

Application of Structural Equation Modelling to Cybersecurity Risk Analysis in the Era of Industry 4.0

Miroslav Gombár ¹, Alena Vagaská ^{2,*}, Antonín Korauš ³ and Pavlína Račková ⁴

¹ Department of Management, Faculty of Management and Business, University of Prešov, 080 01 Prešov, Slovakia; miroslav.gombar@unipo.sk

² Department of Natural Sciences and Humanities, Faculty of Manufacturing Technologies with a Seat in Prešov, Technical University of Košice, 080 01 Prešov, Slovakia

³ Department of Information Science and Management, Academy of the Police Force in Bratislava, 835 17 Bratislava, Slovakia; antonin.koraus@akademiapz.sk

⁴ Department of Mathematics and Physics, Faculty of Military Technology, University of Defence, 662 10 Brno, Czech Republic; pavlina.rackova@unob.cz

* Correspondence: alena.vagaska@tuke.sk

Abstract: In the current digital transformation to Industry 4.0, the demands on the ability of countries to respond responsibly and effectively to threats in the field of cyber security (CS) are increasing. Cyber safety is one of the pillars and concepts of Industry 4.0, as digitization brings convergence and integration of information and operational technologies (IT/OT systems and data). Collecting and connecting a large amount of data in smart factories and cities poses risks, in a broader context for the entire state. The authors therefore focus attention on the issue of CS, where, despite all digitization, the human factor plays a key role - an actor of risk as well as strengthening the sustainability and resilience of CS. It is obvious that how the individual (decision maker) perceives the risk, thus he subsequently evaluates the situation and countermeasures. Perceiving cyber threats/risks in their complexity as a part of hybrid threats (HT) helps decision makers to prevent and manage them. Despite the growing trend of HT, we perceive a lack of research focused on the perception of threats by individuals and companies, there is a lack of methodology and evaluation strategy. Within the study, the authors present the results of the conducted research focused on mathematical modeling of the perception of the risk of threats to the state and industry through the disruption of cyber security and provide the developed factor model of cyber security (FMCS), i.e. the model of CS threat risk perception. When creating the FMCS factor model, the authors apply SEM (Structural Equation Modeling) and confirmatory factor analysis to data obtained through the implementation of the research tool (a questionnaire designed by the authors). Within it, the authors defined the pillars and sub-pillars of CS, which enabled quantification in the perception of the level of risk of CS as well as differentiation and comparison between the analyzed groups of respondents (students of considered universities in SK and CZ). Finally, the convergent and discriminant validity of the research instrument was verified and its reliability was confirmed (Cronbach's alpha = 0.95047). At the significance level $\alpha=5\%$, the influence of the individual defined pillars was demonstrated as significant. For the entire research set $N = 964$, the highest share of risk perception of CS threats was achieved by the DISRIT pillar (Disruption or reduction of the resistance of IT infrastructure).

Keywords: mathematical modeling; Industry 4.0; cybersecurity IT regulation; cybersecurity factor model; risk perception; structural equations modelling; confirmatory factor analysis

Citation: To be added by editorial staff during production.

Academic Editor: Firstname Last-name

Received: date

Revised: date

Accepted: date

Published: date



Copyright: © 2023 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The dynamics of development and implementation of information technology (IT) and operations technologies (OT) in the Industry 4.0 era is quite aggressive. Developments in the field of industrial engineering are influenced and driven by, among others,

the development of digitalization [1], the Internet of Things (IoT) [2], the Internet of Services (IoS) [3], cloud computing [4], robotics, cybernetics [5], artificial intelligence [6], machine learning [7] and other new technologies [4]. The implementation of Industry 4.0 concepts and technologies is almost unlimited [8] and finds application in various branches of industry, which in a revolutionary way changes both the production itself and the distribution of finished products or services in terms of increasing productivity, efficiency and quality [9]. This subsequently affects the quality of the functioning of the entire society and state. Convergence and integration of IT and OT (systems and data) is the cornerstone for realizing these revolutionary changes; the digital ecosystem is being transformed, a hybrid multicloud IT architecture is being created, smart factories and cities are established. It is clear that advanced mathematical methods of data collection and analysis play a very important role in this progress.

However, this revolutionary progress significantly changes and shifts the risks associated with the use of modern technologies and Industry 4.0 concepts [10]. The large interconnection and collection of data creates space for malicious cyber-attacks, we are witnessing pressure in the field of IoS, IoT [10], etc. Cyber-attacks make it possible to hit critical infrastructure (e.g. electricity supplies) and thus threaten operation of manufacturing companies, the functioning of the public sector, the financial sector, as well as the functioning of the state. In the current digital transformation to Industry 4.0, the demands on the ability of countries to respond responsibly and effectively to cyber security threats are increasing [11]. Cyber protection is one of the pillars of Industry 4.0 [12]. The cyber security sustainability and privacy protection in digital ecosystems is a prerequisite for ensuring the sustainability of production and industry, for economic, social, environmental and cultural sustainability, since modern IT technologies have penetrated into every substructure of the globally connected world [13].

Cyber security is also an integral part of the state's resistance to hybrid threats [14], which have become a significant challenge for sustainability of global security in the 21st century [14]. Many research studies and professional articles highlight the vulnerability of sustainability of modern societies, intelligent factories and cities to hybrid threats (HT) and tactics, by which it is possible to achieve objectives with minimal force and destroy preventive defensive actions [15]. As is discussed in many manuscripts and reviews, HT have multidimensional character. Within the last decade, it has been intensified by globalization [16], the sharp increase in the use of modern digital technologies in many areas of professional/personal life [17–19], demography [20], geopolitics [21] and interstate confrontations. The requirements and demands for increasing the state's sustainable stability and resistance to HT are currently on the rise, both worldwide [16] and within the individual countries of the European Union [22], as hybrid threats have the potential to cause devastating consequences in various areas of the state's functioning. The EU is taking important steps to improve its ability to face hybrid threats and is taking measures to strengthen resilience, including in the field of cyber security - as the authors report in [22], focusing mainly on the V4 countries. This topic focused on hybrid warfare/threats/campaigns receives a lot of attention in the professional literature, as it is a highly relevant problem [8] and rich discussions are held between the actors involved.

Cybersecurity [23] is often discussed, as it is one of the pillars on which the country's resistance to hybrid threats and attacks is currently being built. The development and adoption of network technologies is reshaping the daily life of both the individual and the state, which consequently increases the risk of cyber threats and attacks. Currently, new strategies for the detection of cyber security threats are actively being developed [24], attention is paid to this issue from several points of view [25]. Tsaruk et al. [26] explores the hybrid nature of threats to cyber and information security, including cyber attacks merged with conventional techniques. Bachmann et al. [27] focuses on cyber terrorism and war as hybrid threats, emphasizing the need for a comprehensive approach that combines law enforcement, counter cyber strategies, and kinetic responses. Galinec et al. [28] discusses the role of cyber security and cyber defense within the context of hybrid threats, proposing

the creation and performance of EU Cyber Rapid Response Teams (CRRTs) and Mutual Assistance in Cyber Security. In summary, these papers highlight the recognition of cyber security as an integral component of hybrid threats and the importance of comprehensive approaches and collaborative efforts to counter these threats.

The identification of cyber threats/attacks and the implementation of measures (adequate response to identified threats) aimed at maintaining cyber security took place in the past in a relatively stable digital environment. In today's global, even aggressively dynamic environment, the nature of cyber threats has gradually evolved into a complex combination of traditional and non-traditional elements. So in order to ensure a sustainable cyber ecosystem, it is necessary to identify, characterize and classify such threats in accordance with emerging trends (Internet of Things, smart cities, etc.) and solve it with new emerging techniques [29–30]. Based on above mentioned, a very difficult challenge was declared for the reaction of individuals, organizations and nations – to first and foremost insure the forward-looking sustain-ability of cybersecurity. To provide a sustainable and safe society to online users in cyberspace [31].

The ability to maintain effective cybersecurity measures and ensure cyber resilience over time depends not only on technological advances, but also on the complexity of risk perception from the level of the human factor, as is emphasized in [32]. Nam in [32] provide insights into the perception of the risk of threats to cyber security and investigates the relationships of various theoretical determinants of perceived threat and preparedness. The sustainability of cybersecurity and cyber resilience clearly depends on reactions of many societal actors [25], i.e. how individuals, factories, organisations, governments, citizens, clients of banks, students, etc., perceive the risks posed by hybrid threats [32]. The awareness of risks, the perception of them, is a principle prerequisite for the preparing and creating effective cybersecurity strategies that respond to the development of hybrid threats. Perception of the risk of threats to cyber security is a necessary condition for forming the correct attitudes of actors entering cyberspace, especially individuals as Internet users.

The attitudes of Internet users therefore depend on individual cognition and perception of cyber threats; moreover, not only cognitive assessment/evaluation of facts but also psychological factors play a key role in their formation. An individual's psychological reactions or fears (arising from uncertainty) determine the ability to assess risks and prevent future attacks. Larsen et al. in [33] highlights that cyber incidents are often caused by complex relationships between humans and technology; the humans can represent both a risk of cybersecurity threat and an important resource in strengthening the cybersecurity. In general, the behavior of the decision makers play a key role in preventing and handling cyber risks [34].

Despite the growing trend of cybersecurity issues, little research has been conducted on individual threat perception and cybersecurity preparedness and resilience. We perceive a lack of relevant research in the countries neighboring the state involved in the war conflict (Ukraine), specifically in the Slovak Republic and the Czech Republic. The scarcity of relevant research motivated us to approach the issue of threats to cyber security (state, factories, organization, etc.) from the point of view of the individual, specifically through the lens (perception) of the respondents involved in the research. Later, based on the obtained results, it is possible to direct the education and shaping of the attitudes of future actors entering the cyber space. Specifically, in this case, it concerns students from various universities/faculties in the Slovak Republic and the Czech Republic, taking into account the common past of these two countries and the fact that this group of respondents will represent the first line of the fight against hybrid threats in the future.

The aim of the authors of this article and the research carried out through a research tool of their own construction (questionnaire) was first of all to create/develop a basic theoretical model of factors (determinants) influencing cyber security (Factor Model of Cyber Security - FMCS). Within the framework of the study, the authors seek answers to these research questions: (i) What is the relationship between the basic defined pillars of Cyber

Security and the basic demographic indicators of the research sample? In other words: Which defined pillars (determinants) of cyber security are perceived as important and significant from the point of view of risk? (ii) Are there differences between the analyzed groups of respondents in the perception of the seriousness of the threat to the state (cyber security)? (iii) Are there differences in risk perception between respondents from Slovakia and the Czech Republic?

The research questions deal with relationships that have not yet been considered in the relevant literature and the FMCS created by the authors represents a contribution in the subject research issue. To resolve these questions, the study uses data obtained by the questionnaire (more detailed in sub-chapter 2.2) addressed to respondents in Slovak Republic and Czech Republic during 2023. Within this questionnaire, the basic pillars of CS threats and their sub-pillars were defined on the basis of brainstorming session of 15 specialists (more detailed in sub-chapter 2.2). The evaluation and analysis of the obtained data is based on the application of structural equation modelling method (SEM) and confirmatory factor analysis. Mathematical modeling using structural equations finds its application first in psychological research (in psychometrics), gradually the range of SEM applications expands: marketing, strategic management, organizational research, management information systems, and operational management [35]. Currently, the SEM is successfully used in logistics controlling [36Wallenburg], operational management [35], in economics and finance [37] and many others [38]. One of the disadvantages of SEM is that it cannot test the direction of the relationships between variables [39], however this was not necessary in the research described.

This article is further structured into five sections, including the above introduction. Section 2 presents the research sample (description of the research set), the research tool and the applied methods. Section 3 discusses the achieved results (developed factor model) and presents the results of statistical data analysis. Section 4 analyzes and discusses the comparison of results in the Slovak Republic and the Czech Republic and brings some suggestions. Finally, Section 5 concludes this study by summarizing the most relevant findings, outlines the limitations of the paper, and provide future research direction.

2. Research Data, Research Tool and Methodology

2.1. The Research Sample

Research focused on the perception of the risk of cybersecurity threat was carried out from February 2023 to July 2023 using the research instrument, i.e. the questionnaire constructed by authors. The purpose of the research was to determine the subjective level of perception of the importance and risk of cybersecurity threats in relation to the threat in the Slovak Republic and the Czech Republic. A technique developed for measuring attitudes in questionnaires by American psychologist Rensis Likert was used for the evaluation. The research instrument was distributed to the respondents – university students – in electronic form and was implemented based on availability. The research group consists of a total of $N = 964$ respondents and in terms of structure was comprised of 521 (54.046%) men and 443 (45.954%) women from two countries. A total of 580 (60.166%) respondents were from Slovakia, and 384 (39.834%) were from the Czech Republic. The average age of the respondents was 26.03 ± 0.51 years, with a standard deviation of 8.145 years. The minimum age of the respondents was 19 years and the maximum age was 63 years. The age of the respondents was also analysed as an ordinal variable, and a total of 669 (69.398%) respondents were under the age of 25, 156 (16.183%) were 26–35 years old, 95 (9.855%) were aged 36–45, 41 were of age 46–55 years (4.253%), and 3 were older than 55 (0.311%). Out of the 964 respondents, 321 (33.299%) are studying at the bachelor's degree level, 591 (61.307%) at the master's degree level and 52 (5.394%) at the doctoral degree level, while 592 (61.411%) were full-time and 372 were part-time (38.589%) students. A more detailed breakdown of the research sample in terms of country, gender and age is provided in Table 1.

Table 1. Basic description of the research sample in terms of country, gender and age of the respondent.

| <i>N</i> = 964 | <i>COUNT</i> | <i>GEN</i> | <i>AGE1</i> < 25 years | <i>AGE1</i> 26 – 35 years | <i>AGE1</i> 36 – 45 years | <i>AGE1</i> 46 – 55 years | <i>AGE1</i> > 55 years | Row Totals |
|----------------------|--------------|------------|---------------------------|------------------------------|------------------------------|------------------------------|---------------------------|---------------|
| Count | SK | male | 135 | 60 | 34 | 4 | 0 | 233 |
| Column Percent | | | 34.62% | 54.05% | 54.84% | 23.53% | | |
| Row Percent | | | 57.94% | 25.75% | 14.59% | 1.72% | 0.00% | |
| Table Percent | | | 23.28% | 10.34% | 5.86% | 0.69% | 0.00% | 40.17% |
| Count | SK | female | 255 | 51 | 28 | 13 | 0 | 347 |
| Column Percent | | | 65.38% | 45.95% | 45.16% | 76.47% | | |
| Row Percent | | | 73.49% | 14.70% | 8.07% | 3.75% | 0.00% | |
| Table Percent | | | 43.97% | 8.79% | 4.83% | 2.24% | 0.00% | 59.83% |
| Count | Total | | 390 | 111 | 62 | 17 | 0 | 580 |
| Table Percent | | | 67,24% | 19.14% | 10.69% | 2.93% | 0.00% | 100.00% |
| Count | CZ | male | 213 | 39 | 24 | 12 | 0 | 288 |
| Column Percent | | | 76.34% | 86.67% | 72.73% | 50.00% | 0.00% | |
| Row Percent | | | 73.96% | 13.54% | 8.33% | 4.17% | 0.00% | |
| Table Percent | | | 55.47% | 10.16% | 6.25% | 3.13% | 0.00% | 75.00% |
| Count | CZ | female | 66 | 6 | 9 | 12 | 3 | 96 |
| Column Percent | | | 23.66% | 13.33% | 27.27% | 50.00% | 100.00% | |
| Row Percent | | | 68.75% | 6.25% | 9.38% | 12.50% | 3.13% | |
| Table Percent | | | 17.19% | 1.56% | 2.34% | 3.13% | 0.78% | 25.00% |
| Count | Total | | 279 | 45 | 33 | 24 | 3 | 384 |
| Table Percent | | | 72,66% | 11.72% | 8.59% | 6.25% | 0.78% | 100.00% |

* *COUNT* – country, *GEN* – gender, *AGE1* – age (on a numerical scale).

2.2. The Research Tool

The questionnaire, consisting of 39 items, was constructed based on brainstorming session of 15 specialists in mathematical modeling, hybrid threats and psychology (the Academy of the Police Force in Bratislava, the University of Prešov, the University of Defense in Brno and the Technical University of Košice). The questionnaire was addressed to the respondents in electronic form (Google form) as a part of the research conducted on the perception of Cybersecurity Risk as one of the pillars of hybrid threats. Before starting to fill in, the students were familiarized with the purpose and content of the research, as well as with the manner in which the obtained data will be handled. By starting to fill in, the respondents confirmed their consent to the anonymous use of their responses for the research purpose. The research itself was conducted as a part of the solution to the project "In-creasing Slovakia's resilience to hybrid threats by strengthening public administration capacities". The measurement is based on the subjective perception of the level of risk of individual items, while respondents chose answers on a 5-point Likert scale: 1 – no risk, 2 – low risk, 3 – medium risk, 4 – high risk, 5 – critical risk. The research instrument itself was divided into five basic areas of cybersecurity, so the basic 5 pillars of CS threats and their sub-pillars (39) were defined:

1. Cyber spying (*CYBSPY*) – 9 items (sub-pillars);
2. Disrupting or reducing IT infrastructure resilience (*DISRIT*) – 12 items;
3. Enemy campaigns (*ENECAM*) – 5 item;
4. Disrupting or reducing eGovernment security (*DISREG*) – 6 items;

5. Cyberterrorism (CYBTER) – 7 items.

Each of the five defined areas of cybersecurity were assigned statements with which the respondents expressed their subjective perception of the degree of risk. Given the relatively extensive nature of these items, we will mention them only during the actual analysis of the obtained data.

The reliability of the entire research instrument, defined by Cronbach's alpha, achieved a value of 0.95047. This fact shows that the error component of the measurement variance is relatively low and the sub-items of the research instrument are internally consistent; that is, there is a high degree of agreement between the items of the research instrument in the sense that they reflect equally well the a certain phenomenon, in our case cybersecurity. If we analyse the individual defined areas of cybersecurity from the point of view of reliability, then the value of Cronbach's alpha reaches 0.817930 for the area of Cyber spying (CYBSPY), 0.882338 for the area of Disrupting or reducing IT infrastructure resilience (DISRIT), 0.743745 for the area of Enemy campaigns (ENECAM), 0.839804 for the field Disrupting or reducing eGovernment security (DISREG), and 0.846028 for the field Cyberterrorism (CYBTER). On the basis of the presented values, we can conclude that even the individual defined areas show a high degree of internal consistency; therefore, it is possible to proceed with the further analysis of the research instrument.

For an analysis of the research instrument itself, confirmatory factor analysis was selected as one of the structural equation modelling (SEM) tools. The reason for choosing this method was a predefined hypothetical structure in the form of a factor model. The basic logic and mathematics of factor analysis were developed in the early 20th century to test theories about the nature of intelligence [34], making factor analysis one of the oldest statistical techniques for discovering and describing latent variables that were originally given only by sample covariance among a set of indicators [40]. Factor analysis is still widely used today and is also the primary technique for many researchers, especially those performing measurement-related studies. Common variance is shared among the indicators and is the basis for the observed covariances between them, which significantly differ from zero. In factor analysis, it is generally assumed that (1) common variance is caused by the factors and (2) the number of factors of substantial interest is less than the number of indicators. Based on these assumptions, it is not possible to estimate more factors than indicators, but in the interest of reduction, it makes no sense to maintain a model with the same number of explanatory entities (factors) that need to be explained (indicators) [41].

In general, there are two broad categories of factor analysis: exploratory factor analysis (EFA) and confirmatory factor analysis (CFA). The differences between these two methods are as follows:

1. The EFA method does not require a priori specification of the number of factors. Without a specific instruction (the exact determination of the number of factors), the EFA computer process could theoretically generate all potential solutions, from a one-factor model to a model with as many factors as there are indicators. In some computer based EFA processes, the researcher may optionally request a solution with a certain number of factors, and the algorithm will only analyse this specific model. But in CFA, the researcher must always present the exact number of factors of the analysed model.
2. In EFA, no possibility exists to specify the exact correspondence between indicators and factors. This means that indicators can depend on (theoretically) all the factors; thus, unconstrained EFA measurement models are analysed. However, in CFA, each indicator can depend only on the factor (factors) which is specified by the researchers in the defined theoretical model; i.e. in confirmatory analysis constrained measurement models are analysed.
3. Models with multiple factors are not really identified in EFA, because such models have more free parameters than observations. That is, there is no unique set of

statistical estimates of parameters for a particular multifactor EFA model. This relates to the factor rotation phase in exploratory factor analysis. In contrast to this, CFA models must be identified before they are analysed, so that only one exclusive set of parameter estimates exist. In line with this statement, confirmatory factor analysis does not have a factor rotation phase.

4. In general, in EFA it is assumed that the specific variance of each indicator is not shared with any other indicator, but the confirmatory factor analysis procedure allows, depending on the model, an estimate of whether a specific indicator variance is shared between certain pairs of indicators (i.e., error correlations).

2.3. Methodology

On the basis of the above basic information for the analysis of the acquired data and the assumptions that were made within the framework of the theoretical model, confirmatory factor analysis, as one of the structural equation modelling tools, seems to be the most suitable method.

One of the important assumptions associated with structural equation modelling (SEM) when analysing covariance and mean structures is the requirement that the data be continuous and have a multidimensional normal distribution. The requirement of continuity is also fulfilled for ordinal variables, if we start from the research results of Rhemtulla and Xia [42, 43], which also accept the application of classic cut-off estimators via the maximum likelihood (ML) method in the case of ordinal variables, if they have at least 5 response categories, when they can be considered as interval variables. These fundamental assumptions are connected to the theory of large samples in which SEM is incorporated. Stated more precisely, they are derived from the approach used in parameter estimation by means of the SEM methodology, usually either the ML method or a method based on the theory of generalised least squares (GLS) estimation.

3. The Model and Results of Statistical Analysis

3.1. The Model of Cybersecurity

The fundamental theoretical, hypothetical model of Cybersecurity (FMCS), as one of the pillars of hybrid threats, is shown in Figure 1. The factor model itself is comprised of 39 endogenous variables which represent the items of the research instrument, where the respondents assigned the level of risk for individual items on a Likert scale ranging from 1 (no risk) to 5 (critical risk). The second component of the factor model is unobserved; these are exogenous variables that represent the partial pillars of Cybersecurity (CYBSPY, DISRIT, ENECAM, DISREG, CYBTER).

Certain assumptions defined by basic statistical indicators are made about factor models analysed using CFA. In the first step, we defined a hypothetical data structure – factors, manifest variables and relationships between them – based on the theoretical construct and the results of foreign studies. We used the following procedures and indices to test the appropriateness of the verified model: chi-square statistics and the following overall indices of agreement with optimal values: ($\chi^2/df < 2$, $RMSEA < 0.08$, comparative index $TLI > 0.90$, $CFI > 0.90$, $SRMR < 0.08$) and sub-indexes (statistical significance of model parameters). The CFI and TLI indices can take on values from 0 to 1, and values higher than 0.90 indicate the appropriateness of the applied model. The $RMSEA$ index – the root mean square error of approximation – is lower than 0.08 for good models, and if the value is above 0.1, the model should be rejected. The chi-square test takes into consideration the ratio of the chi-square and the number of degrees of freedom. The ideal chi-square is approximated by the size from the number of degrees of freedom, and with multiple models, the one with the lowest chi-square is considered to be more appropriate. In good models, the chi-square is statistically insignificant, but this is seen as a rather strict criterion, especially for larger samples.

The basic recommended evaluation indicators [44] and their realistically achieved values on the applied 5-factor model of Cybersecurity are shown in Table 2.

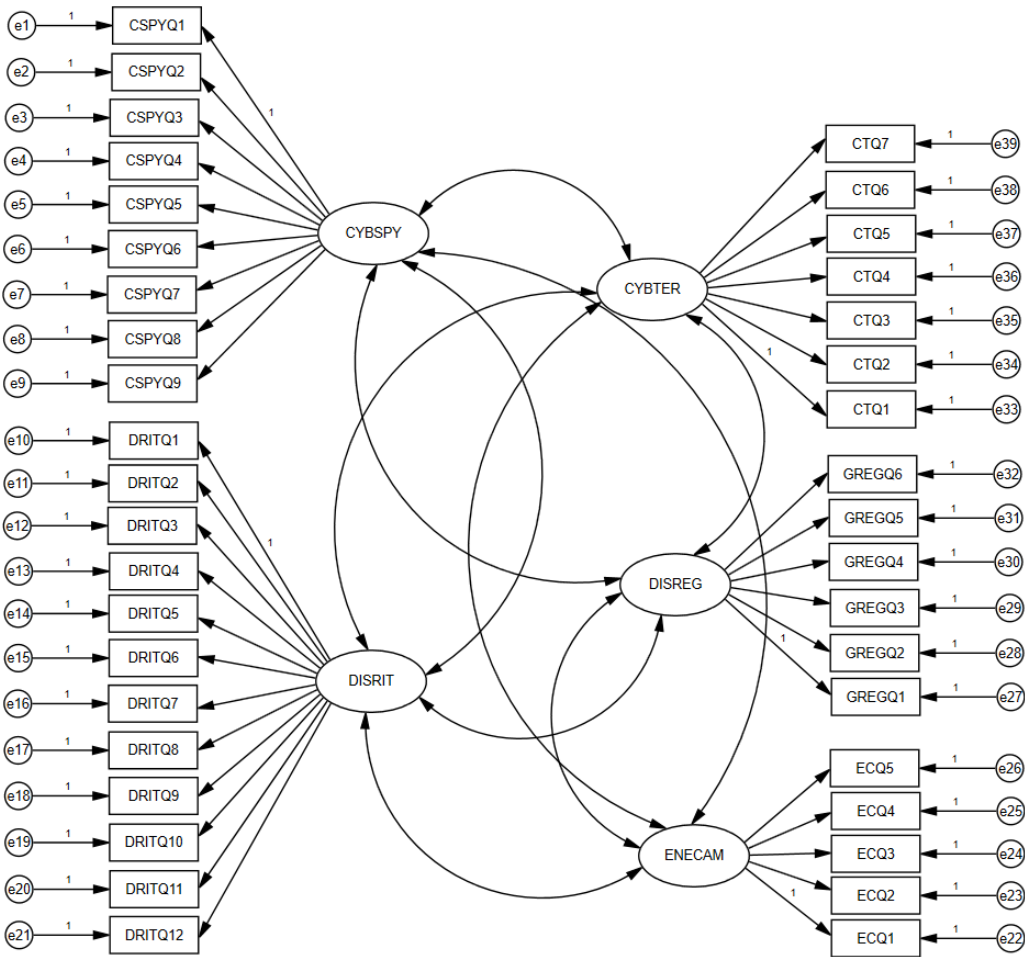


Figure 1. Theoretical factor model of Cybersecurity (FMSC) threat risk perception.

Table 2. Evaluation criteria of the fundamental factor model of cybersecurity.

| Fit Indices Used | Perfect Fit Indices | Acceptable Fit Indices | CFA Results | References |
|------------------|-----------------------------|-----------------------------|-------------|------------------------|
| χ^2/df | $0 \leq \chi^2/df \leq 2$ | $2 \leq \chi^2/df \leq 3$ | 1.085 | [45] |
| GFI | $0.95 \leq GFI \leq 1.00$ | $0.90 \leq GFI \leq 0.95$ | 0.974 | [46], [47], [48] |
| AGFI | $0.90 \leq AGFI \leq 1.00$ | $0.85 \leq AGFI \leq 0.90$ | 0.957 | |
| CFI | $0.95 \leq CFI \leq 1.00$ | $0.90 \leq CFI \leq 0.95$ | 0.998 | |
| NFI | $0.95 \leq NFI \leq 1.00$ | $0.90 \leq NFI \leq 0.95$ | 0.971 | [49], [50], [51] |
| TLI | $0.97 \leq TLI \leq 1.00$ | $0.95 \leq TLI \leq 0.97$ | 0.996 | |
| RMSEA | $0.00 \leq RMSEA \leq 0.05$ | $0.05 \leq RMSEA \leq 0.08$ | 0.009 | [45], [48], [52], [53] |
| SRMR | $0.00 \leq SRMR \leq 0.05$ | $0.05 \leq SRMR \leq 0.10$ | 0.0196 | |
| p | $p > 0.05$ | | 0.098 | |

Note: χ^2 – Chi-square, df – Degrees of freedom, GFI – Goodness of fit index, AGFI – Adjusted goodness of fit index, CFI – Comparative fit index, NFI – The Bentler-Bonett normed fit index, TLI – Tucker-Lewis coefficient, RMSEA – Root mean square error of approximation, SRMR – Standardised root mean square residual.

Based on the results shown in Table 2, it can be concluded that all the applied evaluation criteria for the suitability of the theoretical factor model (Figure 1) are within the required intervals and authorise us to state that the hypothetical model created presents a good degree of agreement with real data and is applicable in this form. Other indicators are $\chi^2 = 507.962$, $df = 468$, $p = 0.098$.

3.2. The Results of Statistical Analysis

We provide the analysis of the 5-factor model of Cybersecurity (Figure 1) for the entire research set ($N = 964$) itself in individual tables (Table 3 to Table 7). The first conclusion of the analysis presented in Table 3 to Table 7 is the fact that all items of the research instrument significantly influence the individual defined pillars of Cybersecurity at the selected level of significance of $\alpha = 0.05$. In the next step, we provide the analysis of the individual pillars of Cybersecurity separately.

3.2.1. Cyber spying (CYBSPY)

The first defined pillar is the exogenous variable CYBSPY (Cyber spying). Cyber spying comprises a total of 9 items of the research instrument (Table 3). Respondents assigned the lowest level of risk (low risk) in comparison with the other items to the item CSPYQ3, with a value of the standardised regression weight at the level of 0.295 ($p < 0.001$). The respondents therefore do not consider the resolution of cybersecurity through outsourcing to be a significant risk in the field of cyber spying.

Table 3. Estimates of the parameters of the Cyber spying pillar for the entire research set ($N = 964$).

| Relationship | | | Estimate | Std. Estimate | Std. error | <i>t</i> – statistic | <i>p</i> – value |
|---------------|----|---------------|----------|---------------|------------|----------------------|------------------|
| <i>CSPYQ1</i> | <— | <i>CYBSPY</i> | 1.000 | 0.620 | 0.062 | 15.214 | < 0.001* |
| <i>CSPYQ2</i> | <— | <i>CYBSPY</i> | 0.865 | 0.541 | 0.065 | 13.377 | < 0.001* |
| <i>CSPYQ3</i> | <— | <i>CYBSPY</i> | 0.430 | 0.295 | 0.051 | 8.448 | < 0.001* |
| <i>CSPYQ4</i> | <— | <i>CYBSPY</i> | 1.112 | 0.635 | 0.070 | 15.954 | < 0.001* |
| <i>CSPYQ5</i> | <— | <i>CYBSPY</i> | 1.135 | 0.658 | 0.074 | 15.289 | < 0.001* |
| <i>CSPYQ6</i> | <— | <i>CYBSPY</i> | 1.108 | 0.608 | 0.077 | 14.448 | < 0.001* |
| <i>CSPYQ7</i> | <— | <i>CYBSPY</i> | 1.142 | 0.643 | 0.079 | 14.471 | < 0.001* |
| <i>CSPYQ8</i> | <— | <i>CYBSPY</i> | 1.154 | 0.650 | 0.076 | 15.210 | < 0.001* |
| <i>CSPYQ9</i> | <— | <i>CYBSPY</i> | 1.017 | 0.564 | 0.075 | 13.560 | < 0.001* |

* – significant at the level of significance $\alpha = 0.05$, Estimate – regression weight, Std. Estimate – standardised regression weight, Std. error – standard error, *t* – *t*-statistic, *p* – probability level, CYBSPY – Cyber spying.

In contrast, the most significant item of the research instrument in terms of the risk of cyber spying is item CSPYQ5 (Inappropriately set and applied cybersecurity policies) with a standardised regression weight value of 0.658 ($p < 0.001$). It is followed by item CSPYQ8 (Purchase of ICT through insufficiently verified intermediaries and without knowledge of the product chain) with a value of the standardised regression weight of 0.650 ($p < 0.001$). The third most significant item of the research instrument that affects cyber spying is the item CSPYQ7 (0.643, $p < 0.001$), which relates to insufficient training of employees in the field of cybersecurity. Other items of the research instrument that make up Cybersecurity and to which the respondents assigned a high level of risk (*Std. Estimate* > 0.600) are the next items. Item CSPYQ4 (0.635, $p < 0.001$), which states that cybersecurity is not solved comprehensively, but only operationally; item CSPYQ1 (0.620, $p < 0.001$), which relates to the issue of insufficient allocation of finances to the issue of cybersecurity; and item CSPYQ6 (0.608, $p < 0.001$), which is devoted to the issue of insufficient screening of employees.

Respondents assigned a medium level of risk to the fact that sensitive information is exposed to the risk of unauthorised use due to the use of private resources (PC, phone, tablet) for work purposes, represented by item *CSPYQ9* (0.564, $p < 0.001$). Medium level of risk was also assigned to the fact that some ICT manufacturers and suppliers have ties to the governments and security forces of other states. This fact is represented in the research instrument by item labelled *CSPYQ2*, with a standardised regression weight of 0.541 ($p < 0.001$).

3.2.2. Disrupting or reducing IT infrastructure resilience (*DISRIT*)

The second pillar of Cybersecurity per the factor model (Figure 1) is the pillar called Disrupting or reducing IT infrastructure resilience (*DISRIT*), the basic analysis of which is presented in Table 4. The *DISRIT* pillar itself is made up of 12 items of the research instrument, and as many as 9 of them were assigned a high level of risk by the respondents (*Std. Estimate* > 0.600).

Table 4. Estimates of parameters of the pillar Disrupting or reducing IT infrastructure resilience for the entire research set ($N = 964$).

| | Relationship | | Estimate | Std. Estimate | Std. Error | <i>t</i> – statistic | <i>p</i> – value |
|----------------|--------------|---------------|----------|---------------|------------|----------------------|------------------|
| <i>DRITQ1</i> | <--- | <i>DISRIT</i> | 1.000 | 0.669 | 0.072 | 16.216 | < 0.001* |
| <i>DRITQ2</i> | <--- | <i>DISRIT</i> | 0.951 | 0.661 | 0.051 | 18.490 | < 0.001* |
| <i>DRITQ3</i> | <--- | <i>DISRIT</i> | 0.892 | 0.627 | 0.050 | 17.839 | < 0.001* |
| <i>DRITQ4</i> | <--- | <i>DISRIT</i> | 0.931 | 0.582 | 0.059 | 15.697 | < 0.001* |
| <i>DRITQ5</i> | <--- | <i>DISRIT</i> | 0.922 | 0.645 | 0.056 | 16.556 | < 0.001* |
| <i>DRITQ6</i> | <--- | <i>DISRIT</i> | 0.741 | 0.517 | 0.050 | 14.898 | < 0.001* |
| <i>DRITQ7</i> | <--- | <i>DISRIT</i> | 0.923 | 0.618 | 0.057 | 16.066 | < 0.001* |
| <i>DRITQ8</i> | <--- | <i>DISRIT</i> | 0.937 | 0.613 | 0.054 | 17.313 | < 0.001* |
| <i>DRITQ9</i> | <--- | <i>DISRIT</i> | 0.931 | 0.583 | 0.056 | 16.556 | < 0.001* |
| <i>DRITQ10</i> | <--- | <i>DISRIT</i> | 1.048 | 0.679 | 0.055 | 19.136 | < 0.001* |
| <i>DRITQ11</i> | <--- | <i>DISRIT</i> | 0.956 | 0.656 | 0.055 | 17.224 | < 0.001* |
| <i>DRITQ12</i> | <--- | <i>DISRIT</i> | 0.928 | 0.622 | 0.053 | 17.420 | < 0.001* |

* – significant at the level of significance $\alpha = 0.05$, Estimate – regression weight, Std. Estimate – standardised regression weight, Std. Error – standard error, *t* – *t*-statistic, *p* – probability level, *DISRIT* – Disrupting or reducing IT infrastructure resilience.

The most significant item with a high level of risk is item *DRITQ10*, which relates to the issue of the fragmentation of systems of communication resources in state/public administration, which does not enable adequate effective use of maintenance, security and control in real time, with a value of the standardised regression weight of 0.679 ($p < 0.001$), followed by item *DRITQ1*, which relates to the risk of critical information infrastructure being attacked by cyber attacks (0.669, $p < 0.001$) with an equally high level of risk. According to the importance of research instrument items represented by the standardised regression weight, the third risk according to the respondents is item *DRITQ2*, which is devoted to the insufficient funds for providing the necessary technical courses and hiring security-vetted experts in ICT and cybersecurity, with a standardised regression weight value of 0.661 ($p < 0.001$). The research instrument items to which the respondents assigned a high level of risk, as in the previous cases, are: *DRITQ11* (Lack of central methodologies for using computing equipment, especially mobile devices), *DRITQ5* (Non-systematically implemented security testing), *DRITQ3* (Strategic industrial branches are not included in critical infrastructure, and their selected information systems therefore cannot be included in critical information infrastructure), *DRITQ12* (Absence of an obligation for secured (commercially encrypted) email and other electronic communication by

interstate/public institutions and state/public administration workers), *DRITQ7* (Incorrect prioritising of some departments and institution when planning investment in security technologies and other ICT) and *DRITQ8* (Insufficient legislative regulation of cyber-crime). From the point of view of a high level of risk, the priority issue for the analysed Cybersecurity pillar is above all technical security and the method of its provision. In the respondents' opinion, the insufficient allocation of resources to this area as well as the absence of legislation in the field of cybersecurity are of no small importance. Respondents assigned a medium level of risk to research instrument item *DRITQ9* of the analysed Cybersecurity pillar, which relates to the use of outdated information infrastructure systems, and the standardised regression weight was at 0.583 ($p < 0.001$), followed by item *DRITQ4* (Employees of the state/public administration do not have sufficient cybersecurity awareness) with a standardised regression weight value of 0.582 ($p < 0.001$) and item *DRITQ6*, which gives priority to the possibilities of attacks on information infrastructure through the production, supply and subcontractor chain (0.517, $p < 0.001$).

3.2.3. Enemy Campaigns

The third pillar of Cybersecurity according to the theoretical factor model (Figure 1), defined as Enemy campaigns (*ENECAM*), is analysed in Table 5. On the basis of the CFA results, it can be stated that the respondents ($N = 964$) assigned the highest level of risk (at the level high risk) to research instrument item *ECQ3*, with the value of the standardised regression weight of 0.677 ($p < 0.001$). This item relates to the ownership structure of individual Internet media, which may follow various private interests or the interests of other states in their behaviour. The second most significant item with a high level of risk is item *ECQ4*, which looks at insufficient vetting of state/public administration employees who may work for third parties. The standardised regression weight of item *ECQ4* is 0.641 ($p < 0.001$). The last research instrument item from the Enemy campaigns pillar to which respondents assigned a high level of risk, is item *ECQ1*, which relates to the issue of possible social unrest caused by hostile campaigns (0.622, $p < 0.001$). Respondents within the Enemy campaigns pillar assigned a medium level of risk to item *ECQ5* (Current legislation on free access to information, which may threaten cybersecurity or can be misused within information campaigns), with the standardised regression weight of 0.553 ($p < 0.001$), and item *ECQ2* (Wide use of the social network environment due to their international aspect and different approach to freedom of speech, which makes it possible to use them to a greater extent to spread hate and disinformation campaigns), with the standardised regression weight at 0.531 ($p < 0.001$). Here it can be noticed that a relatively dangerous tendency exists towards the possibility of limiting the freedom of speech given the possibility of spreading enemy campaigns in order to minimise their risk.

Table 5. Estimates of the parameters of the Enemy campaigns pillar for the entire research set ($N = 964$).

| Relationship | | | Estimate | Std. Estimate | Std. error | <i>t</i> -statistic | <i>p</i> -value |
|--------------|------|---------------|----------|---------------|------------|---------------------|-----------------|
| <i>ECQ1</i> | <--- | <i>ENECAM</i> | 1.000 | 0.622 | 0.061 | 15.834 | < 0.001* |
| <i>ECQ2</i> | <--- | <i>ENECAM</i> | 0.827 | 0.531 | 0.052 | 16.050 | < 0.001* |
| <i>ECQ3</i> | <--- | <i>ENECAM</i> | 1.012 | 0.677 | 0.063 | 16.021 | < 0.001* |
| <i>ECQ4</i> | <--- | <i>ENECAM</i> | 0.991 | 0.641 | 0.063 | 15.690 | < 0.001* |
| <i>ECQ5</i> | <--- | <i>ENECAM</i> | 0.850 | 0.553 | 0.063 | 13.445 | < 0.001* |

* – significant at the level of significance $\alpha = 0.05$, Estimate – regression weight, Std. Estimate – standardised regression weight, Std. Error – standard error, *t* – *t*-statistic, *p* – probability level, *ENECAM* – Enemy campaigns

3.2.4. Disrupting or reducing eGovernment security

The analysis results of the fourth pillar of Cyber threats according to the model defined in Figure 1, the pillar labelled Disrupting or reducing eGovernment security (*DISREG*), are shown in Table 6.

Table 6. Estimates of parameters of the pillar Disrupting or reducing eGovernment security for the entire research set ($N = 964$).

| | Relationship | | Estimate | Std. Estimate | Std. error | <i>t</i> -statistic | <i>p</i> -value |
|---------------|--------------|---------------|----------|---------------|------------|---------------------|-----------------|
| <i>GREGQ1</i> | <--- | <i>DISREG</i> | 1.000 | 0.666 | 0.056 | 19.662 | < 0.001* |
| <i>GREGQ2</i> | <--- | <i>DISREG</i> | 1.059 | 0.707 | 0.052 | 20.282 | < 0.001* |
| <i>GREGQ3</i> | <--- | <i>DISREG</i> | 1.121 | 0.741 | 0.056 | 19.839 | < 0.001* |
| <i>GREGQ4</i> | <--- | <i>DISREG</i> | 0.996 | 0.721 | 0.051 | 19.397 | < 0.001* |
| <i>GREGQ5</i> | <--- | <i>DISREG</i> | 1.060 | 0.716 | 0.055 | 19.415 | < 0.001* |
| <i>GREGQ6</i> | <--- | <i>DISREG</i> | 0.939 | 0.624 | 0.063 | 14.890 | < 0.001* |

* – significant at the level of significance $\alpha = 0.05$, Estimate – regression weight, Std. Estimate – standardised regression weight, Std. Error – standard error, *t* – *t*-statistic, *p* – probability level, *DISREG* – Disrupting or reducing e-government security.

Compared to the other defined pillars, the value of the standardised regression weight is greater than 0.700 for the majority of the research instrument items that make up this pillar (Figure 1), which is still a high risk in terms of the risk level. The most significant research instrument item of the *DISREG* pillar is item *GREGQ3*, which relates to the issue of Insufficient security of information and cyber systems of state/public administration, which serve to communicate between citizens and the state, with a standardised regression weight of 0.741 ($p < 0.001$). The second largest problem according to the respondents, with a standardised regression weight of 0.721 ($p < 0.001$), is item *GREGQ4*, which is devoted to the issue of Poor setting of the cybersecurity policy at the state level, followed by item *GREGQ5* Insufficient education of state/public administration employees regarding cybersecurity (0.716, $p < 0.001$) and item *GREGQ2* (Underestimating cyber threats in state/public administration) (0.707, $p < 0.001$). From the viewpoint of this first group of threats within the *DISREG* pillar, the most significant according to the respondents is the insufficient security of the information systems, the poor setting of the security policy, the insufficient training of employees and the underestimating of cyber threats. The common denominator of these risks is the policy of the state itself in this critical area, which, from the respondents' point of view is insufficient and is not given adequate attention. The second group of risks which still represent a high risk are: *GREGQ1* (Insufficient financing of cybersecurity and insufficient financial assessment of workers in the field of cybersecurity) with a standardised regression weight of 0.666 ($p < 0.001$) and *GREGQ6* (Low level of awareness and education of the population on cybersecurity), where the value of the standardised regression weight is 0.624 ($p < 0.001$). In this group of risks, the dominant problem, of course, is the financing of the issue of cybersecurity and the very awareness of the low level of awareness about cybersecurity. This research instrument item (*GREGQ6*) is in a way complementary to item *GREGQ5*. On the one hand, there is an assumption that employees do not have sufficient awareness and education about the issue of cybersecurity; on the other hand, however, our respondents think adequate education in this area is not provided by the state. Therefore, here space is created for the removing of these combined risks by the state.

3.2.5. Cyberterrorism

The analysis of the last (the fifth) pillar of Cyber Threats (Figure 1), namely Cyberterrorism (*CYBTERR*), is presented in Table 7. The respondents identified item *CTQ6* of the research instrument, which relates to the possibility of managing sympathisers by third parties primarily by inducing their activity against possible targets, planning terrorist

operations, providing feedback, etc., as the most significant high-level risk. The value of the standardised regression weight of this item is 0.730 ($p < 0.001$). The second most significant issue according to the research sample is item *CTQ4*, with a standardised regression weight value of 0.705 ($p < 0.001$), which concerns the possibility of obtaining sensitive information of an intelligence nature for the purpose of using it in a kinetic terrorist attack (selection of specific targets, etc.). This first group of risks, which is, however, the most significant according to the respondents, primarily concerns risks associated with information as such and its potential misuse. The second group of threats that the respondents assigned a high level of risk to are research instrument item *CTQ5* (Spreading propaganda and materials to support followers of radicalisation and their recruitment) with a value of the standardised regression weight of 0.677 ($p < 0.001$) and item *CTQ7* (Low preparedness of the security forces for the specific digital environment and action in it) with a regression weight value of 0.619 ($p < 0.001$). The respondents assigned a medium level of risk to items *CTQ3* (Energy blackout), *CTQ1* (Blackmail of state authorities, business corporations or intimidation of the company) and *CTQ2* (Destruction of specific technology (information, production, operation)), which already have the character of a specific terrorist activity using cyber and computer systems. Of genuine interest is that the respondents attach a lower measure of risk to a specific possible consequence of cyberterrorism, such as the shutdown of electricity distribution, than to the misuse of information for management and terrorist purposes.

Table 7. Estimates of the parameters of the pillar Cyberterrorism for the entire research set ($N = 964$).

| | Relationship | | Estimate | Std. Estimate | Std. error | <i>t</i> -statistic | <i>p</i> -value |
|-------------|--------------|---------------|----------|---------------|------------|---------------------|-----------------|
| <i>CTQ1</i> | <--- | <i>CYBTER</i> | 1.000 | 0.584 | 0.057 | 16.453 | < 0.001* |
| <i>CTQ2</i> | <--- | <i>CYBTER</i> | 0.992 | 0.570 | 0.058 | 17.054 | < 0.001* |
| <i>CTQ3</i> | <--- | <i>CYBTER</i> | 1.104 | 0.599 | 0.068 | 16.120 | < 0.001* |
| <i>CTQ4</i> | <--- | <i>CYBTER</i> | 1.196 | 0.705 | 0.072 | 16.542 | < 0.001* |
| <i>CTQ5</i> | <--- | <i>CYBTER</i> | 1.223 | 0.677 | 0.078 | 15.660 | < 0.001* |
| <i>CTQ6</i> | <--- | <i>CYBTER</i> | 1.296 | 0.730 | 0.076 | 16.990 | < 0.001* |
| <i>CTQ7</i> | <--- | <i>CYBTER</i> | 1.099 | 0.619 | 0.071 | 15.410 | < 0.001* |

* – significant at the level of significance $\alpha = 0.05$, Estimate – regression weight, Std. Estimate – standardised regression weight, Std. Error – standard error, *t* – *t*-statistic, *p* – probability level, *CYBTER* – Cyberterrorism.

It is undoubtedly necessary, however, to pay attention to the mutual links between the individual defined pillars of Cybersecurity (Figure 1). A basic analysis of these links in terms of the model shown in Figure 1 is provided in Table 8.

In terms of the statistical significance of mutual links between the individual defined pillars of Cybersecurity according to the theoretical factor model (Figure 1), all the links are significant at the selected level of significance $\alpha = 5\%$. However, we observe the highest value of the correlation coefficient between the *CYBSPY* pillar and the *DISRIT* pillar (0.909, $p < 0.001$). Therefore, it is clear that the respondents consider the problem of cyber spying and the disrupting or reducing the resilience of IT infrastructure to be the most significant complementary relationship. At the same time, it can be said that by increasing the risk of the *CYBSPY* pillar, the risk of the *DISRIT* cybersecurity pillar will also conditionally increase. The second most significant relationship in the view of the respondents is the link between the *DISRIT* and *DISREG* pillars (0.837, $p < 0.001$), followed by the relationship between the *CYBTER* and *ENECAM* pillars, with a correlation coefficient value of 0.815 ($p < 0.001$).

Table 8. Analysis of the relationships between the pillars of Cybersecurity for the entire research set ($N = 964$).

| Relationship | | | Covariance | | | | Correlation |
|--------------|------|--------|------------|------------|----------|----------|-------------|
| | | | Estimate | Std. error | t-static | p-value | Estimate |
| CYBSPY | <--> | CYBTER | 0.225 | 0.021 | 10.583 | < 0.000* | 0.708 |
| DISRIT | <--> | DISREG | 0.349 | 0.026 | 13.461 | < 0.000* | 0.837 |
| DISRIT | <--> | ENECAM | 0.295 | 0.025 | 11.847 | < 0.000* | 0.732 |
| CYBSPY | <--> | DISREG | 0.279 | 0.023 | 11.881 | < 0.000* | 0.769 |
| DISRIT | <--> | CYBTER | 0.281 | 0.024 | 11.794 | < 0.000* | 0.769 |
| CYBSPY | <--> | ENECAM | 0.251 | 0.022 | 11.337 | < 0.000* | 0.715 |
| CYBSPY | <--> | DISRIT | 0.317 | 0.025 | 12.913 | < 0.000* | 0.909 |
| DISREG | <--> | ENECAM | 0.328 | 0.027 | 12.346 | < 0.000* | 0.783 |
| CYBTER | <--> | ENECAM | 0.299 | 0.026 | 11.669 | < 0.000* | 0.815 |
| CYBTER | <--> | DISREG | 0.292 | 0.024 | 12.085 | < 0.000* | 0.771 |

* – significant at the level of significance $\alpha = 0.05$, Estimate – regression weight, Std. Estimate – standardised regression weight, Std. Error – standard error, t – t -statistic, p – probability level, CYBSY – Cyber spying, CYBTER – Cyberterrorism, DISRIT – Disrupting or reducing IT infrastructure resilience, ENECAM – Enemy campaigns, DISREG – Disrupting or reducing e-government security.

In contrast, respondents assigned the lowest level of importance, even though statistically significant in the sense of Cohen's scale, to the connection between CYBSY and CYBTER with the value of the correlation coefficient of 0.708 ($p < 0.001$). At the same time, if we analyse the importance of the individual pillars of Cyber threats, the respondents view the DISRIT pillar as the most important, with a share of 22.284%, followed by the DISREG pillar with a share of 21.842%. The ENECAM pillar achieves a 19.532% share, the CYBTER pillar an 18.381% share, and the last defined of the Cyber threats pillar, CYBSY, reaches a 17.961% share. These relatively balanced values of the shares of the individual pillars on the hybrid Cybersecurity threat indicate that the respondents perceive their risk in a relatively balanced way, and all pillars are at the same time statistically significant at the chosen level of significance.

4. Results and Discussion

After analysis of the factor theoretical model of the hybrid threat Cybersecurity for the entire research group ($N = 964$), we focus our analysis on the detection of differences in the perception of individual defined pillars of this hybrid threat between respondents from the Slovak and Czech Republics. It would certainly be interesting to observe such differences between other groups, too (gender, age, degree and form of study), but analysing these groups would make the study too extensive. The authors will focus on the analysis of these other groups and the differences in the perception of the individual defined pillars of the hybrid threat Cybersecurity in further planned studies.

4.1. Analysis of differences in perception of the pillars of Cybersecurity between students of the Slovakia and Czech Republic

Based on the theoretical factor model (Figure 1), we in the next round created partial models, especially for respondents from Slovakia ($N = 580$) and especially for respondents from the Czech Republic ($N = 384$). Based on Table 9, it can be said that both partial models of Cybersecurity in the sense of the defined criteria show high agreement with the data obtained using the author's research instrument and are therefore applicable for drawing correct conclusions.

Table 9. Assessment criteria of partial factor models of Cybersecurity for respondents from the Slovak Republic (SK) and Czech Republic (CZ).

| Fit Indices Used | Perfect Fit Indices | Acceptable Fit Indices | Results SK | Results CZ |
|---------------------|-----------------------------|-----------------------------|---------------|---------------|
| χ^2/df | $0 \leq \chi^2/df \leq 2$ | $2 \leq \chi^2/df \leq 3$ | 1.085 | 1.102 |
| GFI | $0.95 \leq GFI \leq 1.00$ | $0.90 \leq GFI \leq 0.95$ | 0.958 | 0.942 |
| AGFI | $0.90 \leq AGFI \leq 1.00$ | $0.85 \leq AGFI \leq 0.90$ | 0.932 | 0.897 |
| CFI | $0.95 \leq CFI \leq 1.00$ | $0.90 \leq CFI \leq 0.95$ | 0.997 | 0.993 |
| NFI | $0.95 \leq NFI \leq 1.00$ | $0.90 \leq NFI \leq 0.95$ | 0.960 | 0.933 |
| TLI | $0.97 \leq TLI \leq 1.00$ | $0.95 \leq TLI \leq 0.97$ | 0.995 | 0.988 |
| RMSEA | $0.00 \leq RMSEA \leq 0.05$ | $0.05 \leq RMSEA \leq 0.08$ | 0.012 | 0.016 |
| SRMR | $0.00 \leq SRMR \leq 0.05$ | $0.05 \leq SRMR \leq 0.10$ | 0.0238 | 0.0385 |
| p | $p > 0.05$ | | 0.093 | 0.068 |

χ^2 – Chi-square, df – Degrees of freedom, GFI – goodness of fit index, AGFI – adjusted goodness of fit index, CFI – comparative fit index, NFI – Bentler-Bonett normed fit index, TLI – Tucker-Lewis coefficient, RMSEA – root mean square error of approximation, SRMR – standardised root mean square residual, p – probability level, SK – Slovak Republic, CZ – Czech Republic.

The differences themselves in the perception of the individual defined pillars of Cybersecurity in terms of the theoretical factor model (Figure 1) between Slovak (SK) and Czech (CZ) respondents can be observed from two points of view. The first is the assigning of importance of the individual items of the research instrument; the second is the assigning the degree of risk of the individual items of the research instrument. More detailed differences in perception within the individual pillars of Cybersecurity are shown in Table 10 to Tab. 14, and in the analysis we focus only on the most important ones.

Table 10. Estimates of the parameters of the Cyber spying pillar for respondents from the Slovak and Czech Republics.

| Relationship | | | Slovak Republic | | | | Czech Republic | | | |
|--------------|------|--------|-----------------|-----------|--------|----------|----------------|-----------|-------|----------|
| | | | Est. | Std. Est. | t | p | Est. | Std. Est. | t | p |
| CSPYQ1 | <--- | CYBSPY | 1.000 | 0.637 | 13.521 | < 0.000* | 1.000 | 0.640 | 0.818 | < 0.000* |
| CSPYQ2 | <--- | CYBSPY | 0.862 | 0.583 | 12.385 | < 0.000* | 0.818 | 0.500 | 8.083 | < 0.000* |
| CSPYQ3 | <--- | CYBSPY | 0.496 | 0.361 | 8.237 | < 0.000* | 0.509 | 0.346 | 6.443 | < 0.000* |
| CSPYQ4 | <--- | CYBSPY | 1.073 | 0.638 | 14.841 | < 0.000* | 1.122 | 0.645 | 9.422 | < 0.000* |
| CSPYQ5 | <--- | CYBSPY | 1.159 | 0.709 | 14.684 | < 0.000* | 1.220 | 0.706 | 9.382 | < 0.000* |
| CSPYQ6 | <--- | CYBSPY | 1.045 | 0.651 | 13.573 | < 0.000* | 1.203 | 0.611 | 8.755 | < 0.000* |
| CSPYQ7 | <--- | CYBSPY | 1.111 | 0.667 | 13.976 | < 0.000* | 0.978 | 0.543 | 7.943 | < 0.000* |
| CSPYQ8 | <--- | CYBSPY | 1.064 | 0.621 | 13.340 | < 0.000* | 1.027 | 0.594 | 8.799 | < 0.000* |
| CSPYQ9 | <--- | CYBSPY | 1.056 | 0.598 | 12.664 | < 0.000* | 0.836 | 0.479 | 7.806 | < 0.000* |

* – significant at the level of significance $\alpha = 0.05$, Est. – regression weight, Std. Est. – standardised regression weight, t – t -statistic, p – probability level, CYBSPY – Cyber spying.

We show the basic analysis for respondents from the Slovak and Czech Republics of the partial models of the first defined pillar of Cybersecurity in the sense of the model (Figure 1), namely Cyber spying (CYBSY) in Table 10. The first conclusion is that both SK and CZ respondents consider inappropriate cybersecurity policies (CSPYQ5) as the most significant problem, with a high degree of risk assigned (0.709 for SK, 0.701 for CZ), and at the same time both groups of respondents assigned a low degree of risk (0.361 for SK, 0.346 for CZ) to the problem that the cybersecurity solution is solved through outsourcing (CSPYQ3). For respondents from Slovakia, the second most important problem

in the field of Cyber spying is that of the insufficient training of employees in the field of cybersecurity (CSPYQ7), and they assigned it a high degree of risk (0.667, $p < 0.000$), while for respondents from the Czech Republic, this issue is ranked in sixth place of importance with a medium level of risk (0.543, $p < 0.000$). For the respondents of the CZ group, the second most important problem is the question of a comprehensive and systemic solution to cybersecurity (CSPYQ4), with a high degree of risk (0.645, $p < 0.000$), while for the respondents of the SK group this problem is fourth in order but with an equally high degree of risk (0.638, $p < 0.000$). Third place in order of importance for SK respondents is the problem of insufficient screening of employees (CSPYQ6), with a high degree of risk, while for CZ respondents this same place of importance belongs to the problem of insufficient allocation of funds to the issue of cybersecurity (CSPYQ1), with a high degree of risk (0.640, $p < 0.000$). A graphic depiction of the differences in the perception of the risk of individual items of the Cyber spying (CYBSPY) pillar of the hybrid Cybersecurity threat between the SK and CZ respondents, including the entire research file, is shown in Figure 2.

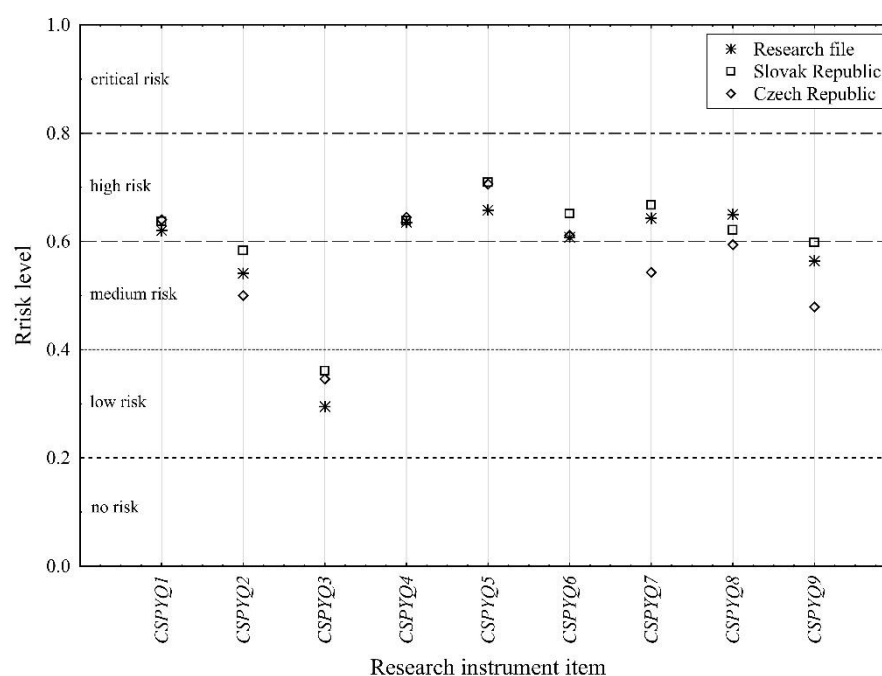


Figure 2. Differences in risk perception of the Cyber spying (CYBSPY) pillar between SK and CZ groups.

(CSPYQ1 – Insufficient allocation of cybersecurity funds, CSPYQ2 – Some ICT manufacturers and suppliers have ties to governments and security forces of other countries, CSPYQ3 – Cybersecurity is carried out by means of outsourcing, CSPYQ4 – Cybersecurity is not solved systemically, only operatively, CSPYQ5 – Cybersecurity policies are poorly set and applied, CSPYQ6 – Employees are examined insufficiently, CSPYQ7 – Insufficient education and training of employees in the field of cybersecurity, CSPYQ8 – Purchase of ICT through insufficiently verified third-party agents without knowing the product chain, CSPYQ9 – Sensitive information at risk of being leaked due to unauthorised use or due to the fact that the staff works using devices in their personal ownership (PCs, telephones, tablets))

An analysis of the differences of the second defined pillar of the hybrid threat Cybersecurity in terms of the theoretical model (Fig. 1), namely the pillar Disrupting or reducing IT infrastructure resilience (DISRIT), between SK respondents and CZ respondents is presented in Table 11. In this case, too, we focus only on the most significant differences between the assessed groups, either from the point of view of the level of risk or the order of importance of the individual items of the research instrument.

Table 11. Estimates of the parameters of the pillar Disrupting or reducing IT infrastructure resilience for respondents from the Slovak and Czech Republics.

| Relationship | | | Slovak Republic | | | | Czech Republic | | | |
|--------------|------|--------|-----------------|-----------|--------|----------|----------------|-----------|--------|----------|
| | | | Est. | Std. Est. | t | p | Est. | Std. Est. | t | p |
| DRITQ1 | <--- | DISRIT | 1.000 | 0.786 | 16.237 | < 0.000* | 1.000 | 0.596 | 10.264 | < 0.000* |
| DRITQ2 | <--- | DISRIT | 0.787 | 0.694 | 16.035 | < 0.000* | 1.196 | 0.627 | 10.508 | < 0.000* |
| DRITQ3 | <--- | DISRIT | 0.688 | 0.619 | 14.263 | < 0.000* | 1.335 | 0.683 | 11.355 | < 0.000* |
| DRITQ4 | <--- | DISRIT | 0.751 | 0.577 | 12.812 | < 0.000* | 1.027 | 0.518 | 9.065 | < 0.000* |
| DRITQ5 | <--- | DISRIT | 0.749 | 0.673 | 14.234 | < 0.000* | 1.328 | 0.701 | 11.433 | < 0.000* |
| DRITQ6 | <--- | DISRIT | 0.654 | 0.584 | 13.498 | < 0.000* | 0.924 | 0.473 | 8.536 | < 0.000* |
| DRITQ7 | <--- | DISRIT | 0.822 | 0.686 | 15.870 | < 0.000* | 1.000 | 0.525 | 7.960 | < 0.000* |
| DRITQ8 | <--- | DISRIT | 0.745 | 0.639 | 14.817 | < 0.000* | 1.172 | 0.559 | 10.060 | < 0.000* |
| DRITQ9 | <--- | DISRIT | 0.893 | 0.703 | 16.153 | < 0.000* | 0.981 | 0.482 | 8.244 | < 0.000* |
| DRITQ10 | <--- | DISRIT | 0.908 | 0.733 | 16.949 | < 0.000* | 1.064 | 0.531 | 9.274 | < 0.000* |
| DRITQ11 | <--- | DISRIT | 0.792 | 0.670 | 15.506 | < 0.000* | 0.920 | 0.509 | 8.460 | < 0.000* |
| DRITQ12 | <--- | DISRIT | 0.856 | 0.698 | 16.054 | < 0.000* | 0.805 | 0.438 | 7.880 | < 0.000* |

* – significant at the level of significance $\alpha = 0.05$, Est. – regression weight, Std. Est. – standardised regression weight, t – t -statistic, p – probability level, DISRIT – Disrupting or reducing IT infrastructure resilience.

For respondents from the SK group the most significant problem of the pillar DISRIT with a high degree of risk is the one that relates to the risk of critical information infrastructure being attacked by cyber attacks (DRITQ1), with a standardised regression weight value of 0.786 ($p < 0.000$). This same issue is in fourth place in terms of importance for the CZ respondents, and they assigned it a medium level of risk (0.596, $p < 0.000$). In contrast, for CZ respondents, the most important security issue is related to unsystematically implemented security testing, with a high degree of risk (0.701, $p < 0.000$), while for the SK respondents this issue is only in seventh place, though it is assigned an equally high degree of risk (0.673, $p < 0.000$). The second most significant threat of the DISRIT pillar for respondents from the SK group is that of fragmentation of the systems of communication means of public administration (DRITQ10), with an assigned high level of risk (0.732, $p < 0.000$), while the CZ respondents assigned this issue a medium level of risk (0.531, $p < 0.000$) and ranked it sixth in the order of importance. The second most important problem for the group of CZ respondents is the issue of not including strategic industries in critical infrastructure, with a high degree of risk (0.683, $p < 0.000$), while this problem is also perceived by SK respondents with an equally high degree of risk (0.619, $p < 0.000$), though it is in tenth place in terms of order. The third most important issue of the DISRIT pillar for SK respondents is that of using outdated information infrastructure systems (DRITQ9), with a high degree of risk (0.703, $p < 0.000$). The CZ respondents put this issue in eleventh place in terms of importance, with a medium level of risk (0.482, $p < 0.000$). In order of importance, the CZ respondents put the issue of a lack of funds for selected areas of cybersecurity (DRITQ2) in third place, with a high degree of risk assigned (0.627, $p < 0.000$). A graphic depiction of differences in risk perception of individual items of the pillar Disrupting or reducing IT infrastructure resilience of (DISRIT), hybrid threat Cybersecurity, between SK and CZ respondents, including a display of the entire research file, is shown in Figure 3.

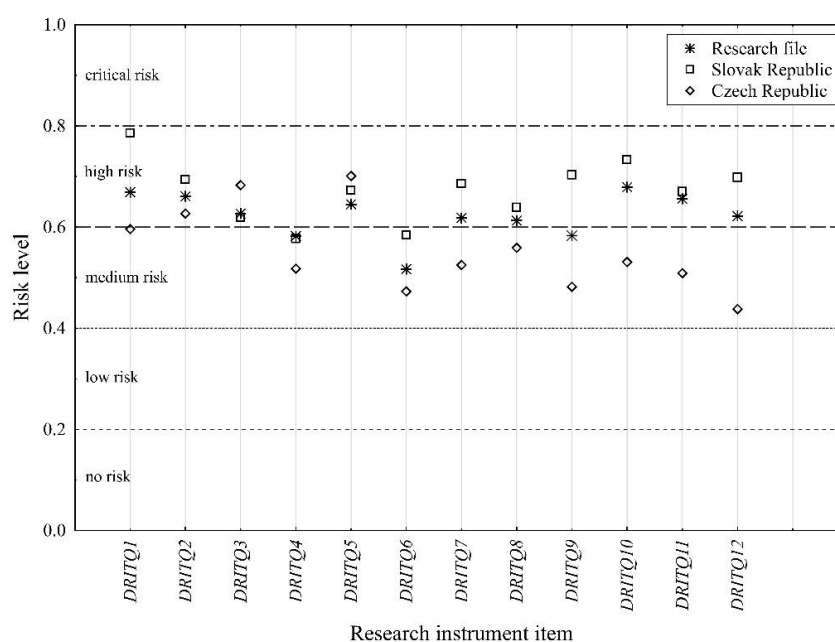


Figure 3. Differences in the perception of the risk of the pillar Disrupting or reducing IT infrastructure resilience (DISRIT) between the SK and CZ groups.

(*DRITQ1* – Risk of attacking critical information infrastructure by cyber attacks through cyber spying, criminal organisations, hackers, etc., *DRITQ2* – Lack of funds to ensure the necessary technical courses and hire workers with verified expertise in ICT and cybersecurity, *DRITQ3* – Strategic industries are not included in the critical infrastructure and their selected information systems cannot be included in the critical information infrastructure, *DRITQ4* – State/public administration employees are not sufficiently aware of cybersecurity, *DRITQ5* – Security testing not being systematically carried out, *DRITQ6* – Attacks on information infrastructure by means of production, supply and subcontracting chains, *DRITQ7* – Incorrect prioritising of some governmental bodies and institutions in planning their investment in security technologies and other ICT, *DRITQ8* – Insufficient amendment of cyber crime legislation, *DRITQ9* – Use of obsolete information infrastructure systems, *DRITQ10* – Fragmentation of systems of communication in state/public administration not allowing their adequately efficient use, maintenance and check-up in real time, *DRITQ11* – Absence of central methodologies for the use of computing means, especially mobile devices, *DRITQ12* – Absence of the mandatory securing of e-mails (commercial encryption) and other electronic communication in use of international as well as national institutions)

The third pillar of Cybersecurity (Figure 1), defined as Cyberterrorism (*CYBTER*), is analysed from the viewpoint of both the order of importance and the degree of assigned risk by respondents from the Slovak and Czech Republics, including the differences between the analysed groups in Table 12.

Table 12. The parameters estimation of the Cyberterrorism pillar for the CZ and SK respondents.

| Relationship | | | Slovak Republic | | | | Czech Republic | | | |
|--------------|------|---------------|-----------------|-----------|----------|----------|----------------|-----------|----------|----------|
| | | | Est. | Std. Est. | <i>t</i> | <i>p</i> | Est. | Std. Est. | <i>t</i> | <i>p</i> |
| <i>CTQ1</i> | <--- | <i>CYBTER</i> | 1.000 | 0.685 | 15.197 | < 0.000* | 1.000 | 0.360 | 5.254 | < 0.000* |
| <i>CTQ2</i> | <--- | <i>CYBTER</i> | 0.875 | 0.612 | 14.986 | < 0.000* | 1.688 | 0.593 | 7.435 | < 0.000* |
| <i>CTQ3</i> | <--- | <i>CYBTER</i> | 1.096 | 0.717 | 17.640 | < 0.000* | 1.357 | 0.455 | 5.637 | < 0.000* |
| <i>CTQ4</i> | <--- | <i>CYBTER</i> | 1.091 | 0.765 | 16.479 | < 0.000* | 1.740 | 0.632 | 6.715 | < 0.000* |
| <i>CTQ5</i> | <--- | <i>CYBTER</i> | 1.115 | 0.721 | 15.536 | < 0.000* | 1.334 | 0.478 | 5.671 | < 0.000* |
| <i>CTQ6</i> | <--- | <i>CYBTER</i> | 1.140 | 0.732 | 16.265 | < 0.000* | 1.638 | 0.622 | 6.373 | < 0.000* |
| <i>CTQ7</i> | <--- | <i>CYBTER</i> | 0.915 | 0.643 | 13.547 | < 0.000* | 1.814 | 0.595 | 7.087 | < 0.000* |

* – significant at the level of significance $\alpha = 0.05$, Est. – regression weight, Std. Est. – standardised regression weight, *t* – *t*-statistic, *p* – probability level, *CYBTER* – Cyberterrorism.

The first conclusion of Table 12 is the fact that both analysed groups (*SK*, *CZ*) marked the same items of the research instrument in terms of the order of importance of the individual threats of the *CYBTER* pillar as well as in terms of the degree of risk. For both groups, the issue of obtaining sensitive information of an intelligence nature for the purpose of using it in a kinetic terrorist attack (*CTQ4*) is in first place, with an assigned high level of risk, and the issue of managing sympathisers by third parties, primarily by inciting their activity against possible targets, planning terrorist operations, providing feedback, etc. (*CTQ6*) is in second place, with an equally high level of risk. For the *SK* group of respondents, the third most important issue is the spread of propaganda and materials to support followers of radicalisation and their recruitment (*CTQ5*), with a high level of risk assigned (0.721, $p < 0.000$), while for the *CZ* respondents this issue is in fifth place with a medium level of risk (0.478, $p < 0.000$). The third most significant problem for the *CZ* respondents is the question on the low preparedness of the security forces for a specific digital environment and operating in it (*CTQ7*), with a medium level of risk, while this problem for the *SK* group is in sixth place but with a high level of risk (0.643, $p < 0.000$). It can be seen in Table 12 that the respondents from the *SK* group assigned a high level of risk to all items of the research instrument, while those from the *CZ* group marked only two items as high risk (*CTQ4*, *CTQ6*) and assigned a medium level of risk to the remaining five. Thus, even here, differences are evident in the perception of the degree of risk between the analysed groups. A graphic depiction of the differences in the perception of the risk of individual items of the Cyberterrorism (*CYBTER*) pillar of the hybrid threat Cybersecurity between the *SK* and *CZ* respondents, including the display of the entire research file, is shown in Figure 4.

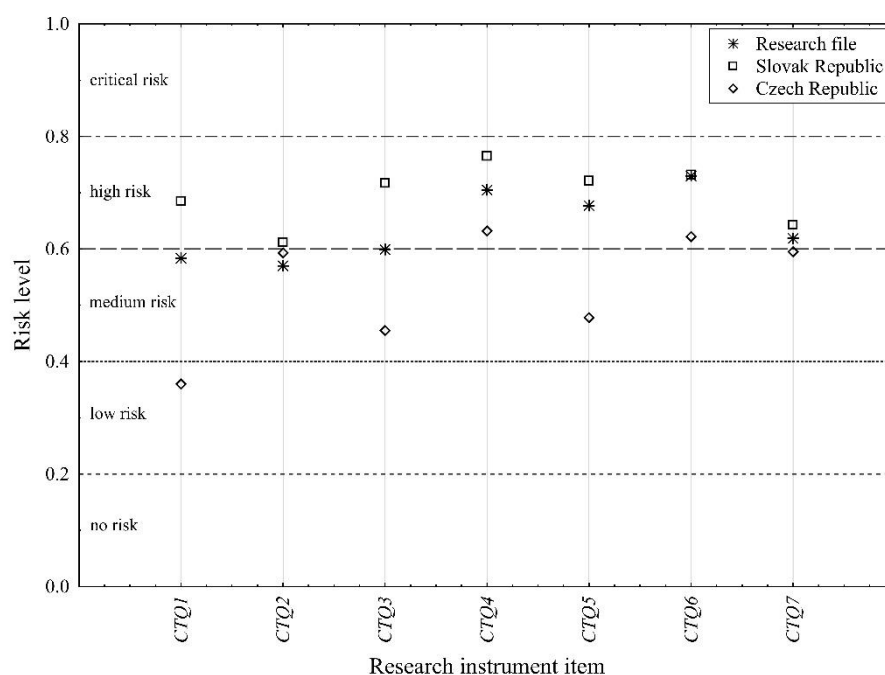


Figure 4. Differences in the perception of the risk of the Cyberterrorism (*CYBTER*) pillar between the *SK* and *CZ* groups.

(*CTQ1* – Blackmail of state authorities, commercial corporations or intimidation of society, *CTQ2* – Destruction of specific technology (information, manufacturing, operating), *CTQ3* – Energy distribution (energy blackout), *CTQ4* – Acquisition of sensitive intelligence information for their use in a kinetic terrorist attack (selection of specific goals, etc.), *CTQ5* – Spread of propaganda and materials aimed at radicalisation of supporters and their recruitment, *CTQ6* – Management of sympathisers by using third parties, in particular to evoke activities against possible goals, planning of terrorist operations, providing feedback, etc., *CTQ7* – Low readiness of security forces to operate within specific digital environment)

The analysis of the differences in respondents' views on the degree of risk of the fourth defined pillar of the hybrid threat Cybersecurity (Figure 1), that of the pillar Disrupting or reducing eGovernment security (*DISREG*), is presented in Table 13.

Table 13. Estimates of the parameters of the pillar Disrupting or reducing eGovernment security for respondents from the Slovak and Czech Republics.

| Relationship | | | Slovak Republic | | | | Czech Republic | | | |
|---------------|------|---------------|-----------------|-----------|----------|----------|----------------|-----------|----------|----------|
| | | | Est. | Std. Est. | <i>t</i> | <i>p</i> | Est. | Std. Est. | <i>t</i> | <i>p</i> |
| <i>GREGQ1</i> | <--- | <i>DISREG</i> | 1.000 | 0.759 | 18.936 | < 0.000* | 1.000 | 0.555 | 9.163 | < 0.000* |
| <i>GREGQ2</i> | <--- | <i>DISREG</i> | 1.112 | 0.829 | 21.007 | < 0.000* | 0.904 | 0.511 | 9.007 | < 0.000* |
| <i>GREGQ3</i> | <--- | <i>DISREG</i> | 1.044 | 0.727 | 17.877 | < 0.000* | 1.068 | 0.681 | 9.850 | < 0.000* |
| <i>GREGQ4</i> | <--- | <i>DISREG</i> | 0.909 | 0.732 | 18.063 | < 0.000* | 1.174 | 0.727 | 10.253 | < 0.000* |
| <i>GREGQ5</i> | <--- | <i>DISREG</i> | 0.978 | 0.758 | 17.394 | < 0.000* | 1.132 | 0.638 | 10.658 | < 0.000* |
| <i>GREGQ6</i> | <--- | <i>DISREG</i> | 0.916 | 0.686 | 15.202 | < 0.000* | 0.811 | 0.467 | 6.833 | < 0.000* |

* – significant at the level of significance $\alpha = 0.05$, Est. – regression weight, Std. Est. – standardised regression weight, *t* – *t*-statistic, *p* – probability level, *DISREG* – Disrupting or reducing e-government security.

The most significant problem perceived as a critical risk by the SK respondents (0.829, $p < 0.000$) is that of the underestimating of cyber threats in state or public administration (*GREGQ2*), and at the same time, for this one question only, respondents indicated a critical degree of risk. This same problem has only a medium level of risk (0.511, $p < 0.000$) for respondents from the CZ group and in order of importance was in the penultimate, or fifth, place. For respondents from the Czech Republic, the most important from the in regard to the *DISREG* pillar is the question that relates to the bad setting of the cybersecurity policy by the state (*GREGQ4*), with a high degree of risk (0.727, $p < 0.000$). Respondents from the SK group assigned an equally high level of risk (0.732, $p < 0.000$) to this problem, but for them it is only in fourth place in terms of importance. The second most significant threat for SK respondents is insufficient funding in the field of cybersecurity (*GERGQ1*), with a high level of risk, while for the comparison group (CZ) this problem is in fourth place with a medium level of risk (0.555, $p < 0.000$). In contrast, for the groups of respondents from the Czech Republic the issue of insufficient security of information systems intended for communication with citizens (*GREGQ3*) is in second place, with a high degree of risk (0.671, $p < 0.000$), and this same problem was put in fifth place by the SK respondents, but with the same high degree of risk (0.727, $p < 0.000$). The problem relating to the low awareness and education of the population about cybersecurity (*GREGQ6*) is in third place for both compared groups in terms of importance, with the same high degree of risk. As with the previous analysed pillar (*CYBTER*), with this one (*DISREG*), an interesting fact can be seen: that while the respondents from the SK group assigned a critical level of risk to one item and a high level of risk to the remaining five, the respondents from the CZ group assigned a high level of risk to three items of the research instrument and a medium level of risk to four items. A graphic depiction of differences in risk perception of individual items of the pillar Disrupting or reducing eGovernment security (*DISREG*), hybrid threat Cybersecurity, between respondents of the SK and CZ groups, including a display of the entire research file, is shown in Figure 5.

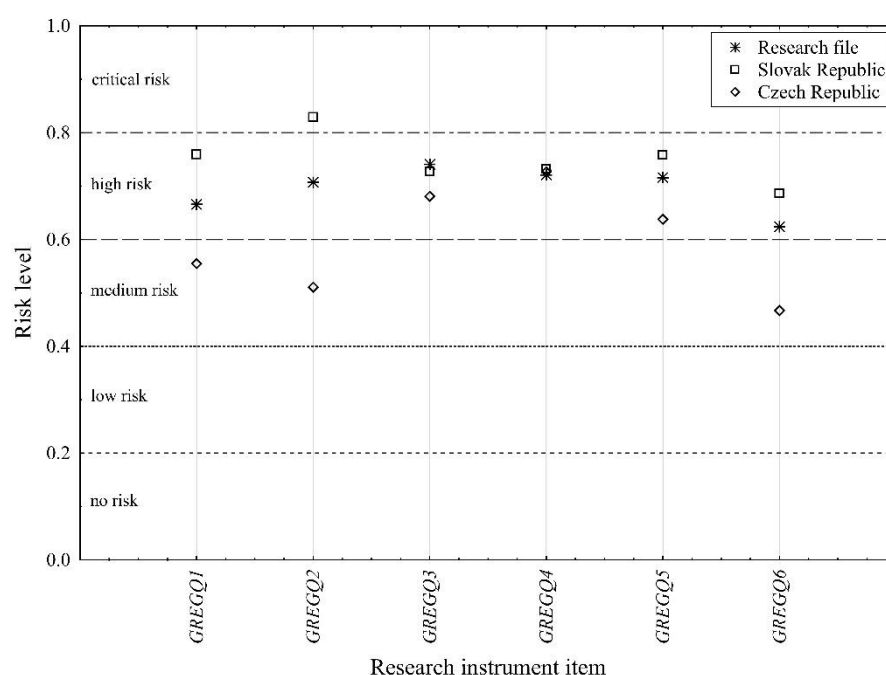


Figure 5. Differences in risk perception of the pillar Disrupting or reducing eGovernment security (DISREG) between the SK and CZ groups.

(GREGQ1 – Insufficient financing of cybersecurity and insufficient financial evaluation of cybersecurity workers, GREGQ2 – Underestimating cyber threats in state/public administration, GREGQ3 – Insufficient investment in information and cyber systems of state/public administration serving as means of communication between citizens and the state, GREGQ4 – Poor setting of cybersecurity policy from the state level, GREGQ5 – Insufficient education of state/public administration employees regarding cybersecurity, GREGQ6 – Low level of awareness and education of the population on cybersecurity)

The analysis of the last pillar of the hybrid threat Cybersecurity in the sense of the theoretical model (Figure 1), which we called Enemy campaigns (ENECAM), is presented for the compared groups in Table 14.

Table 14. Estimates of the parameters of Enemy campaigns pillar for respondents from the Slovak and Czech Republics.

| Relationship | | | Slovak Republic | | | | Czech Republic | | | |
|--------------|------|--------|-----------------|-----------|----------|----------|----------------|-----------|----------|----------|
| | | | Est. | Std. Est. | <i>t</i> | <i>p</i> | Est. | Std. Est. | <i>t</i> | <i>p</i> |
| ECQ1 | <--- | ENECAM | 1.000 | 0.648 | 15.551 | < 0.000* | 1.000 | 0.475 | 8.055 | < 0.000* |
| ECQ2 | <--- | ENECAM | 0.990 | 0.645 | 15.339 | < 0.000* | 0.345 | 0.181 | 3.783 | < 0.000* |
| ECQ3 | <--- | ENECAM | 1.036 | 0.684 | 14.244 | < 0.000* | 0.825 | 0.457 | 8.506 | < 0.000* |
| ECQ4 | <--- | ENECAM | 0.983 | 0.651 | 13.698 | < 0.000* | 1.224 | 0.629 | 8.228 | < 0.000* |
| ECQ5 | <--- | ENECAM | 0.840 | 0.542 | 11.708 | < 0.000* | 1.021 | 0.550 | 7.821 | < 0.000* |

* – significant at the level of significance $\alpha = 0.05$, Est. – regression weight, Std. Est. – standardised regression weight, *t* – *t*-statistic, *p* – probability level, ENECAM – Enemy campaigns.

The most important problem of the ENECAM pillar for the SK respondents is the question that relates to the ownership structure of individual Internet media, which can follow their own interests or the interests of other states (ECQ3), with a high level of risk (0.684, $p < 0.000$), while this problem is in fourth place for the CZ respondents, with a medium level of risk (0.457, $p < 0.000$). For the CZ respondents the most significant problem is that of insufficient screening of state/public administration employees who may work for the benefit of third parties (ECQ4), with a high degree of risk (0.629, $p < .000$), while for the SK respondents, this issue ranks second and has an equally high degree of risk (0.651,

$p < 0.000$). The third most significant problem in terms of order of importance for the first compared group (SK) is the one related to the effect of influence and disinformation campaigns on the Internet to shape residents' moods (ECQ1), with an assigned high degree of risk (0.648, $p < 0.000$), while respondents from the CZ group assigned a medium level of risk to this problem (0.475, $p < 0.000$), but, like the SK group, put it in third place in terms of importance. An interesting difference between the opinions of the compared groups is the problem of the wide use of the social networks environment due to their international aspect and different approach to freedom of speech, which enables them to be used to a greater extent to spread hate and disinformation campaigns (ECQ2). While the respondents from the SK group assigned a high level of risk to this problem (0.645, $p < 0.000$), the respondents from the CZ group assigned the "no risk" degree of risk (0.181, $p < 0.000$) to this item of the research instrument (ECQ2). Here it should be noted that within the entire research instrument, only this item (ECQ2) is perceived as risk free. In this case, too, it can be seen that the SK respondents assign a higher level of risk to individual items of the research instrument than those from the CZ group. A graphic depiction of the differences in the perception of the risk of individual items of the Enemy campaigns (ENECAM) pillar of the hybrid threat Cybersecurity between the respondents of the SK and CZ groups, including the display of the entire research file, is shown in Figure 6.

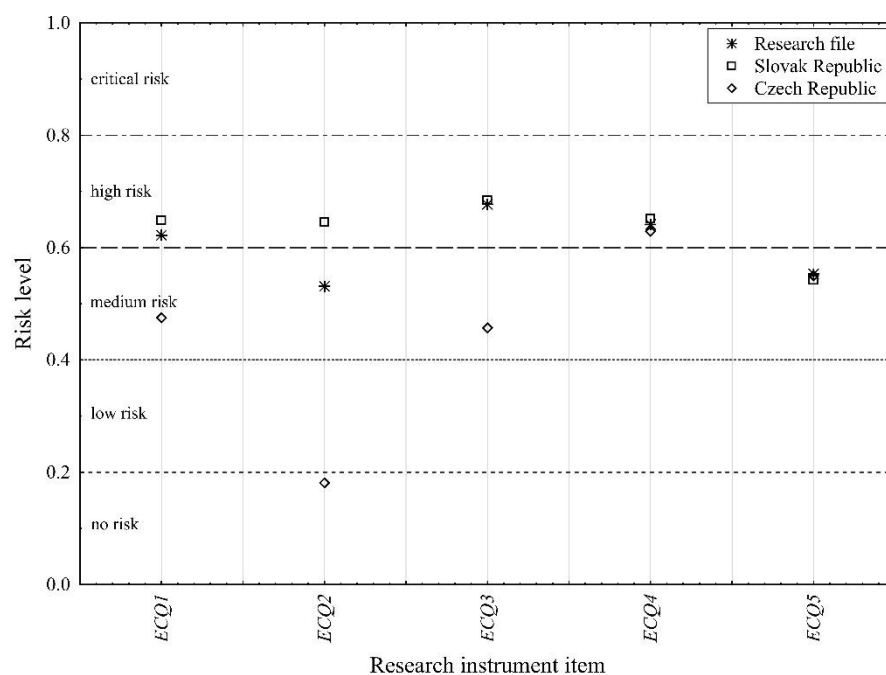


Figure 6. Differences in the perception of risk of the Enemy campaigns (ENECAM) pillar between the SK and CZ groups.

(ECQ1 – Online influencing and disinformation campaigns may have a major impact on evoking the mood in the population (provoking social unrest), ECQ2 – Wide use of social networks, their international aspect and ambiguous approach to freedom of speech, enables the spreading of hate and disinformation campaigns, ECQ3 – Structure of ownership of individual online media enabling them to pursue various private interests or interests of other countries in their news reports, ECQ4 – Insufficient review of state/public administration employees who may work in favour of third parties, ECQ5 – Current legislation on free access to information may endanger cybersecurity or can be abused in information campaigns)

The differences in the perception of the relationships between the individual defined pillars of the hybrid threat Cybersecurity between the compared groups can also be analysed. We present a basic analysis of these relationships in Table 15.

Table 15. Analysis of the interrelationships of the individual pillars of Cybersecurity.

| Relationship | | | Slovak Republic | | | Czech Republic | | |
|--------------|------|--------|-----------------|-----------------|-------------|----------------|-----------------|-------------|
| | | | Covar. | <i>p</i> -value | Correlation | Covar. | <i>p</i> -value | Correlation |
| CYBSPY | <--> | CYBTER | 0.324 | < 0.001 * | 0.809 | 0.103 | < 0.001 * | 0.531 |
| DISRIT | <--> | DISREG | 0.523 | < 0.001 * | 0.882 | 0.227 | < 0.001 * | 0.837 |
| DISRIT | <--> | ENECAM | 0.415 | < 0.001 * | 0.793 | 0.150 | < 0.001 * | 0.627 |
| CYBSPY | <--> | DISREG | 0.325 | < 0.001 * | 0.758 | 0.237 | < 0.001 * | 0.757 |
| DISRIT | <--> | CYBTER | 0.447 | < 0.001 * | 0.805 | 0.123 | < 0.001 * | 0.730 |
| CYBSPY | <--> | ENECAM | 0.295 | < 0.001 * | 0.782 | 0.188 | < 0.001 * | 0.680 |
| CYBSPY | <--> | DISRIT | 0.419 | < 0.001 * | 0.908 | 0.237 | < 0.001 * | 0.883 |
| DISREG | <--> | ENECAM | 0.407 | < 0.001 * | 0.839 | 0.204 | < 0.001 * | 0.728 |
| CYBTER | <--> | ENECAM | 0.402 | < 0.001 * | 0.886 | 0.132 | < 0.001 * | 0.762 |
| CYBTER | <--> | DISREG | 0.386 | < 0.001 * | 0.749 | 0.130 | < 0.001 * | 0.663 |

* – significant at the level of significance $\alpha = 0.05$, Covar. – covariation, *p*-value – probability level, CYBSY – Cyber spying, CYBTER – Cyberterrorism, DISRIT – Disrupting or reducing IT infrastructure resistance, ENECAM – Enemy campaigns, DISREG – Disrupting or reducing e-government security.

Both compared groups consider the link between the CYBSPY and DISRIT pillars to be the most important relationship. The correlation coefficient of this relationship for respondents from the SK group is at the level of 0.908 ($p < 0.000$), while this relationship in terms of Cohen's scale can be considered almost perfect, and for respondents from the CZ group, the value of the correlation coefficient for the analysed relationship of the pillars of Cybersecurity is at the level 0.883 ($p < 0.000$), which means a very significant relationship. For the group of SK respondents, the relationship between the pillars of Cybersecurity CYBTER and DISREG reaches the value of the correlation coefficient of 0.862 ($p < 0.000$) and takes second place in the order of importance, while for the group of CZ respondents the correlation coefficient is 0.762 ($p < 0.000$) and occupies the third place. For respondents from the SK group a change of order also occurs in the third most significant relationship between the pillars of Cybersecurity, namely the relationship between DISRIT and DISREG, with a correlation coefficient value of 0.882 ($p < 0.000$), while this relationship is in third place for respondents from the CZ group, with the correlation coefficient at 0.837 ($p < 0.000$) with the second level of significance. We see most significant shift in the perception of the relationship between the CYBSPY and CYBTER pillars, where for the SK respondents this relationship is very significant (0.809, $p < 0.000$) and is in fifth place in terms of importance, and for the CZ respondents this relationship is characterised as significant (0.531, $p < 0.000$) and fills the last place in terms of importance. In terms of the significance of the individual defined pillars of Cybersecurity for the individual compared groups, the respondents from the SK group consider the DISREG pillar, with 22.700% influence, as the biggest risk versus the CZ respondents, who consider the DISRIT pillar, with 24.274% influence, as the biggest problem. The DISRIT pillar is the second most important pillar for Slovak respondents with a share of 21.885%, while the second most important pillar for the Czech respondents is the CYBSPY pillar with a share of influence at the level of 22.637%. The third most important pillar of Cybersecurity as a hybrid threat for respondents of the SK group is the CYBTER pillar (19.447%), followed by the ENECAM pillar (17.995%) and the CYBSPY pillar (17.924%). If we rank the Cybersecurity pillars in the same way for the CZ respondents, third place in terms of the share of influence goes to the DISREG pillar (21.612%), followed by the ENECAM pillar (18.268%) and the CYBTER pillar (13.210%). Therefore, it is possible to state that there are significant differences between the compared groups of respondents (SK, CZ) both in the perception

of the relationships between the individual defined pillars of Cybersecurity and in the perception of the risk of the individual pillars as a whole. This creates an interesting starting point, which must reflect the obtained results in education and the approach to Cybersecurity in both of these countries. In conclusion, it needs to be noted that the respondents were students of police and military universities in Slovakia and the Czech Republic, and their preparation to battle against hybrid threats is crucial in terms of protecting countries from the danger of hybrid threats.

5. Conclusions

No state these days is completely protected from the threats of cyberspace. The worsening security situation, and not only in areas immediately bordering NATO and EU Member States, is amplifying the increasing demands on countries' abilities to independently respond to security threats in cyberspace. It is possible to observe the growing efforts of both state and non-state actors to build and use cyber offensive resources, whose aim is mainly critical infrastructure, or those parts of it exposed in cyberspace – critical information infrastructure and significant information systems. Indeed, these represent a key system of elements whose disruption or non-functionality would have a serious impact on the security of a state, the provision of the basic life needs of the population or the economic situation.

Our study on maintaining cybersecurity in the face of hybrid threats through risk perception analysis clarified the multifaceted challenges that organisations and individuals are facing in the digital age. The presented findings emphasise the principle importance of not only technical guarantees, but also the human factor in cybersecurity. Understanding and managing risk perception can significantly affect an organisation's ability to effectively mitigate hybrid threats and respond to them. By being aware that perceptions shape behaviour, organisations can invest in training, awareness campaigns and collaborative efforts to strengthen their security. What's more, our research highlights the need for ongoing collaboration between government agencies, private sector entities and academia to address the evolving hybrid threat environment. This interdisciplinary approach can lead to the development of more robust cybersecurity strategies, information sharing mechanisms and policy frameworks. Maintaining cybersecurity is an ongoing process that requires vigilance, adaptability and proactive thinking and taking a proactive approach towards rapidly evolving technologies and threats. By incorporating knowledge about risk perception into cybersecurity strategies and cultivating a culture of cybersecurity awareness, it becomes possible to work together and coordinate a safer and more resilient digital ecosystem. Protecting the digital future will in the end depend on the ability to stay one step ahead, to innovate and to work together effectively in the battle against hybrid threats.

As part of the presented study, we attempted to analyse the opinions and attitudes towards the risk assessment of one of the basic hybrid threats, namely Cybersecurity, based on the author's research instrument on a sample ($N = 964$) of students of the Slovak and Czech Republics who study at universities of the police and military type of study. The choice of the target group of respondents was motivated by the fact that it is this group of respondents who will represent the first line of the battle against hybrid threats in the future. The research instrument, as such, is based on official documents of the Slovak and Czech Republics in the field of security. Within the analysis, the authors defined a basic theoretical factor model (Figure 1) of the hybrid threat "Cybersecurity", which is defined by five basic pillars: Cyber spying (CYBSPY), Disrupting or reducing IT infrastructure resilience (DISRIT), Enemy campaigns (ENECAM), Disrupting or reducing eGovernment security (DISREG) and Cyberterrorism (CYBTER). An analysis of the agreement of the respondents' answers (Table 2, Table 9) with the factor theoretical model (Figure 1) was subsequently carried out using confirmatory factor analysis (CFA) for the entire research set and then separately for respondents from the Slovak and Czech Republics

with the aim of defining the basic differences in the perception of the level of risk between the analysed groups.

Within the framework of the theoretical factor model (Figure 1) of the hybrid threat “Cybersecurity”, a significant influence of all defined pillars was demonstrated at the chosen level of significance $\alpha = 5\%$. From the point of view of the significance and impact of individual pillars on Cybersecurity in terms of view of risk, the most significant pillar for the entire research set ($N = 964$) is “Disrupting or reducing IT infrastructure resilience” (*DISRIT*) with a share of Cybersecurity risk perception at a level of 22.284%. The second most important pillar of cybersecurity is the pillar Disrupting or reducing eGovernment security (*DISREG*) with a share of 21.842%. The third most important pillar is the Enemy campaigns pillar (*ENECAM*) with a share of 19.532%, followed by the Cyberterrorism pillar (*CYBTER*) with a share of 18.381% and the Cyber spying pillar (*CYBSPY*) with a share of 17.961%. The relatively small differences in the importance of the individual pillars of cybersecurity suggests that all the defined pillars are perceived by the respondents as having approximately the same level of risk. On the other hand, based on the analysis conducted, it is possible to define basic differences in the perception of the pillars of cybersecurity between respondents from the Slovak and Czech Republics. For respondents from Slovakia, the most important pillar in terms of its risk is the *DISREG* pillar (22.700%), followed by the *DISRIT* (21.885%), *CYBTER* (19.477%), *ENECAM* (17.995%) and *CYBSPY* (17.942%) pillars. Here, too, relatively small differences in the perception of individual shares can be identified. Among respondents from the Czech Republic a change occurs in the order of importance as well as the share of the individual pillars of cybersecurity. For this group of respondents, the most important pillar is the *DISRIT* pillar (24.274%), followed by the *CYBSPY* (22.637%), *DISREG* (21.612%), *ENECAM* (18.268%) and *CYBTER* (13.210%) pillars. The difference in risk perception of individual pillars is greater among the Czech respondents than among those from Slovakia. The biggest difference between the compared groups is the perception of the *CYBTER* pillar. A detailed analysis of the differences in the perception of individual items of the research instrument that form the defined pillars of cybersecurity is presented in the study. The overall conclusion is that respondents from the Slovak Republic attach a higher degree of risk to most individual threats than respondents from the Czech Republic, which we document in the analytical part of the contribution.

The Factor Model of Cybersecurity (FMCS) represents an attempt to quantify the attitudes towards risk perception of the individual defined pillars *CYBSPY*, *DISRIT*, *ENECAM*, *DISREG* and *CYBTER* of the FMCS model and the individual threats that make up the pillars. A practical output could be the defining of critical threats and pillars which are perceived by the respondents at the level of high or critical risk with subsequent focusing of the attention of the responsible state authorities on these areas. A second indisputable benefit should be the effort to educate specifically in these critical areas of cybersecurity. Of course, it would be correct and is also one of the main aims of the authors to expand the research set with relevant groups of respondents in EU countries while also expanding the research set with respondents from the state and public administration. The current makeup of the research group also represents a certain limitation of the presented research. At the same time, it is also necessary to analyse the views and attitudes of the respondents on the perception of the risk of cybersecurity (FMCS) from the point of view of other groups of respondents (gender, age) and to focus the education of the respondents in the field of cybersecurity according to the results obtained. A very important challenge, on which the team of authors is currently working on actively, is an analysis of other relevant hybrid threats and, above all, sustainable and resilient cybersecurity.

Author Contributions: Conceptualization, M.G., A.K., P.R. and A.V.; methodology, M.G., P.R. and A.V.; software, M.G.; validation, A.V., M.G., A.K. and P.R.; formal analysis, A.K. and A.V.; investigation, M.G., A.K., A.V. and P.R.; resources, A.V., A.K. and M.G.; data curation, M.G.; writing—

original draft preparation, M.G., A.V., A.K. and P.R.; writing—review and editing, M.G., A.V., A.K. and P.R.; visualization, A.K., M.G., A.V. and P.R.; supervision, M.G., A.K., P.R. and A.V.; project administration, A.K.; funding acquisition, A.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by The European Social Fund and Ministry of Interior of the Slovak Republic, grant number code ITMS2014+:314011CDW7, grant title “Increasing Slovakia’s resilience to hybrid threats by strengthening public administration capacities”. The APC was funded by this grant ITMS2014+:314011CDW7. The fourth author was supported by the grant VAROPS.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Data are available based upon the request.

Acknowledgments: This research is one of the partial outputs under the scientific research grant with grant code ITMS2014+:314011CDW7; grant title “Increasing Slovakia’s resilience to hybrid threats by strengthening public administration capacities”.

The fourth author thanks to the Ministry of Defence of the Czech Republic for the support via grant VAROPS.

Conflicts of Interest: The authors declare no conflict of interest.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

References

- Zhong, R.Y.; Xu, X.; Klotz, E.; Newman, S.T. Intelligent Manufacturing in the Context of Industry 4.0: A Review. *Engineering* **2017**, *3*, 616–630. <https://doi.org/10.1016/J.ENG.2017.05.015>
- Rudenko, R.; Pires, IM; Oliveira, P.; Barroso, J.; Reis, A. Stručný prehľad o internete vecí, priemysle 4.0 a kybernetickej bezpečnosti. *Electronics* **2022**, *11*, 1742. <https://doi.org/10.3390/electronics11111742>
- Matana G.; Simon, A.T.; Filho M.G.; Helleno A.L. Method to assess the adherence of internal logistics equipment to the concept of CPS for industry 4.0. *International Journal of Production Economics* **2020**, *228*, 107845, <https://doi.org/10.1016/j.ijpe.2020.107845>
- O'Donovan, P.; Gallagher, C.; Leahy, K.; O'Sullivan, D.T.J. A comparison of fog and cloud computing cyber-physical interfaces for Industry 4.0 real-time embedded machine learning engineering applications. *Computers in Industry* **2019**, *110*, pp. 12–35, <https://doi.org/10.1016/j.compind.2019.04.016>.
- Gao, Z.; Wanyama, T.; Singh, I.; Gadhri, A.; Schmidt, R. From Industry 4.0 to Robotics 4.0 - A Conceptual Framework for Collaborative and Intelligent Robotic Systems. *Procedia Manufacturing* **2020**, *46*, pp. 591–599. <https://doi.org/10.1016/j.promfg.2020.03.085>
- 06de Azambuja, A.J.G.; Plesker, C.; Schützer, K.; Anderl, R.; Schleich, B.; Almeida, V.R. Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey. *Electronics* **2023**, *12*, 1920. <https://doi.org/10.3390/electronics12081920>
- Jan, Z.; Ahamed, F.; Mayer, W.; Patel, N.; Grossmann, G.; Stumptner, M.; Kuusk, K. Artificial intelligence for industry 4.0: Systematic review of applications, challenges, and opportunities. *Expert Systems with Applications* **2023**, *216*, 119456, <https://doi.org/10.1016/j.eswa.2022.119456>
- Aceto, G.; Persico, V.; Pescapé, A. Industry 4.0 and Health: Internet of Things, Big Data, and Cloud Computing for Healthcare 4.0, *Journal of Industrial Information Integration* **2020**, *18*, 100129, <https://doi.org/10.1016/j.jii.2020.100129>
- Ray Y. Zhong, Xun Xu, Eberhard Klotz, Stephen T. Newman, Intelligent Manufacturing in the Context of Industry 4.0: A Review, *Engineering* **2017**, *3*, Issue 5, pp. 616–630, <https://doi.org/10.1016/J.ENG.2017.05.015>.
- Corallo, A.; Lazoi, M.; Lezzi, M.; Luperto, A. Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review, *Computers in Industry*, Volume 137, **2022**, 103614, <https://doi.org/10.1016/j.compind.2022.103614>.
- Kohout, D.; Lieskovan, T.; Mlynek, P. Smart Metering Cybersecurity—Requirements, Methodology, and Testing. *Sensors* **2023**, *23*, 4043. <https://doi.org/10.3390/s23084043>
- What is Industry 4.0? Available online (accessed on 27 November 2023) <https://www.ibm.com/topics/industry-4-0#What+technologies+are+driving+Industry+4.0%3F>.
- Alqudhaibi, A.; Albarrak, M.; Aloose, A.; Jagtap, S.; Salonitis, K. Predicting Cybersecurity Threats in Critical Infrastructure for Industry 4.0: A Proactive Approach Based on Attacker Motivations. *Sensors* **2023**, *23*, 4539. <https://doi.org/10.3390/s23094539>
- Trevert, G.F.; Thvedt, A.; Chen, A.R.; Lee, K.; McCue, M. *Addressing Hybrid Threats*, 1st ed.; Swedish Defence University: Stockholm, Sweden, 2018; p. 101, Printed by: Arkitektkopia AB, Bromma **2018**, ISBN 978-91-86137-73-1.
- Aslan, Ö.; Aktuğ, S.S.; Ozkan-Okay, M.; Yilmaz, A.A.; Akin, E. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics* **2023**, *12*, 1333. <https://doi.org/10.3390/electronics12061333>.

16. Granholm, F.; Tin, D.; Ciotton, G.R. Not war, not terrorism, the impact of hybrid warfare on emergency medicine. *Am. J. Emerg. Med.* **2022**, *62*, pp. 96–100, <https://doi.org/10.1016/j.ajem.2022.10.021>. 1006
17. Cox, E. “I hope they shouldn't happen”: Social vulnerability and resilience to urban energy disruptions in a digital society in Scotland. *Energy Research & Social Science* **2023**, *95*, 102901, <https://doi.org/10.1016/j.erss.2022.102901>. 1007
18. Almaiah, M.A.; Al-Otaibi, S.; Shishakly, R.; Hassan, L.; Lutfi, A.; Alrawad, M.; Qatawneh, M.; Alghanam, O.A. Investigating the Role of Perceived Risk, Perceived Security and Perceived Trust on Smart m-Banking Application Using SEM. *Sustainability* **2023**, *15*, 9908. <https://doi.org/10.3390/su15139908>. 1008
19. Bıçakcı, A.S.; Evren, A.G. Thinking multiculturalism in the age of hybrid threats: Converging cyber and physical security in Akkuyu nuclear power plant. *Nuclear Engineering and Technology* **2022**, *54* (7), pp. 2467–2474, <https://doi.org/10.1016/j.net.2022.01.033>. 1009
20. Nshom, E.; Khalimzoda, I.; Sadaf, S.; Shaymardanov, M. Perceived threat or perceived benefit? Immigrants' perception of how Finns tend to perceive them. *International Journal of Intercultural Relations* **2022**, *86*, pp. 46–55, <https://doi.org/10.1016/j.ijintrel.2021.11.001>. 1010
21. Eberle, J.; Daniel, J. Anxiety geopolitics: Hybrid warfare, civilisational geopolitics, and the Janus-faced politics of anxiety. *Political Geography* **2022**, *92*, 102502, <https://doi.org/10.1016/j.polgeo.2021.102502>. 1011
22. Procházka, J.; Vinkler, P.; Jojart, K.; Szenes, Z.; Gruszczak, A.; Kandrák, M. One threat – multiple responses. Countering Hybrid Threats in V4 countries/Jedna hrozba – více způsobů reakce. Členění hybridního působení v zemích V4. *Obrana a strategie /Defence and Strategy* **2023**, *23*, p. 049–073. [10.3849/1802-7199.23.2023.01.049-073](https://doi.org/10.3849/1802-7199.23.2023.01.049-073). 1012
23. Mekala, S.H.; Baig, Z.; Anwar, A.; Zeadally, S. Cybersecurity for Industrial IoT (IIoT): Threats, countermeasures, challenges and future directions. *Computer Communications* **2023**, *208*, p. 294–320, ISSN 0140-3664, <https://doi.org/10.1016/j.comcom.2023.06.020>. 1013
24. Qin, X.; Jiang, F.; Cen, M.; Doss, R. Hybrid cyber defense strategies using Honey-X: A survey. *Computer Networks* **2023**, *230*, 109776, ISSN 1389-1286, <https://doi.org/10.1016/j.comnet.2023.109776>. 1014
25. Hausken, K. Cyber resilience in firms, organizations and societies. *Internet of Things* **2020**, *11*, 100204, ISSN 2542-6605, <https://doi.org/10.1016/j.iot.2020.100204>. 1015
26. Tsaruk, O.; Korniiets, M. Hybrid nature of modern threats for cybersecurity and information security. *Smart Cities and Regional Development Journal* **2020**, *4* (1), pp. 57–78, [10.25019/scrd.v4i1.63](https://doi.org/10.25019/scrd.v4i1.63). 1016
27. Bachmann, S.D.; Gunneriusson, H. Terrorism and Cyber Attacks as Hybrid Threats: Defining a Comprehensive Approach for Countering 21st Century Threats to Global Risk and Security. *The Journal on Terrorism and Security Analysis* **2014**, pp. 26–36, <https://ssrn.com/abstract=2252595>. 1017
28. Galinec, D.; Steingartner, W.; Zebić, V. Cyber Rapid Response Team: An Option within Hybrid Threats. In Proceedings of the 2019 IEEE 15th International Scientific Conference on Informatics, Poprad, Slovakia, 20–22 November 2019, pp. 000043–000050, [10.1109/Informatics47936.2019.9119292](https://doi.org/10.1109/Informatics47936.2019.9119292). 1018
29. Maglaras, L.; Janicke, H.; Ferrag, M.A. Combining Security and Reliability of Critical Infrastructures: The Concept of Securability. *Appl. Sci.* **2022**, *12*, 10387. <https://doi.org/10.3390/app122010387>. 1019
30. Shaked, A.; Margalit, O. Sustainable Risk Identification Using Formal Ontologies. *Algorithms* **2022**, *15*, 316. <https://doi.org/10.3390/a15090316>. 1020
31. Sadik, S.; Ahmed, M.; Sikos, L.F.; Islam, A.K.M.N. Toward a Sustainable Cybersecurity Ecosystem. *Computers* **2020**, *9*, 74. <https://doi.org/10.3390/computers9030074>. 1021
32. Nam, T. Understanding the gap between perceived threats to and preparedness for cybersecurity. *Technology in Society* **2019**, *58*, 101122, <https://doi.org/10.1016/j.techsoc.2019.03.005>. 1022
33. Larsen, M.H.; Lund, M. S.; Bjørneseth, F.B. A model of factors influencing deck officers' cyber risk perception in offshore operations. *Maritime Transport Research* **2022**, *3*, 100065, <https://doi.org/10.1016/j.martra.2022.100065>. 1023
34. Spearman, C. “General intelligence” objectively determined and measured. *American Journal of Psychology* **1904**, *15*, pp. 201–293. 1024
35. Shah, R.; Goldstein, S. M. Use of structural equation modeling in operations management research: Looking back and forward. *Journal of Operations Management* **2006**, *24*(2), 148–169. 1025
36. Wallenburg, C. M.; Weber, J. Structural Equation Modelling as a Basis for Theory Development within Logistics and Supply Chain Management Research. In Kotzab, H., Seuring, S., Muller, M., Reiner, G. Eds.; *Research Methodologies in Supply Chain Management*. Heidelberg: Physica, 2005; pp. 171–186. 1026
37. Huang, Z.; Shahzadi, A.; Khan, Y.D. Unfolding the Impact of Quality 4.0 Practices on Industry 4.0 and Circular Economy Practices: A Hybrid SEM-ANN Approach. *Sustainability* **2022**, *14*, 15495. <https://doi.org/10.3390/su142315495>. 1027
38. Ritmak, N.; Rattanawong, W.; Vongmanee, V. A New Dimension of Health Sustainability Model after Pandemic Crisis Using Structural Equation Model. *Sustainability* **2023**, *15*, 1616. <https://doi.org/10.3390/su15021616>. 1028
39. Stoelting, R. Structural Equation Modeling/Path Analysis. [online]. **2002** Available from <http://userwww.sfsu.edu/~efc/classes/biol710/path/SEMwebpage.htm>. 1029
40. Mulaik, S.A. A brief history of the philosophical foundations of exploratory factor analysis. *Multivariate Behavioral Research* **1987**, *22*, pp. 267–305, DOI: [10.1207/s15327906mbr2203_3](https://doi.org/10.1207/s15327906mbr2203_3); https://doi.org/10.1207/s15327906mbr2203_3. 1030
41. Mulaik, S.A. *Factor Scores and Factor Indeterminacy. Foundations of Factor Analysis*. 2nd ed.; Chapman and Hall/CRC: London, United Kingdom, **2009**. 1031

42. Rhemtulla, M.; Brosseau-Liard, P.; Savalei, V. (2012): When Can Categorical Variables Be Treated as Continuous? A Comparison of Robust Continuous and Categorical SEM Estimation Methods Under Suboptimal Conditions. *Psychological Methods* **2012**, *17*(3), pp. 354–373, 10.1037/a0029315. 1064
43. Xia, Y.; Yang, Y. RMSEA, CFI, and TLI in structural equation modeling with ordered categorical data: The story they tell depends on the estimation methods. *Behav Res* **2019**, *51*, pp. 409–428. <https://doi.org/10.3758/s13428-018-1055-2>. 1065
44. Torun, E.D. Educational Use of Social Media in Higher Education: Gender and Social Networking Sites as the Predictors of Consuming, Creating, and Sharing Content. *Acta Educ. Gen.* **2020**, *10*, 112–132. <https://doi.org/10.2478/atd-2020-0013>. 1066
45. Hu, L.-T.; Bentler, P.M. Fit indices in covariance structure modeling: Sensitivity to underparameterized model misspecification. *Psychol. Methods* **1998**, *3*(4), pp. 424–453. <https://doi.org/10.1037/1082-989X.3.4.424>. 1067
46. Jöreskog, K.G.; Sörbom, D. *LISREL 8: Structural Equation Modeling with the SIMPLIS Command Language*; Scientific Software International: Skokie, IL, USA, **1993**. 1068
47. Marsh, H.W.; Balla, J.R.; McDonald, R.P. Goodness-of-fit indexes in confirmatory factor analysis: The effect of sample size. *Psychol. Bull.* **1988**, *103*, 391–410. <https://doi.org/10.1037/0033-2909.103.3.391>. 1069
48. Schermelleh-Engel, K.; Moosbrugger, H.; Müller, H. Evaluating the Fit of Structural Equation Models: Tests of Significance and Descriptive Goodness-of-Fit Measures. *Methods Psychol. Res.* **2003**, *8*, 23–74. 1070
49. Bentler, P.M.; Bonett, D.G. Significance tests and goodness of fit in the analysis of covariance structures. *Psychological Bulletin* **1980**, *88*, pp. 588–606. 1071
50. Bentler, P.M. Multivariate analysis with latent variables: Casual modeling. *Annu. Rev. Psychol.* **1980**, *31*, 419–456. 1072
51. Marsh, H.W.; Hau, K.-T.; Artelt, C.; Baumert, J.; Peschar, J.L. OECD's Brief Self-Report Measure of Educational Psychology's Most Useful Affective Constructs: Cross-Cultural, Psychometric Comparisons Across 25 Countries. *Int. J. Test.* **2006**, *6*, 311–360. https://doi.org/10.1207/s15327574ijt0604_1. 1073
52. Browne, M. W.; Cudeck, R. Alternative Ways of Assessing Model Fit. *Sociological Methods & Research* **1992**, *21*(2), pp. 230–258. <https://doi.org/10.1177/0049124192021002005>. 1074
53. Byrne, B.M.; Campbell, T.L. Cross-Cultural Comparisons and the Presumption of Equivalent Measurement and Theoretical Structure: A Look Beneath the Surface. *Journal of Cross-Cultural Psychology* **1999**, *30*(5), pp. 555–574. <https://doi.org/10.1177/0022022199030005001>. 1075