted a comparative analysis between the competences sets required for the cyberintelligence analyst in intelligence and national security, as determined in our research, and the existing competences sets in study programs that train cybersecurity experts and intelligence analysts in national and European degree programs (i.e., research objective 8). In this way, we compared the existing curricula in our field of interest with our own educational model, developed and verified through scientific research at the borderline between intelligence and security, education sciences, and cybersecurity. Also, by achieving **objective 8,** we have pointed out synergies between cyberintelligence analysis education at the level of the European Union Member States and the level of CSDP.

In the first part of Chapter 6, we defined a five-step benchmarking procedure, through which we have managed to: 1) configure a database of official sources that contains all existing university degree programs at the level of the European Union, covering 25 of the 27 Member States; 2) perform searches in all national databases identified by terms derived from our fields of interest - *cyberintelligence analysis*, *intelligence analysis* and *cyber security*, after which we selected 10 degree programs at the level of the European Union; 3) perform searches on the website of the selected university, faculty, department or study program to identify the taught competences; 4) compare our validated set of cyberintelligence analysis competences in intelligence and security and the contents identified as suitable for benchmarking; 5) integrate the obtained results to determine whether our educational model optimizes the training processes in cyberintelligence analysis by comparison with those carried out in the selected study programs.

By applying this procedure, we obtained that if there were to be a study program in cyberintelligence analysis in intelligence and security, integrating the elements of our educational model, it should: 1) propose the formation of competences starting from the existing ones and complementing them with those specific to our educational model, the least effort in this regard would be the program organized by the University of Nebrija[1]; 2) start from the competences of the existing programs, integrating those sets for which the highest scores were obtained according to the 5 typologies. Thus, we consider that our educational model: 1) can be integrated into degree programs that train competencies in *cyberintelligence analysis*, *cyberintelligence*, *intelligence analysis* or *cybersecurity*; 2) can be a basis for the creation of a distinct degree program, by leveraging the validated competencies, developing learning objectives and grouping them thematically into study disciplines.

In the context of all the results and interpretations formulated in Chapter 6, we conclude that the analyzed curricula optimize in different proportions, but not more than 70%, the educational processes of cyberintelligence analysis in intelligence and security of the model developed in our research. We believe that through the research approach presented in Chapter 6, we have succeeded in highlighting the current state of cyberintelligence analysis training at the European level and have formulated recommendations whose implementation could benefit both Member States and EU institutions.

[1] The program obtained a similarity percentage of 70.04%, obtaining the first position in the descending list of the study programs with which we made the comparative analysis, found in Chapter 6 of the PhD thesis.

CONCLUSIONS

Starting from the premise of the importance of the education of the cyberintelligence analyst in intelligence and security organizations, we managed to achieve **the goal of the doctoral research** – *configure an educational model for the training of the cyberintelligence analyst for the intelligence and national security field, which contains educational competences, learning objectives and educational content, a model achieved by applying scientific research methods.* We also managed to verify the results we obtained by achieving **objective 8 of the doctoral research** – *carry out a comparative analysis between the set of competences needed by the cyberintelligence analyst in intelligence and national security and the existing sets of competences in university study programs that train cybersecurity experts and intelligence analysts*.

We started our doctoral research approach from the need to contextualize and provide a theoretical foundation for cyberintelligence analysis in intelligence and security. We have highlighted during the research that: 1) the securitization of the cybersecurity field from the perspective of security studies is justified, given that we have emphasized recent scenarios where cyber threats manifest themselves as existential threats to states; 2) the strategic cybersecurity discourse is included in the national security discourse, as it is linked to several national security issues; 3) cyberintelligence analysis is at the border between intelligence analysis and cybersecurity; 4) there is an important need to standardize educational approaches in cyberintelligence analysis; 5) the *NICE Framework* is the most suitable occupational and competency framework to configure educational models of cyberintelligence analysis in intelligence and national security; 6) the configuration of a training and assessment model in cyberintelligence analysis depends on the application of the theory and methodology of training and assessment; 7) the applied scientific research in the fields of cybersecurity and intelligence analysis education presents results from applying the right scientific research methods, including in the context of our doctoral research. All these elements represented premises and landmarks for our research activity and allowed us to complete all five stages laid out in the *Introduction.*

Through applied research activities that led to achieving **the research goal,** we have obtained a series of important results that provide the foundation for our educational model of cyberintelligence analysis in intelligence and security. In the **first stage** of our research, we showed how cybersecurity is reflected at a strategic level, both through the content analysis of several national cybersecurity strategies and by an explanatory analysis of the strategic elements of security, defense, and cybersecurity at the level of the European Union. The most important result we obtained is that of the prevalence of the strategic dimensions of *cyber threat assessment, national security* and *cybersecurity education* within the analyzed national cybersecurity strategies. We relied on this result in our choice of cybersecurity analytical reports as support for the steps to configure cyberintelligence analytical competences in intelligence and national security.

In **the second stage** of our research we have configured, validated and prioritized a set of cyberintelligence analysis competences in intelligence and security. The configuration was achieved through the content analysis of several cybersecurity analytical reports, where we highlighted the most important cyberintelligence topics they addressed. We obtained that *intelligence analysis* and the *techniques, tactics, and procedures of hostile cyber actors are the most important cyberintelligence topics in these reports, and that they also empirically reflect the dual and complementary nature of cyberintelligence analysis, which is at the intersection of intelligence and cybersecurity*. Leveraging these results and the completeness of the *NICE Framework* for the field of intelligence and cybersecurity, we were able to set up an initial set of cyberintelligence analysis competences. Considering that up to this point our method has integrated only secondary data sources, we conducted a sociological survey where we consulted experts in cyberintelligence analysis, cybersecurity, intelligence and national security on the importance of the competences included in the set we configured for the cyberintelligence analyst in intelligence and security. This is how we validated 91.5% of the competences included in the initial set and obtained the first relevant product for the educational practice in the field – the validated set of competences for cyberintelligence analysis in intelligence and security. Then, we leveraged these results by establishing thresholds based on descriptive statistical parameters and we managed to extract those priority skills for the cyberintelligence analyst in intelligence and security. Both the validated and the priority set were directed in terms of the content of the competences more towards the intelligence analysis field than the cybersecurity one when we analyzed them according to the 5 typologies of competences defined by Borum and Sanders.

In the **third stage** of our research, we capitalized on the priority set of cyberintelligence analysis competences in order to configure an educational model that includes both a pedagogical assessment tool and a training tool for cyberintelligence analysis competences in intelligence and security. We have thus done a new sociological survey by involving experts in cyberintelligence, intelligence and cybersecurity analysis in order to identify the best pedagogical assessment methods for each priority competence. Using these results and applying elements from the theory and methodology of pedagogical assessment, we obtained that a tool aimed to assess cyberintelligence analysis skills in intelligence and security must be configured in the form of a written test, but should contain items relevant to the practice in the field – the most important of which is writing a cyberintelligence analysis report. As we continued to capitalize on the elements specific to the theory and methodology of pedagogical assessment, especially those related to Bloom's Taxonomy, we managed to configure learning objectives, make an argumented choice of types of assessment items and configure the assessment items themselves; all these elements constitute our model of a tool to assess the priority competences of cyberintelligence analysis. We also verified compliance with the quality criteria for our assessment tool model, and the most important result we obtained was fidelity (i.e., value of *0.937300744*), thus proving that our tool produces similar results for successive applications on similar samples of students. Capitalizing on the learning objectives, the elements we extracted from the theory and methodology of training and the practical and theoretical elements specific to the fields of intelligence and cybersecurity, we have also configured a model of pedagogical training for the priority competences for cyberintelligence analysis in intelligence and security. This proved to be another extremely important result in the context of our research, as it represented a ready-to-implement solution both in the educational practice of the field of cyberintelligence analysis and in that of scientific research.

In the **fourth stage** of our research, we aimed to experimentally verify the educational model we configured based on the set of priority competences for cyberintelligence analysis in intelligence and security. We thus carried out a pedagogical quasi-experiment where we involved students from the *Security Studies and Intelligence* program within ANIMV. We aimed to validate several research hypotheses regarding testing the effectiveness of the educational cyberintelligence analysis model, both immediately after the completion of the educational interventions and 6 months afterwards. Although we did not succeed in the *Hyp2* validation, where we tested the effectiveness of an educational intervention that included the simulation of an adverse cybersecurity event, we succeeded in the *Hyp1* and *Hyp3* validations, which prove the effectiveness of the educational model configured in the third stage of our research. Thus, the experimental groups that benefited from the intervention obtained statistically significantly better results on average than the group that did not benefit from the intervention, and 6 months after the intervention was completed, the groups that benefited from the intervention maintained the performance they obtained immediately after the intervention, which was significantly better than that before the intervention. We consider that we have configured an educational model that trains cyberintelligence analysis competences in intelligence and security that can be used to train competences that generate behaviors of educated subjects, both in the short and medium term.

We consider that our doctoral research brings multiple benefits to educational practice in the field of cyber intelligence analysis in intelligence and security, with beneficial effects for professional practice in this field and implicitly for the missions of intelligence and security organizations. The set of validated competences, the set of priority competences and the educational model consisting of learning objectives, the pedagogical assessment tool and the training model, represent elements with immediate and direct applicability in the educational practice of cyberintelligence analysis or even in the one specific to the field of information and national security. Considering that all these results were obtained including through their validation by experts with professional activity in this field, we consider our research meets the need of practitioners in the field of cyberintelligence analysis in intelligence and security and proposes a practical implementation method specific to the academic environment, thus reducing the gap between the two environments. Such an approach could contribute to better training of future cyberintelligence analysts in intelligence and security organizations so they could have the necessary competence to successfully fulfill organizational missions at the intersection of intelligence analysis and cybersecurity. We also consider that our research contributes to the body of scientific knowledge specific to the information and national security field, both through the specificity of the topic and through the use of a complex methodological apparatus, specific to other fields of scientific research, such as sociology or educational sciences.

Nonetheless, the most important conclusion regarding the practical relevance for the field of cyberintelligence analysis in intelligence and security, especially in terms of educational practice in the field, was drawn in the **fifth stage**, where we achieved objective 8 and the purpose of our doctoral research. We have done a comparative analysis of the competences, learning outcomes or specific content of 10 study programs from the European Union that train intelligence analysis and cybersecurity competences, with our validated set of cyberintelligence analysis competences. We obtained that none of the study programs we analyzed fully optimize the training of the cyberintelligence analyst in intelligence and security, compared to our educational model of cyberintelligence analysis. The result reinforces the relevance of our research for the practice in the field of cyberintelligence analysis and emphasizes the existence of a gap between the training needs of professional communities and the existing study programs that train intelligence analysis and cybersecurity competences both at the European Union and at the national level.

Moreover, understanding that cyberintelligence is part of all stages of operations and missions carried out in the context of the *Common Security and Defence Policy* (CSDP), we consider the role of educational formats for cyberintelligence analysis in intelligence and security all the more important. Although the European Union has defined elements of the strategic framework in the cybersecurity education field, has implemented cybersecurity training programs operationalized by the *European Security and Defence College* (ESDC), has established the *Cyber Skills Academy,* and the *Strategic Compass* provides for the synergy between intelligence and cyberintelligence analysis, the training of cyberintelligence analysis competences was not taken into account in any of these approaches. We therefore consider it necessary and appropriate to have measures that can strengthen the training of competences in the field, both for the member states and for the institutions, bodies and agencies of the European Union. For the member states where we have not identified such programs, we recommend these are created according to the needs of the professional communities. For the member states where we have identified study programs, we consider it appropriate to create new study programs that address various academic coordinates (i.e., according to the Spanish model, presented in Chapter 6) or to reconceptualize the existing ones by strengthening the types of deficient cyberintelligence competences or by collaborating within national or international university consortia to create new programs. For the EU institutions with responsibilities in cybersecurity education, in the configuration of occupational and competences frameworks and in the financing of international university study programs, we recommend: 1) updating the *European Cybersecurity Skills Framework* (ECSF) so that it also includes the occupational profile of the cyberintelligence analyst in intelligence and security; 2) the integration of the training needs in the field of cyberintelligence analysis in intelligence and security by the *European Security and Defence College* (ESDC), through consultation with the *European Union Intelligence and Situation Centre* (EU INTCEN), and the piloting of a training format aimed at professionals in the field who work both within the European Union (EU) institutions, as well as within public institutions with responsibilities in intelligence and security from member states; 3) updating the *European Skills, Competences, Qualifications and Occupations* (ESCO) so that there is a better representation of occupations specific to the field of intelligence and security in general, and to cyberintelligence analysis in particular; 4) having an open call for projects with non-reimbursable European funding for a master's degree program in the field of cyberintelligence analysis in intelligence and security carried out in a consortium with European representation.

Although these recommendations represent only our vision, since we have not obtained feedback from the competent bodies, we consider that they represent a first step, important for strengthening the occupational and competence profile of the cyberintelligence analyst in intelligence and security, and necessary in the current context of national, European and international security transformations and developments.

BIBLIOGRAPHY

Aaltola, Kirsi, Harri Ruoslahti, and Jarmo Heinonen. "Desired cybersecurity skills and skills acquisition methods in the organizations." *21st European Conference on Cyber Warfare and Security.* 2022. 1 - 9.

Agenția pentru Asigurarea Calității în Învățământul Supeiror din Letonia. *About us.* fără an. https://www.aika.lv/aika/par-mums/ (accesat ianuarie 5, 2025).

Alainati, Shaikhah, Sarmad AlShawi, and Wafi Al-Karaghouli. "THE EFFECT OF EDUCATION AND TRAINING ON COMPETENCY." *European and Mediterranean Conference on Information Systems 2010.* Abu Dhabi: EMCIS2010, 2010. 1 - 9.

Alammari, Abdullah, Osama Sohaib, and Sayed Younes. "Developing and evaluating cybersecurity competencies for students in computing programs." *PeerJ Computer Science,* 2022: 1 - 24.

AlDaajeh, Saleh, Heba Saleous, Saed Alrabaee, Ezedin Barka, Frank Breitinger, and Kim-Kwang Raymond Choo. "The Role of National Cybersecurity Strategies on the Improvement of Cybersecurity Education." *Computers & Security,* 2022: 1 - 22.

Alsmadi, Izzat. *The NICE Cyber Security Framework.* San Antonio, Texas: Springer, 2023.

—. *The NICE Cyber Security Framework. Cyber Security Intelligence and Analytics.* Cham: Springer, 2019.

Alsmadi, Izzat, Robert Burdwell, Ahmed Aleroud, Abdallah Wahbeh, Mahmoud Ali Al-Qudah, and Ahmad Al-Omari. *Practical Information Security. A Competency-Based Education Course.* Cham: Springer, 2018.

Alwan, Hala Bou. "National Cyber Governance Awareness Policy and Framework." *International Journal of Legal Information,* 2019: 70 - 89.

ANC. "Registrul Național al Calificărilor din Învățământul Superior – RNCIS." *ANC.* 2022. https://intern.anc.edu.ro/virtualanc/crud/rncis/rncis_programe/brain/upload/1669627620.pdf (accessed January 5, 2025).

—. "RNCIS." *ANC.* n.d. https://intern.anc.edu.ro/virtualanc/crud/rncis/rncis_programe/brain/upload/1678875117.pdf (accessed January 7, 2025).

Anderson, Lorin, and David Krathwohl. *A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives: complete edition.* New York: Addison Wesley Longman, Inc., 2001.

ANIMV. *Licență.* 2023. https://www.animv.ro/licenta/ (accessed May 23, 2024).

—. „Managementul Calității." *ANIMV.* 2023. https://www.animv.ro/wp-content/uploads/2023/10/manag_calit-2023-Ghidul-studentului-anul-universitar-2023-2024.pdf (accesat ianuarie 3, 2025).

—. *Master profesional.* 2023. https://www.animv.ro/master-profesional/ (accessed May 23, 2024).

Arqus. *Master's Programme in International Cybersecurity and Cyberintelligence.* n.d. https://arqus-alliance.eu/study-in-arqus/joint-masters-programmes/master-in-cybersecurity-cyberintelligence/ (accessed January 5, 2025).

—. *Professional opportunities.* n.d. https://arqus-alliance.eu/study-in-arqus/joint-masters-programmes/master-in-cybersecurity-cyberintelligence/cybersecurity-professional-opportunities/ (accessed January 7, 2025).

ASD. "ASD Cyber Skills Framework." *ASD.* 2020. https://www.asd.gov.au/sites/default/files/2022-10/ASD-Cyber-Skills-Framework-v2.pdf (accessed November 24, 2024).

—. *Cyber Skills Framework.* 2020. https://www.asd.gov.au/careers/how-apply/cyber-skills-framework (accessed November 28, 2024).

Atherton, J.S. "Learning and Teaching; Assessment." In *How do I Create Tests for my Students?*, by Mekiva Callahan and Micah Meixner, 3-4. Lubbock: Texas Tech University, 2020.

Australian Cyber Security Centre. *Annual Cyber Threat Report (July 2021 - June 2022).* Raport analitic de securitate ciberentică, Australian Government, 2023.

Aviv, Shahar Sean. *An Examination of User Detection of Business Email Compromise Amongst Corporate Proffesionals.* Florida: Nova Southeastern University, 2019.

Bendler, Daniel, and Michael Felderer. "Competency Models for Information Security and Cybersecurity Professionals: Analysis of Existing Work and a New Model." *ACM Transactions on Computing Education,* 2023: 1 - 33.

Blažič, Borka Jerman. "Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?" *Education and Information Technologies,* 2022: 3011 - 3036.

Bloom's Taxonomy. *Bloom's Taxonomy.* n.d. https://bloomstaxonomy.net/#:~:text=Bloom's%20Taxonomy%20is%20a%20hierarchical,the%20end%20of%20the%20course. (accessed December 11, 2023).

Boja, Alina. *Teoria și Metodologia Instruirii. Suport de curs.* Cluj-Napoca: UTPRESS, 2023.

Bonfanti, Matteo. "Cyber Intelligence: In Pursuit of a Better Understanding." *Cyber, Intelligence, and Security*, 2018: 105-121.

Borrell, Josep. "Foreword." In *HANDBOOK ON CSDP THE COMMON SECURITY AND DEFENCE POLICY OF THE EUROPEAN UNION*, by Jochen Rehrl, 10. Viena: Directorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria, 2021.

Borum, Randy, and Ron Sanders. "Preparing America's Cyber Intelligence Workforce." *IEEE Security & Privacy* 18, no. 5 (2020): 67 - 73.

Bostan-Pop, Mihaela Anamaria, and Ghiță Bârsan. "AN EDUCATIONAL APPROACH TO THE NATIONAL SECURITY ISSUES IN A DIGITAL SOCIETY." *The 16th International Scientific Conference eLearning and Software for Education.* București: Univesritatea Națională de Apărare „Carol I", 2020. 182 - 189.

Brantly, Aaron. „Cyber intelligence: method or target?" În *Research Handbook on Cyberwarfare*, de Tim Stevens și Joe Devanny, 98 - 114. Cheltenham: Edward Elgar Publishing Limited, 2024.

Brantly, Aaron. "Defining the role of intelligence in cyber: a hybrid push and pull." In *Understanding the Intelligence Cycle*, by Mark Phythian, 90-112. Oxon: Routledge, 2013.

Bruce, James, and Roger George. "Professionalizing Intelligence Analysis." *Journal of Strategic Security* 8, no. 3 (2015): 1 - 23.

Bryman, Alan. *Social Resarch Methods.* New York: Oxford University Press Inc., 2012.

Burgoyne, J. "Competency Based Approaches to Management Development." In *Bologna Handbook, Introducing Bologna Objectives and Tools*, by Declan Kennedy, Aine Hyland and Norma Ryan, 1-18. Cork, 2009.

Burt-Miller, Joseph James. *EXPLORING CYBERSECURITY EXPERT RECOMMENDATIONS TO FORTIFY U.S. NATIONAL SECURITY: A GENERIC QUALITATIVE INQUIRY.* Oklahoma: Capella University, 2021.

Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security: A new framework for analysis.* London: Lynne Rienner Publishers, 1998.

Callahan, Mekiva, and Micah Meixner. "How do I Create Tests for my Students?" *Texas Tech University.* 2020. https://www.depts.ttu.edu/tlpdc/Resources/Teaching_resources/TLPDC_teaching_resources/Documents/HowdoICreateaTestforMyStudentswhitepaper.pdf (accessed December 11, 2023).

Campbell, Donald T., and Julian C. Stanley. *Experimental and Quasi-Experimental Designs for Research.* Boston: Houghton Mifflin Company, 1963.

Campus France. *Campus France's missions.* fără an. https://www.campusfrance.org/en/Campus-France-missions (accesat ianuarie 5, 2025).

—. *The Campus France organisation.* 31 ianuarie 2024. https://www.campusfrance.org/en/organisation-conseils-organigramme (accesat ianuarie 5, 2025).

Carley, Kathleen. "Social cybersecurity: an emerging science." *Computational and Mathematical Organization Theory*, 2020: 365 - 381.

Carley, Kathleen, Guido Cervone, Nitin Agarwal, and Huan Liu. "Social Cyber-security." *11th International Conference, SBP-BRiMS 2018.* Washington: Springer, 2018. 389-394.

Carroll, Jami. "Offensive and Defensive Cyberspace Operations Training: Are we There Yet?" *European Conference on Cyber Warfare and Security.* Reading, 2018. 77 - 86.

Catal, Cagatay, Alper Ozcan, Emrah Conmez, and Ahmet Kasif. "Analysis of cyber security knowledge gaps based on cyber security body of knowledge." *Education and Information Technologies*, 2023: 1809 - 1831.

CEN. "EUROPEAN ICT PROFESSIONAL ROLE PROFILES." 2018.

Center for Strategic & International Studies. *Cyber Operations during the Russo-Ukrainian War.* iulie 13, 2023. https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war#h2-in-the-future- (accessed noiembrie 24, 2024).

Cerghit, I., and C. Vlăsceanu. "Curs de pedagogie." In *Teoria și metodologia instruirii; Teoria și metodologia evaluării*, by Elena Tiron and Tudor Stanciu, 154. București: Editura Didactică și Pedagogică, 2019.

Choi, Kyung-Shick, Chitkushev Lou, Kyung-Seok Choo, and Claire Seungeun Lee. "Bureau of Justice Assistance Student Computer and Digital Forensics Education Opportunities Program: The Assessment of Online Graduate Students." *Proceedings of the 17th International Conference on Information Warfare and Security.* Albany: University of New York, 2022. 36 - 44.

CISCO. *Firewalls, IDS, and IPS Explanation and Comparison.* 2023. https://study-ccna.com/firewalls-ids-ips-explanation-comparison/ (accesat decembrie 11, 2023).

Clark, Robert, and Peter Oleson. "Cyber Intelligence." *Intelligencer: Journal of U.S. Intelligence Studies*, 2018: 11 - 23.

Condruț, Cristian. "ANALIZĂ DE CONȚINUT A ARIILOR STRATEGICE DE SECURITATE CIBERNETICĂ – STATELE UNITE ALE AMERICII, MAREA BRITANIE, SPANIA ȘI ROMÂNIA." *Intelligence și Cultura de Securitate.* București: ANIMV, 2023. 21 - 38.

Condruț, Cristian. „Comparative Analysis of Strategic Cyber Seucrity Focus Areas - United Kingdom, Estonia, Romania.” *Romanian Intelligence Studies Review* 29, nr. 1 (2023): 33 - 61.

—. "CYBERSECURITY KNOWLEDGE, SKILLS AND ABILITIES FOR INTELLIGENCE AND NATIONAL SECURITY ANALYSTS." *16th International Conference of Education, Research and Innovation.* Sevilia: IATED Academy, 2023. 4200 - 4209.

Condruț, Cristian. "Validation and Prioritization of Knowledge, Skills and Abilities for Cyberintelligence Analysis in Intelligence and National Security." *Impact Strategic*, 2024: 130 - 143.

Consiliul Uniunii Eruopene. *Recomandările Consiliului din 22 mai 2018 privind competențele cheie pentru învățarea pe parcursul întregii vieți.* Recommendations, Bruxelles: Official Journal of the European Union, 2018.

Constitutional Court of Romania. *COMUNICAT DE PRESĂ, 6 decembrie 2024.* December 6, 2024. https://www.ccr.ro/comunicat-de-presa-6-decembrie-2024/ (accessed February 11, 2025).

Corkill, Jeffrey, Teresa Kasprzyk Cunow, Elisabeth Ashton, and Amanda East. "Attributes of an analyst: What we can learn from the intelligence analysts job description." *8th Australian Security and Intelligence Conference.* Perth: Edith Cowan University, 2015. 35 - 42.

Coughlan, Michael, Patricia Cronin, and Frances Ryan. "Survey research: Process and limitatios." *International Journal of Therapy and Rehabilitation*, 2009: 9 - 15.

Coulthart, Stephen. *IMPROVING THE ANALYSIS OF FOREIGN AFFAIRS: EVALUATING STRUCTURED ANALYTIC TECHNIQUES.* Pittsburgh: University of Pittsburgh, 2015.

Crowdstrike. *2023 Global Threat Report.* Raport analitic de securitate ciberentică, Crowdstrike, 2023.

Cucoș, Constantin. *Teoria și metodologia evaluării.* Iași: Polirom, 2008.

Curelaru, Mihai. "Ancheta." In *Metode Cantitative de Cercetare. Designuri și Aplicații în Ştiințele Sociale,* by Loredana Diaconu-Gherasim, Cornelia Măierean and Mihai Curelaru, 161 - 187. București: Polirom, 2022.

Curelaru, Mihai. "Eșantionarea." In *Metode Cantitative de Cercetare. Designuri și Aplicații în Ştiințele Sociale,* by Loredana Diaconu-Gherasim, Cornelia Măierean and Mihai Curelaru, 295 - 318. București: Polirom, 2022.

Cyber Peace Institute. *Geopolitical map.* 2023. https://cyberconflicts.cyberpeaceinstitute.org/impact/geography (accessed November 26, 2024).

Daengsi, Therdpong, Phisit Pornpongtechavanich, și Pongpisit Wuttidittachotti. „Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks.” *Education and Information Technologies*, 2022: 4729 - 4752.

Delgado, Alan Briones, Sara Ricci, Argyro Chatzopoulou, Jakub Čegan, Petr Dzurenda, and Ioannis Koutoudis. "Enhancing Cybersecurity Education in Europe: The REWIRE’s Course Selection Methodology." *ARES 2023*,. Benevento: ACM, 2023. 1 - 7.

Denscombe, Martyn. *The Good Research Guide.* Berkshire: Open University Press, 2010.

Deparment of Labor. „Cybersecurity Model Download.” *Competency Model Clearinghouse.* aprilie 2024. https://www.careeronestop.org/CompetencyModel/competency-models/pyramid-download.aspx?industry=cybersecurity (accesat decembrie 5, 2024).

DGES Portugalia. *Who We Are.* fără an. https://www.dges.gov.pt/en/pagina/dges (accesat ianuarie 5, 2025).

Diaconu-Gherasim, Loredana R. „Validitatea internă în studiile cantitative.” În *Metode cantitative de cercetare. Designuri și aplicații în științele sociale*, de Loredana R. Diaconu-Gherasim, Cornelia Măierean și Mihai Curelaru, 229 - 245. Iași: Polirom, 2022.

Diaconu-Gherasim, Loredana. „Validitatea metodelor cantitative.” În *Metode cantitative de cercetare. Designuri și aplicații în științele sociale*, de Loredana Diaconu-Gherasim, Cornelia Măierean și Mihai Curelaru, 221 - 228. Iași: Polirom, 2022.

Dimitrov, Dimiter M., and Phillip D. Jr. Rumrill. "Pretest-posttest designs and measurement of change." *Speaking of Research*, 2003: 159 - 165.

Dobák, Imre. "Thoughts on the evolution of national security in cyberspace." *Security&Defence Quarterly*, 2021: 75-85.

DSN. "National Cybersecurity Strategy 2019." *DSN.* 2019. https://www.dsn.gob.es/eu/file/2989/download?token=EuVy2lNr (accessed April 24, 2023).

Dumitrache, Adrian. *SRI caută servicii de instruire în domeniul securității cibernetice. Buget de peste 26 milioane lei.* noiembrie 7, 2024. https://www.profit.ro/povesti-cu-profit/it-c/sri-cauta-servicii-de-instruire-in-domeniul-securitatii-cibernetice-buget-de-peste-26-milioane-lei-21821129 (accessed decembrie 7, 2024).

Dunn Cavelty, Myriam. "Cybersecurity between hypersecuritization and technological routine." In *Routledge Handbook of International Cybersecurity*, by Eneken Tikk and Mika Kerttunen, 11 - 20. Oxon: Routledge, 2020.

Dunn Cavelty, Myriam, and Andreas Wenger. "Cyber security between socio-technological uncertainty and political fragmentation." In *Cyber Security Politics. Socio-Technological Transformations and Political Fragmentation*, by Myriam Dunn Cavelty and Andreas Wenger, 1 -14. Oxon: Routledge, 2022.

ECCC. „Strategic Agenda.” *ECCC.* 17 martie 2023. https://cybersecurity-centre.europa.eu/system/files/2023-03/20230224%20-%20ECCC%20Strategic%20Agenda%20with%20cover.pdf#page=9.63 (accesat decemrbie 10, 2024).

ECHO Network. "Deliverables." *ECHO.* January 31, 2021. https://echonetwork.eu/wp-content/uploads/2021/03/ECHO_D2.6_Cyberskills-Framework.pdf (accessed November 28, 2024).

EEAS. *About the European External Action Service.* December 1, 2024. https://www.eeas.europa.eu/eeas/about-european-external-action-service_en (accessed December 9, 2024).

—. "European Union External Action." *A STRATEGIC COMPASS FOR SECURITY AND DEFENCE.* March 24, 2022. https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-0_en (accessed December 8, 2024).

Elsad, Amer. *THE EVOLUTION OF DOPPEL SPIDER FROM BITPAYMER TO GRIEF RANSOMWARE.* Raport analitic de securitate cibernetică, ARMOR, 2022.

ENISA. *European Cybersecurity Skills Framework (ECSF) - User Manual.* Framework, Athens: ENISA, 2022.

—. *European Cybersecurity Skills Framework (ECSF).* 2022. https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework (accessed November 28, 2024).

ENISA. *European Cybersecurity Skills Framework Role Profiles.* Framework, European Union Agency for Cybersecurity (ENISA), 2022.

Ernits, Margus, Kaie Maennel, Sten Mäses, Toomas Lepik, and Olaf Maennel. "From Simple Scoring Towards a Meaningful Interpretation of Learning in Cybersecurity Exercises." *15th International Conference on Cyber Warfare and Security.* Norfolk: Academic Conferences and publishing limited, 2020. 135 - 143.

Erstad, Erlend, Rory Hopcraft, Avanthika Vineetha Harish, and Kimberly Tam. "A human-centred design approach for the development and conducting of maritime cyber resilience training." *WMU Journal of Maritime Affairs* (Springer), 2023: 241 - 266.

ESDC. *ESDC.* n.d. https://esdc.europa.eu/who-we-are/#who (accessed December 9, 2024).

—. "ESDC Courses/Curricula." *ESDC.* 2024. https://esdc.europa.eu/wp-content/uploads/2024/11/2024-25-ESDC-Training-Catalogue-1.pdf#page=99.11 (accessed December 9, 2024).

Estes, Adriane, Dan Kim, and Andrew Yang. "Exploring How the NICE Cybersecurity Workforce Framework Aligns Cybersecurity Jobs with Potential Candidates." *Int'l Conf. Frontiers in Education: CS and CE | FECS'18.* CSREA Press, 2018. 58 - 64.

EU4Digital. *European ICT Professional Role Profiles.* 2018. https://eufordigital.eu/library/european-ict-professional-role-profiles/ (accesat November 28, 2024).

European Commission. "Communication on the Cybersecurity Skills Academy." *Comisia Europeană.* April 20, 2023. https://digital-strategy.ec.europa.eu/en/library/communication-cybersecurity-skills-academy (accessed December 9, 2024).

—. *DESI indicators.* 2024. https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts/desi-indicators?period=desi_2024&indicator=desi_ci_in_h&breakdown=hh_total&unit=pc_hh&country=AT,BE,BG,HR,CY,CZ,DK,EE,EU,FI,FR,DE,EL,HU,IE,IT,LV,LT,LU,MT,NL,PL,PT,RO,SK,SI,ES,S (accessed noiembrie 25, 2024).

—. *ESCOpedia.* May 15, 2024. https://esco.ec.europa.eu/en/about-esco/escopedia/escopedia (accessed November 24, 2024).

—. "EU Policy on Cyber Defence - EEAS - European Union." *European External Action Service.* November 10, 2022. https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf (accessed December 9, 2024).

—. *The ESCO Classification.* n.d. https://esco.ec.europa.eu/en/classification/occupation_main#overlayspin (accessed November 28, 2025).

—. "The EU's Cybersecurity Strategy for the Digital Decade." *Comisia Europeană.* December 16, 2020. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (accessed December 8, 2024).

Frost, Jim. *ANCOVA: Uses, Assumptions & Example.* 2024. https://statisticsbyjim.com/anova/ancova/ (accesat mai 25, 2024).

Gatewood, Robert, Hubert Feild, and Murray Barrick. *HUMAN RESOURCE SELECTION.* Mason, Ohio: Cengage Learning, 2011.

Georgieva, Ilina. "The unexpected norm-setters: Intelligence agencies in cyberspace." *CONTEMPORARY SECURITY POLICY,* 2019: 1-22.

Ghernouti-Hélie, Solange. "A national strategy for an effective cybersecurity approach and culture." *2010 International Conference on Availability, Reliability and Security.* Cracovia: IEEE, 2010. 370 - 373.

Ghosh, Tirthankar, and Guillermo Francia III. "Assessing Competencies Using Scenario-Based Learning in Cybersecurity." *Journal of Cybersecurity and Privacy,* 2021: 539 - 552.

Giesecke, Jan Peter. "CYBER SECURITY/DEFENCE AND THE CSDP." In *HANDBOOK ON CSDP THE COMMON SECURITY AND DEFENCE POLICY OF THE*

EUROPEAN UNION, by Jochen Rehrl, 125 - 130. Viena: Directorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria, 2021.

Google. *APT42: Crooked Charms, Cons, and Compromises.* September 7, 2022. https://cloud.google.com/blog/topics/threat-intelligence/apt42-charms-cons-compromises (accessed December 11, 2024).

—. *Mandiant Cyber Security Forecast 2023.* November 7, 2022. https://cloud.google.com/blog/topics/threat-intelligence/cyber-security-forecast-2023-predictions/ (accessed December 2, 2024).

—. *We (Did!) Start the Fire: Hacktivists Increasingly Claim Targeting of OT Systems.* March 22, 2023. https://cloud.google.com/blog/topics/threat-intelligence/hacktivists-targeting-ot-systems/ (accessed December 11, 2024).

Gopalan, Maithreyi, Kelly Rosinger, and Jee Bin Ahn. "Use of Quasi-Experimental Research Designs in Education Research: Growth, Promise, and Challenges." *Review of Research in Education*, 2020: 218 - 243.

Gorbănescu, Adrian. "Curs 5 - ANCOVA." *SCRIBD.* March 23, 2024. https://www.scribd.com/document/716408057/Curs-5-ANCOVA-1 (accessed May 23, 2024).

Górka, Marek. "CONCEPTUALISING SECURITISATION IN THE FIELD OF CYBER SECURITY POLICY." *Journal of Modern Science*, 2023: 263 - 290.

Goss-Sampson, Mark. "Resources." *JASP.* 2020. https://jasp-stats.org/wp-content/uploads/2020/11/Statistical-Analysis-in-JASP-A-Students-Guide-v14-Nov2020.pdf (accessed December 21, 2024).

Hansen, Lene, and Helen Nissenbaum. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly*, 2009: 1155-1175.

Heuer Jr., Richards J. *Psychology of Intelligence Analysis.* Center fot the Study of Intelligence, 1999.

HM Government . "National Cyber Strategy 2022." 2022. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf (accessed March 16, 2023).

Hodges, Duncan, and Sadie Creese. "Understanding cyber-attacks." In *Cyber Warfare A multidisciplinary analysis*, by James Green, 33 - 60. Oxon: Routledge, 2015.

Hodhod, Rania, Harlie Hardage, Safia Abbas, and Eman Abdullah Aldakheel. "CyberHero: An Adaptive Serious Game to Promote Cybersecurity Awareness." *Electronics*, 2023: 1 - 18.

Hollnagel, Erik. „Epilogue: RAG – The Resilience Analysis Grid." În *Resilience Engineering in Practice. A Guidebook*, de Erik Hollnagel , Jean Paries, David Woods și John Wreathall, 275-296. Surrey: Ashgate Publishing Limited, 2011.

Hsieh, Hsiu-Fang, and Sarah Shannon. "Three Approaches to Qualitative Content Analysis." *Qualitative Health Research* (SAGE publications) 15, no. 9 (2005): 1277-1288.

Huhn, Heidi. *DEFENDING INFRASTRUCTURE AGAINST CYBER ATTACKS THROUGH QUALIFIED CYBERSECURITY PROFESSIONALS IN THE FEDERAL GOVERNMENT: A CASE STUDY.* Minneapolis: Capella University, 2020.

Hytönen, Eveliina, Amir Trent, and Harri Ruoslahti. "Societal Impacts of Cyber Security in Academic Literature: Systematic Literature Review." *Proceedings of the 21st European Conference on Cyber Warfare and Security.* Academic Conferences International Limited, 2022. 86 - 93.

Iliescu, Dragoș, Sergiu Condrea, and Raluca Duțu. "Calități psihometrice ale scalelor de evaluare." In *Metode cantitative de cercetare. Designuri și aplicații în științele sociale,* by Loredana Diaconu-Gherasim, Cornelia Măierean and Mihai Curelaru, 345 - 364. Iași: Polirom, 2022.

IMDA. *Skills Framework for Infocomm Technology.* August 14, 2024. https://www.imda.gov.sg/how-we-can-help/techskills-accelerator-tesa/skills-framework-for-infocomm-technology-sfw-for-ict#:~:text=Some%20critical%20skill%20areas%20include,and%20develop%20the%20necessary%20skills. (accessed November 28, 2024).

—. "Skills Framework for Infocomm Technology." *IMDA.* 2024. https://www.imda.gov.sg/-/media/imda/images/programmes/skills-framework-for-ict/consolidated-career-maps.pdf#page=185.99 (accessed November 28, 2024).

Imperva. *Website Defacement Attack.* 2024. https://www.imperva.com/learn/application-security/website-defacement-attack/ (accesat mai 27, 2024).

IMSISS. *Programme Structure.* 2023. https://www.securityintelligence-erasmusmundus.eu/the-programme/programme-structure/ (accessed January 5, 2025).

—. "What is IMSISS?" *IMSISS.* 2023. https://www.securityintelligence-erasmusmundus.eu/ (accessed January 5, 2025).

International Association for Intelligence Education. "Academic Programs & Standards." *IAFIE.* octombrie 25, 2011. https://iafie.org/docs/iafie_intelligence_education.pdf (accessed November 27, 2024).

ITU Development Sector. „Global Cybersecurity Index 2020.” *ITUPublications.* 2021. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accesat Aprilie 6, 2023).

ITU. "Guide to Devepoling a National Cybersecurity Strategy." *United Nations.* 2021. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2021-ncs-guide.pdf (accessed March 16, 2023).

Jacob, Johanna, Wei Wei, Kewei Sha, Sadegh Davari, and Andrew Yang. "IS THE NICE CYBERSECURITY WORKFORCE FRAMEWORK (NCWF) EFFECTIVE FOR A

WORKFORCE COMPRISED OF INTERDISCIPLINARY MAJORS?" *Int'l Conf. Scientific Computing | CSC'18.* CSREA Press, 2018. 124 - 130.

Jinga, Ioana, and Elena Istrate. "Manual de Pedagogie." In *Teoria și Metodologia Evaluării*, by Marin Manolescu, 26. București: ALL, 2010.

Joinson, Adam, Matt Dixon, Lynne Coventry, and Pam Briggs. "Development of a new 'human cyber-resilience scale'." *Journal of Cybersecurity* (Oxford Academic) 9, no. 1 (aprilie 2023): 1-10.

Justice, Connie, Char Sample, Sin Ming Loo, Alex Ball, and Clay Hampton. "Future Needs of the Cybersecurity Workforce." *17th International Conference on Information Warfare and Security.* 2022. 81 - 91.

Kang, Hyun. „Sample size determination and power analysis using the G*Power software." *J Educ Eval Health Pro*, 2021: 1 - 12.

Karinsalo, Anni, Karo Saharinen, Jani Päijänen, and Jarno Salonen. "Pedagogical and self-reflecting approach to improving the learning within a cyber exercise." *21st European Conference on Cyber Warfare and Security.* Chester: Academic Conferences International Limited, 2022. 105 - 114.

Kennedy, Declan, Aine Hyland, and Norma Ryan. In *Bologna Handbook, Introducing Bologna Objectives and Tools*, 1 - 18. Cork, 2009.

Krathwohl, David. „A Revision of Bloom's Taxonomy: An Overview." *Theory Into Practice*, 2002: 212 - 218.

Kuzminykh, Ievgeniia, Maryna Yevdokymenko,, Oleksandra Yeremenko, and Oleksandr Lemeshko. "Increasing Teacher Competence in Cybersecurity Using the EU Security Frameworks." *I.J. Modern Education and Computer Science*, 2021: 60 - 68.

Laerd Statistics. *Mixed ANOVA using SPSS Statistics.* 2024. https://statistics.laerd.com/spss-tutorials/mixed-anova-using-spss-statistics.php#:~:text=A%20mixed%20ANOVA%20compares%20the,%22between%2Dsubjects%22%20factor. (accessed December 21, 2024).

Laerd statistics. *ruskal-Wallis H Test using SPSS Statistics.* 2024. https://statistics.laerd.com/spss-tutorials/kruskal-wallis-h-test-using-spss-statistics.php (accesat decembrie 27, 2024).

Le Deist, Delamare Francoise, and Jonathan Winterton. "What Is Competence?" *Human Resource Development International*, 2005: 27 - 46.

Lee, Robert. *Cyber Intelligence Part 1: An Introduction to Cyber Intelligence.* 27 6 2015. https://www.robertmlee.org/cyber-intelligence-part-1-an-introduction-to-cyber-intelligence/ (accesat 12 4, 2022).

Lehto, Martti. "Cyber Security Capacity Building: Cyber Security Education in Finnish Universities." *European Conference on Cyber Warfare and Security.* Reading, 2020. 221 - 231.

Limnéll, Jarno , et al. *Cyber citizen skills and their development in the European Union.* Aalto University Research Group, 2023.

Linkov , Igor, and Alexander Kott. "Fundamental Concepts of Cyber Resilience: Introduction and Overview." In *Cyber Resilience of Systems and Networks*, by Igor Linkov and Alexander Kott, 1-28. Cham: Springer International Publishing, 2019.

MAEC Estonia. „Cybersecurity Strategy. Republic of Estonia." 2019. https://www.mkm.ee/media/703/download (accesat Martie 16, 2023).

Maftei, Dănuț. "The Cyber Competences Act - a Vital EU Regulation Concerning Mandatory Certification of Critical Network and Information Systems' Operators across the European Union." *Informatica Economică*, 2024: 45 - 60.

Major, James. *Writing Classified and Unclassified Papers in the Intelligence Community.* New York: Scarecrow Press, 2009.

Manolescu, Marin. *Teoria și Metodologia Evaluării.* București: Editura Universitară, 2010.

Mardar, Sorina-Mihaela. "NEEDS ASSESSMENT QUESTIONNAIRE FOR THE INTELLIGENCE ANALYSTS." *The 13th International Scientific Conference eLearning and Software for Education.* București: Carol I National Defence University Publishing House, 2017. 154 - 159.

Martin, Chris, Chris Quillen, and Tim Shaw. "Lessons Learned from Intelligence Internships from Three Midwest Universities." *Journal of Strategic Security*, 2013: 207 - 213.

„Master of Intelligence and Security Studies (MISS)." *University of the Bundeswehr Munich.* 2023. https://www.unibw.de/ciss/miss/details/mhb-miss-2023-2024-01-12-23-final.pdf (accesat ianuarie 5, 2025).

MAXQDA. *Code Co-Occurence Model.* n.d. https://www.maxqda.com/help-mx20/maxmaps/the-co-occurrence-model (accessed April 23, 2023).

McKinney, Giovanni Bryan Jamal. *ASSESSING CORPORATE IMPACTS OF CYBER TRAINING ON EMAIL PHISHING ATTACKS.* Oklahoma: Southern Nazarene University, 2021.

Melnikovas, Aleksandras, Ricardo G. Lugo, Kaie Maennel, Agnė Brilingaitė, Stefan Sütterlin, and Aušrius Juozapavičius. "Teaching Pentesting to Social Sciences Students Using Experiential Learning Techniques to Improve Attitudes towards Possible Cybersecurity Careers." *Proceedings of the 22nd European Conference on Cyber Warfare and Security.* 2023. 294 - 302.

Microsoft. *Defending Ukraine: Early Lessons from the Cyber War.* Microsoft, 2022.

Ministry of Defence. "GRU close access cyber operation against OPCW." *Ministry of Defence.* October 4, 2018. https://english.defensie.nl/topics/cyber-security/documents/publications/2018/10/04/gru-close-access-cyber-operation-against-opcw (accessed November 25, 2024).

Ministry of Internal Affairs. "Standarde Ocupaționale." *Autoritatea Națională pentu Calificări.* April 4, 2013. https://intern.anc.edu.ro/virtualanc/crud/standarde/standarde_ocupationale/brain/upload/analist%20de%20informatii_00.pdf (accessed November 28, 2024).

Ministry of Labour and Social Protection. "CLASIFICAREA OCUPAȚIILOR DIN ROMÂNIA." *Ministry of Labour and Social Protection.* October 15, 2024. https://mmuncii.ro/j33/index.php/ro/2014-domenii/munca/c-o-r?id=46:cor-isco- (accessed November 28, 2024).

MIVD. *Russian cyber operation disrupted.* 13 aprilie 2018. https://english.defensie.nl/topics/cyber-security/russian-cyber-operation (accesat noiembrie 25, 2024).

Mueller, Robert. *Report On The Investigation Into Russian Interference In The 2016 Presidential Election.* Washington D.C.: U.S. Department of Justice, 2019.

Mukherjee, Madhav, Ngoc Thuy Le, Yang-Wai Chow, and Willy Susilo. "Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes." *Information*, 2024: 1 - 23.

National Security Agency. *NSA, FBI, CISA, and Allies Issue Advisory about Russian Military Cyber Actors.* septembrie 5, 2024. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3895808/nsa-fbi-cisa-and-allies-issue-advisory-about-russian-military-cyber-actors/ (accessed noiembrie 26, 2024).

Nebrija University. *Máster en Análisis de la Inteligencia y Ciberinteligencia.* n.d. https://www.nebrija.com/programas-postgrado/master/ciberinteligencia/#planEstudios (accessed January 5, 2025).

—. *Master's Degree in Intelligence Analysis and Cyberintelligence.* fără an. https://www.nebrija.com/en/postgraduate-degree/master/cyberintelligence/#principal (accesat ianaurie 5, 2025).

Nevmerzhitskaya, Julia, Elisa Norvanto, and Csaba Virag. "High Impact Cybersecurity Capacity Building." *The 15th International Scientific Conference.* Bucharest: Universitatea Națională de Apărare „Carol I", 2019. 306 - 312.

Newhouse, William, Stephanie Keith, Benjamin Scribner, and Greg Witte. *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.* NIST Special Publication, Gaithersburg: National Institute of Standards and Technology, 2017.

NICCS. *About NICCS.* n.d. https://niccs.cisa.gov/about-niccs (accessed November 28, 2024).

NICSS. *Workforce Framework for Cybersecurity (NICE Framework).* June 17, 2024. https://niccs.cisa.gov/workforce-development/nice-framework (accessed November 28, 2024).

Nilsen, Richard. *Measuring Cybersecurity Competency: An Exploratory Investigation of the Cybersecurity Knolwledge, Skills and Abilities Necessary for Organizational Network*

Access Privileges. Fort Lauderdale-Davie, Florida: Nova Southeastern University, 2017.

—. *Measuring Cybersecurity Competency: An Exploratory Investigation of the Cybersecurity Knowledge, Skills, and Abilities Necessary for Organizational Network Access Privileges.* Florida: Nova Southeastern University, 2017.

NIST. „Change Logs.” *NICE Framework Resource Center.* 5 martie 2024. https://www.nist.gov/system/files/documents/2024/03/04/NICE%20Framework%20Components%20v1.0.0_Summary%20of%20Changes_March2024.pdf (accesat noiembrie 28, 2024).

—. *Change Logs.* 2024. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/change-logs (accessed November 24, 2024).

—. "Change Logs." *NIST.* 2017. https://www.nist.gov/document/supplementnicespecialtyareasandworkroleksasandtasksxlsx (accessed November 28, 2024).

—. "Change Logs." *NIST.* March 5, 2024. https://www.nist.gov/document/nice-framework-components-v100 (accessed November 28, 2024).

Nobles, Calvin. "The Cyber Talent Gap and Cybersecurity Professionalizing." *International Journal of Hyperconnectivity and the Internet of Things*, 2018: 42 - 51.

Nuffic. *Who we are?* fără an. https://www.nuffic.nl/en/subjects/about-us/who-are-we (accesat ianuarie 5, 2025).

Nweke, Livinus Obiora, Anthony Jnr Bokolo, Gibson Mba, and Emeka Nwigwe. "Investigating the effectiveness of a HyFlex cyber security training in a developing country: A case study." *Education and Information Technologies*, 2022: 10107 - 10133.

Office for Director of National Intelligence. *ICD-203_TA_Analytic_Standards.* 21 December 2022. https://www.odni.gov/files/documents/ICD/ICD-203_TA_Analytic_Standards_21_Dec_2022.pdf (accesat November 27, 2024).

Office of the Director of National Intelligence. *Background to “Assessing Russian Activities and Intentions in Recent US Elections”: The Analytic Process and Cyber Incident Attribution.* Raport analitic de securitate ciberentică, ODNI, Washington: ODNI, 2017.

OPM. „Competency Model for Cybersecurity.” *Chief Human Capital Officers Council* . 16 februarie 2011. https://www.chcoc.gov/content/competency-model-cybersecurity (accesat decembrie 5, 2024).

Oprea, Crenguța-Lăcrămioara. *Strategii Didactice Interactive.* București: Editura Didactică și Pedagogică, 2006.

Ottis, Rain. *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective.* Analysis, Tallinn: Cooperative Cyber Defence Centre of Excellence, 2018.

Päijänen, Jani, Jarno Salonen, Anni Karinsalo, Tuomo Sipola, and Tero Kokkonen. "Participants Prefer Technical Hands-on Cyber Exercises Instead of Organisational and Societal Ones." *22nd European Conference on Cyber Warfare and Security.* Pireu: Academic Conferences International Limited, 2023. 349 - 357.

Petersen, Rodney, Danielle Santos, Karen Wetzel, Matthew Smith, and Greg Witte. "The Workforce Framework for Cybersecurity (NICE Framework)." *NIST.* November 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf (accessed November 27, 2023).

Petersen, Rodney, Danielle Santos, Karen Wetzel, Matthew Smith, and Greg Witte. *Workforce Framework for Cybersecurity (NICE Framework).* NIST Special Publication, Gaithersburg: National Institute of Standards and Technology, 2020.

President of Romania. November 28, 2024. https://csat.presidency.ro/ro/comuni/sedinta-consiliului-suprem-de-aparare-a-tarii1732806302 (accessed December 8, 2024).

—. *Comunicat de presă.* Decembrie 4, 2024. https://www.presidency.ro/ro/media/comunicate-de-presa/comunicat-de-presa1733327193 (accessed Decembrie 2025, 11).

—. "Strategia Națională de Apărare a Țării pentru perioada 2020 - 2024." *President of Romania.* 2020. https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf (accessed December 6, 2024).

Proctor, R.W., and A. Dutta. "Skill Acquisition and Human Performance." In *Typology of knowledge, skills and competences: clarification of the concept and prototype*, by Jonathan Winterton, Françoise Delamare - Ledeist and Emma Stringfellow, 28. Thesaloniki: Cedefop, 2005.

Rausch, Joseph, Scott Maxwell, and Ken Kelley. "Analytic Methods for Questions Pertaining to a Randomized Pretest, Posttest, Follow-Up Design." *Journal of Clinical Chil and Adolescent Psychology,* 2003: 467 - 486.

Rehrl, Jochen. *HANDBOOK ON CSDP THE COMMON SECURITY AND DEFENCE POLICY OF THE EUROPEAN UNION.* Viena: Directorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria, 2021.

Reichardt, Charles. *Quasi-Experimentation A Guide to Design and Analysis.* New York: The Guilford Press, 2019.

Reith, Mark, Eric Trias, Chad Dacus, Seth Martin, and Landon Tomcho. "Rethinking USAF Cyber Education and Training." *Proceedings of the 13th International Conference on Cyber Warfare and Security.* 2018. 439 - 447.

Republic of Estonia Education and Youth Board. *The Education and Youth Board.* fără an. https://harno.ee/en (accesat ianuarie 5, 2025).

REWIRE. *About.* 2020. https://rewireproject.eu/about/ (accessed November 28, 2024).

—. „Deliverables.” *REWIRE.* 25 octombrie 2022. https://rewireproject.eu/wp-content/uploads/2022/11/R3.3.1.-Cybersecurity-Skills-Framework_FINAL.pdf#page=54.10 (accesat noiembrie 28, 2024).

Richardson, John. "Eta squared and partial eta squared as measures of effect size in educational research." *Educational Research Review*, 2011: 135 - 147.

Romanian Government. "E-monitor." *Monitorul Oficial.* January 3, 2022. https://monitoruloficial.ro/Monitorul-Oficial--PI--2Bis--2022.html (accessed April 18, 2023).

Romanian Intelligence Service. "Comunicat de presă." *Președintele României.* December 4, 2024. http://www.presidency.ro/files/userfiles/Documente%20CSAT/Document%20CSAT%20SRI%20II.pdf (accessed December 8, 2024).

Rupp, Christina. „Navigating the EU Cybersecurity Policy Ecosystem.” *interface.* 27 iunie 2024. https://www.interface-eu.org/publications/navigating-the-eu-cybersecurity-policy-ecosystem (accesat decembrie 9, 2024).

Saharinen, Karo, and Sampo Kotikoski. "Critical Infrastructure Protection: Employer Expectations for Cyber Security Education in Finland." *20th European Conference on Cyber Warfare and Security.* Chester: University of Chester, 2021. 195 - 202.

Salamah, Fai Ben, Marco Palomino, Matthew Craven, Maria Papadaki, and Steven Furnell. "An Adaptive Cybersecurity Training Framework for the Education of Social Media Users at Work." *Applied Sciences*, 2023: 1 - 18.

Salminen, Mirva, Niko Candelin, Kaisa Cullen, Sari Latvanen, Marianne Lindroth, and Teemu Matilainen. "Cybersecurity education in European higher education institutions." *9th International Conference on Higher Education Advances.* Valeincia: Universitatea din Valencia, 2023. 1357 - 1364.

Salzberger, Alina. "Cyber Risk Awareness of German SMEs: An Empirical Study on the Influence of Biases and Heuristics." *Zeitschrift für die gesamte Versicherungswissenschaft*, 2024: 55 - 104.

Satewatch. February 5, 2015. https://www.statewatch.org/media/documents/news/2016/may/eu-intcen-factsheet.pdf (accessed December 9, 2024).

SDU. *Curriculum for Master in Intelligence and Cyber Studies.* 1 septembrie 2021. https://odin.sdu.dk/sitecore/index.php?a=sto&id=54032&lang=da (accesat ianuarie 5, 2025).

—. *Master in Intelligence and Cyber Studies.* 2024. https://www.sdu.dk/da/uddannelse/efter_videreuddannelse/master/master-in-intelligence-and-cyber-studies (accesat January 5, 2025).

„Security Strategy for the Kingdom of the Netherlands.” *Government of the Netherlands.* 2023. https://www.government.nl/topics/security-strategy-for-the-kingdom-of-the-netherlands (accesat November 26, 2024).

SFIA Foundation. *SFIA - a framework for cyber security skills.* 2023. https://sfia-online.org/en/tools-and-resources/cybersecurity-skills-framework (accessed November 28, 2024).

—. *Skills at a glance.* 2023. https://sfia-online.org/en/tools-and-resources/en/sfia-9/sfia-views/information-and-cyber-security/?path=/glance (accesat noiembrie 28, 2024).

Shadish, William R., Thomas D. Cook, and Donald T. Campbell. *Experimental and quasi-experimental designs for generalized causal inference.* Boston: Houghton Mifflin Company, 2002.

Sharpe, Donald, and Robert Cribbie. "Analysis of Treatment-Control Pre-Post-Follow-up Design Data." *The Quantitative Methods for Psychology*, 2023: 25 - 46.

Sisyuk, Kristina. "Training, knowledge, competence, performance: What is the relationship?" *Journal of Administrative and Business Studies* 4, no. 6 (2018): 295 - 310.

Sithole, Thenjiwe, Jaco Du Toit, and Sebastian H von Solms. "A Cyber Counterintelligence Competence Framework: Developing the Job Roles." *22nd European Conference on Cyber Warfare and Security.* Atena, 2023. 450 - 457.

Sithole, Thenjiwe, Petrus Duvenage, Victor Jaquireand, and Sebastian von Solms. "Eating the Elephant-A structural outline of Cyber Counterintelligence Awareness and Training." *14th International Conference on Cyber Warfare and Security: ICCWS 2019.* Stellenbosch: Academic Conferences and publishing limited, 2019. 396 - 404.

Sofendi, S. "CONSTRUCTING A STANDARDIZED TEST." *Sriwijaya University Learning and Education International Conference.* Sriwijaya, 2016. 97 - 106.

Stanciu, Tudor. „Teoria și metodologia evaluării.” În *Teoria și metodologia instruirii. Teoria și metodologia evaluării*, de Elena Tiron și Tudor Stanciu, 195 - 275. București: Editura Didactică și Pedagogică , 2019.

Statisticshowto. *Winsorize: Definition, Examples in Easy Steps.* 2024. https://www.statisticshowto.com/winsorize/ (accesat mai 25, 2024).

Stavrou, Eliana, and Andriani Piki. "Cultivating self-efficacy to empower professionals’ re-up skilling in cybersecurity." *Information & Computer Security*, 2024: 523 - 541.

Stuparu, Ana Aurora. *Educational pathwaysto national cyber resilience: the Australian story.* Canberra: Australian National University, 2020.

Sussman, Lori. "Exploring the Value of Non-Technical Knowledge, Skills, and Abilities (KSAs) to Cybersecurity Hiring Managers." *Journal of Higher Education Theory and Practice*, 2021: 99 - 117.

TalTech. *Intelligence Methods for Cyber Professionals.* fără an. https://ois2.taltech.ee/uusois/subject/ITC8007 (accesat ianaurie 5, 2025).

—. *MSC IN CYBERSECURITY.* n.d. https://taltech.ee/en/masters-programmes/cybersecurity (accessed January 5, 2025).

Technical University of Valencia. *A Professional Vision Of Cybersecurity.* n.d. https://www.upv.es/pls/oalu/sic_asi.Busca_Asi?p_codi=34884&p_caca=2024&P_IDIOMA=i&p_vista=MSE&p_tit=2287 (accessed January 7, 2025).

—. *Cyber Situational Awareness.* n.d. https://www.upv.es/pls/oalu/sic_asi.Busca_Asi?p_codi=34882&p_caca=2024&P_IDIOMA=i&p_vista=MSE&p_tit=2287 (accessed January 7, 2025).

—. „Master's Degree in Cybersecurity and Cyberintelligence.” *Technical University of Valencia.* fără an. https://www.upv.es/titulaciones/MUCC/menu_1100975i.html (accesat ianaurie 5, 2025).

—. *Master's Degree in Cybersecurity and Cyberintelligence.* 2024. https://www.upv.es/titulaciones/MUCC/indexi.html (accessed January 5, 2025).

Tempus Public Foundation. *About us.* fără an. https://tka.hu/37/about-us (accesat ianuarie 5, 2025).

The White House. "FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy." *The White House.* March 2, 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (accessed April 24, 2023).

Thorsten, Kodalle. "Cyber Wargaming on the Technical/Tactical Level: The Cyber Resilience Card Game (CRCG)." *European Conference on Cyber Warfare and Security.* Reading, 2020. 195 - 204.

Tiron, Elena. "Teoria și metodologia instruirii." In *Teoria și metodologia instruirii. Teoria și metodologia evaluării*, by Elena Tiron and Tudor Stanciu, 8 - 194. București: Editura Didactică și Pedagogică, 2019.

Tomcho, Landon, Alan Lin, David Long, Mark Coggins, and Reith Mark. "Applying Game Elements to Cyber eLearning: An Experimental Design." *International Conference on Cyber Warfare and Security.* 2019. 422 - 430.

UHR. *About the Council.* fără an. https://www.uhr.se/en/start/about-the-council/ (accesat ianuarie 5, 2025).

UK Government. *Professional Development Framework for all-source intelligence assessment.* 4 April 2023. Professional Development Framework for all-source intelligence assessment (accesat November 27, 2024).

UNAp. "Facultatea de Securitate și Apărare - Studii universitare de masterat." *UNAp.* February 14, 2024. https://www.unap.ro/RO/PREZENTARE_GENERALA/Regulament%20de%20admitere%20UNAp%20MASTER.pdf (accessed January 7, 2025).

—. „Ghid de studii FSA." *UNAp.* 2022. https://www.unap.ro/ro/unitati/fsa/Ghid%20de%20studii/Ghid%20de%20studii%202022-2023%20-%20smcta.pdf (accesat ianaurie 5, 2025).

University for Continuing Education Krems. *Counter-Terrorism, Prevention of Violent Extremism and Intelligence* . 2024. https://www.donau-uni.ac.at/de/studium/counter-terrorism.html#%C3%9Cberblick (accesat ianuarie 5, 2025).

—. "Counter-Terrorism, Prevention of Violent Extremism and Intelligence." *University for Continuing Education Krems.* August 23, 2024. https://www.donau-uni.ac.at/dam/jcr:70dce787-aad9-4b24-a000-e7e8383e5ef0/Curriculum-Counter-Terrorism-Prevention-of-Violent-Extremism-and-Intelligence-MA-MB-2024-51.pdf#page=null (accessed January 5, 2025).

University of the Bundeswehr Munich. *Master of Intelligence and Security Studies (MISS).* 2023. https://www.unibw.de/ciss/miss (accesat ianuarie 5, 2025).

US Deparment of Commerce. „Guide to Cyber Threat Information Sharing." *NIST.* octombrie 2016. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-150.pdf (accesat decembrie 11, 2023).

van Niekerk, Brett, Trishana Ramluckan, and Petrus Duvenage. "An Analyisis of Selected Cyber Intelligence Texts." *18th European Conference on Cyber Warfare and Security (ECCWS 2019).* Coimbra: Curran Associates, Inc., 2019. 551-559.

Varbanov, Pavel. "Perspectives in the Design of a Modern Cybersecurity Training Programme: The ECHO Approach." *Information & Security,* 2022: 177 - 190.

Villalón-Fonseca, Ricardo. „The nature of security: A conceptual framework for integral-comprehensive modeling of IT security and cybersecurity." *Computers & Security,* 2022: 1 - 22.

Vilnius University. *The Arqus Joint Master's Programme "International Cybersecurity and Cyberintelligence".* 2024. https://www.vu.lt/en/studies/master-studies/the-arqus-joint-master-s-programme-international-cybersecurity-and-cyberintelligence#key-learning-outcomes (accessed January 5, 2025).

Vîrgă, Delia, and Luca Tisu. "Cvasi-experimentul ca alternativă la cercetarea experimentală." In *Metode Cantitative de Cercetare - Designuri și aplicații în științele sociale*, by Loredana Diaconu-Gherasim, Cornelia Măierean and Mihai Curelaru, 120 - 135. Iași: Polirom, 2022.

Walmsley, Angela, and Michael Brown. *What Is Power?* September 15, 2017. https://www.statisticsteacher.org/2017/09/15/what-is-power/ (accessed December 23, 2024).

Westby, Jody. "COUNTERING TERRORISM WITH CYBER SECURITY." *International Seminar On Nuclear War And Planetary Emergencies—36th Session.* Erice, 2006. 279-294.

White, Marilyn Domas, and Emily Marsh. "Content Analysis: A Flexible Methodology." *Library Trends,* 2006: 22-45.

Williams, Phil, Timothy Shimeal, and Casey Dunlevy. "Intelligence Analysis for Internet Security." *Contemporary Security Policy,* 2010: 1-38.

Winterton, Jonathan, Emma Stringfellow, and Francoise Delamare - Le Deist. *Typology of Knowledge, Skills and Competences: Clarification of the Concept and Prototype.* Edited by Cedefop. Thessaloniki: Centre for European Research on Employment and Human Resources / Groupe ESC Toulouse, 2005.

Yang, Yang Lydia. *3.4: Factorial ANOVA - Simple Effects.* January 4, 2023. https://stats.libretexts.org/Courses/Kansas_State_University/EDCEP_917%3A_Experimental_Design_(Yang)/03%3A_Between-Subjects_Factorial_Design/3.04%3A_Factorial_ANOVA_-_Simple_Effects (accessed December 21, 2024).