

The resilience of public administration to hybrid threats in the context of sustainable competitiveness of a country

Koraus Antonin, Palinchak Mykola, Miroslav Gombar, Stehlikova Beata

Abstract

The aim of the article is to identify the most important factors needed for the functioning of public administration so that it is capable of effectively facing hybrid threats, determining their weights. The results clearly show that competitiveness and the quality of public administration are strongly and significantly correlated. This is exploratory research and is a quantitative study based on the type of data used. Hybrid threats represent a serious risk for the security and stability of a state, as they can be used to destabilise a political system, disrupt economic growth or endanger national security. Therefore, public administration must be resilient to hybrid threats. For this reason, determining which factors have the greatest influence on the resilience of public administration to hybrid threats is a topical issue. We selected four factors on the basis of expert analyses, and we chose the Analytical Hierarchy Process (AHP) for processing expert opinions acquired via questionnaires. We assessed the consistency of the responses using the Consistency Ratio. From the calculations, we concluded that Slovak experts consider the following as the most important factors for the functioning of public administration so that it can effectively face hybrid threats: ensuring compliance with laws and security, avoiding a national debt crisis, ensuring cyber security and ensuring resilience against disinformation.

Keywords: *country competitiveness, public administration, hybrid threats, AHP, increasing resilience, quality of public administration*

JEL Classification: H00, H12

1 INTRODUCTION

The security environment in Europe has seen fundamental changes in recent years, and as a result, already known conventional threats have acquired a completely new dimension and a raised intensity due to the development of technology.

In its global strategy, the EU defined hybrid threats as being among the most serious security challenges for the EU and its citizens, and in this context, the battle against hybrid threats should be based on the recommendations previously defined in EU documents and EU-NATO cooperation agreements in order to ensure the highest possible effectiveness of the measures taken.

Competitiveness and the quality of public administration are closely linked. The quality of public administration can affect a country's competitiveness in a number of ways. Public administration can support a country's competitiveness by investing in business. This can be done by creating a favourable business environment, supporting research and development and ensuring education and training. Public administration may also support a country's competitiveness by investing in infrastructure. It can also support a country's competitiveness by being efficient. This means it should be capable of providing services efficiently and

affordably. Public administration should also be transparent and it should act with all laws and regulations.

When public administration is of good quality, it can create a favourable business environment, which can in turn lead to economic growth, increased employment and improved living standards. On the other hand, public administration of low quality can have a negative impact on a country's competitiveness, which can lead to capital outflows, job losses and reduced living standards. Therefore, if countries want to be competitive on the global market, it is important that they invest in the quality of public administration.

2 THEORETICAL BACKGROUND

Hybrid threats are complex and sophisticated attacks that use a combination of traditional and non-traditional methods to target political, economic and military targets. They can be used to undermine public trust, destabilise governments and make it more difficult to do business.

Definitions of hybrid threats vary, and there is no clearly accepted definition of a hybrid threat. They must remain flexible to respond to their evolving nature. However, it cannot be said that there is a consensus on how hybrid threats should be defined. For this reason, Gökce's (2017) study focuses on creating a framework for the hybrid threat concept. Definitions within the EU and NATO also differ (Zandee, van der Meer and Stoetman 2021). An article by Pawlak (2017) outlines new areas of practical EU-NATO cooperation, especially regarding hybrid threats.

Public administration is purposively understood in the broadest possible meaning as “the process of translating public policies into results” (Kettl, 2018). Tittlova et al. (2021) state that public administration is one of the crucial components by which a state and its power are exercised. In public administration, public authorities decide on the rights, legally protected interests and obligations of natural persons and legal entities.

According to Giannopoulos et al. (2021), public administration exists to implement laws and regulations, but though this concept is clear in theory, it can be difficult to apply in practice.

The competitiveness and resilience of public administration to hybrid threats are closely linked, and the resilience of public administration against hybrid threats is essential for maintaining a country's competitiveness.

Public administration must be able to resist hybrid threats in order to protect a country's interests. According to Profiroiu & Nastaca (2021), public administration must deal with the constant changes that affect contemporary society and continue to ensure the well-being of citizens. In consequence, public institutions should strengthen their ability to handle unforeseen situations, specifically to become resilient to different types of shocks.

Article by Dalgaard-Nielsen (2017) examines the resulting managerial dilemmas through interviews with Danish managers attempting to find a balance between resilience, fiscal austerity and democratic accountability. The ability of an organisation to cope with environmental uncertainties, hybrid threats, crises and unexpected events depends on their own resilience (Ince et al., 2017). But worldwide, the evidence is irrefutable high income per capita economies have the most efficient and effective public institutions (Thijs et al., 2017).

Public administration plays an important role in supporting the competitiveness of businesses by providing infrastructure, education, research and development. Public administration can also support the competitiveness of businesses by creating a favourable business environment.

The competitiveness of a country and the resilience of its public administration are two important aspects that affect a country's prosperity and security. A country's competitiveness is its ability to successfully manage and compete on the global market. Its resilience rests in its

ability to withstand and recover from crises and shocks.

In public administration, ensuring sustainable competitiveness in the case of hybrid threats must be done by means of proactive steps that can anticipate, prevent and effectively respond to such dangers. Public administration authorities must make a comprehensive assessment of potential risks with an emphasis on the hierarchical identification of potential hybrid threats and their eventual impact on the smooth and problem-free provision of all essential activities.

Resilience and thus also the resilience of public administration means the ability to return to the original state after a destructive event or worsening situation (Bhamra et al., 2011). Management in public administration should implement flexible decision-making processes and should be able to respond promptly to hybrid dangers that arise. Public administration must implement effective management systems (Borgonovi et al., 2021). Spodná časť formulára

It is necessary education and the professional training of workers are aimed not only at the acquisition of knowledge, but also strengthening the necessary skills for effective resolution and response in critical situations in areas such as cyber security, information analysis, risk management and communication in difficult crisis situations. An ever-increasing volume of information flows through the network, including messages regarding potential future risks such as hybrid threats (Ronchi, 2020). It is greatly important to obtain and to maintain long-term public trust and ensure an effective flow of information about hybrid threats.

By accepting critical factors, public administration can significantly increase its ability to manage respond to hybrid threats effectively and to support the sustainability of the country's competitiveness.

The aim of the contribution is to identify the most important factors needed for the functioning of the public administration so that it can effectively face hybrid threats and determine their weights.

3 RESEARCH OBJECTIVE, METHODOLOGY AND DATA

We measure competitiveness using the Global Sustainable Competitiveness Index (GSCI). The GSCI measures the competitiveness of countries based on 189 measurable, quantitative indicators based on reliable sources, such as the World Bank, the IMF and the United Nations.

A study by the EU Joint Research Centre and the European Centre of Excellence for Countering Hybrid Threats identified 13 different areas of potential hybrid threats: infrastructure, cyberspace, space, the economy, military/defence, culture, social/community, public administration, legal, intelligence, diplomacy, political and information. In our view, this is the most comprehensive view of hybrid threats. The first step was to identify the key factors that can influence the functioning of public administration in the case of hybrid threats. Based on expert analysis, we selected four factors which are essential for the functioning of the public administration so that it is able to effectively confront hybrid threats and support a country's competitiveness.

Cyber security (CS)

Cyber security is understood as the state in which networks and information systems are capable of resisting with a certain degree of reliability any action that endangers the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or related services provided or made accessible through these networks and information systems. It is necessary to professionally and technically secure more effective prevention and detection of cyber incidents in the public administration environment and a more effective reaction to cyber incidents in the entire economy, with an emphasis on the sustainability of the country's

competitiveness (Wallden, Kashefi, 2019; Wang et al. , 2020; Von Solms, B. & Von Solms, R., 2018; Perwej et al., 2021).

Resistance to disinformation (RI)

Disinformation is part of a wider process of information influencing, which is referred to as information operations. Information operations can, along with targeted spreading of potentially harmful information, also include the gathering of sensitive data, inciting people to action (violent or nonviolent) and overtly or covertly promoting a particular party (such as the state). Creating and spreading disinformation is a growing problem (Shu et al., 2020, Freelon, and Wells, 2020; McKay and Tenove, 2021). Integrated strategies must be created to combat disinformation, which will not only weaken the operations of hostile actors, but also strengthen the resilience and critical thinking of the population and, ultimately, the competitiveness of the country.

Compliance with laws and safety (LS)

Public administration represents one of the crucial components through which the state and its power are exercised. How regulations are implemented and enforced is important. In public administration, public authorities decide on the rights that protect the interests and obligations of natural persons and legal entities. Regulations, both legal and administrative, determine behaviour within a government and outside it (Hildebrandt, 2018). A society ensures the safety of persons and property, which is one of the defining aspects and the basic function of every rule of law. It is also a prerequisite for the carrying out the rights and freedoms that the rule of law applies.

Prevention of crisis level – General government debt (DG)

General government debt is a major fiscal indicator that represents the state of public finances. Public debt is usually expressed as the ratio of debt-to-GDP expressed as a percentage. Gross debt has a significant impact on a country's competitiveness, particularly in connection with the application of the constitutional law on budgetary responsibility.

In the following text, we will use the acronyms already presented.

To conduct our research, we addressed 15 experts, as defined above, but only 9 of them, all from Slovakia, showed interest in cooperating in the research. Tab. 1 shows the most important characteristics of the participating experts.

Tab. 1 – Characteristics of the participating experts

Education	Professional experience (years)	Major responsibilities/ job title
Full Professor Dipl. Ing., Ph.D. or Full Professor JUDr. */ Ph.D.	41, 33	Academic employee at a university
Associate Professor Dipl. Ing. Ph.D. or Associate Professor JUDr.*/ Ph.D.	20, 17, 27	Academic employee at a university
Associate Professor Dipl. Ing., Ph.D.	31	Researcher at the SAS**/

Education	Professional experience (years)	Major responsibilities/ job title
JUDr.*/, Ph.D.	16	Senior employee in public administration
JUDr.*/	19, 22	Senior employee in public administration

Comment :*/ iuris utriusque doctor, JD, JUDr; **/ Slovak Academy of Sciences

Source: own processing based on data provided by experts

For processing the expert opinions acquired via questionnaires we used the Analytical Hierarchy Process (AHP) method (Kulakowski, 2020; Munier and Hontoria, 2021; Costa et al., 2022). Psychologists say that it is easier and more exact to express one's view on only two alternatives than on all alternatives at the same time. With pairwise comparison of criteria, experts (we will mark the number of experts as k) compared pairs of criteria in the questionnaire and judged their importance. We know several scales for pairwise comparisons from Ishizaka & Labib (2011). For comparisons, the experts used the nine-point rating scale proposed by Saaty (1990).

If two criteria are considered to be equally important, then a score of one is assigned. If the criterion on the left side is considered more important than the one on the right side, it is assigned a score from 2 to 9 (in transcription with a minus sign). Conversely, when the right-hand criterion is considered to be more important, a score from 2 to 9 (in transcription with a plus sign) is assigned to the comparison.

The experts marked their answers in the questionnaire. The advantage of AHP is that when comparing n indicators, we must only make $N = n(n-1)/2$ comparisons. In our case, we are comparing 4 indicators, i.e. $n = 4$ and the number of comparisons N is $4(4-1)/2 = 6$. So, the questionnaire is short. Let's give a specific example: when an expert considers Cyber security (CS) to be "strongly important" (the point rating is 5) versus Resistance to misinformation (RI). In the transcription, this is the value $q_{12} = -3$.

We mark as $\mathbf{Q}^{(r)}$ the matrix of values (of size $1 \times N$) transcribed from the questionnaire for expert r . The values from the matrix $\mathbf{Q}^{(r)}, r = 1, 2, \dots, k$

$$\mathbf{Q}^{(r)} = (q_{12}^{(r)} \quad q_{12}^{(r)} \quad \dots \quad q_{1n}^{(r)} \quad q_{23}^{(r)} \quad \dots \quad q_{2n}^{(r)} \quad \dots \quad q_{n(n-1)}^{(r)})$$

we transform into Saaty's matrix $\mathbf{S}^{(r)}, r = 1, 2, \dots, k$. We replace the positive values of the matrix $\mathbf{Q}^{(r)}$ with their reciprocal values, and we replace the negative values with their absolute value. The values on the diagonal are 1. We fill in the lower part of the matrix below the diagonal using the relationship $a_{ij} = \frac{1}{a_{ji}}$. For the elements of Saaty's matrix \mathbf{S} $a_{ij} = 1/a_{ji}$ applies for all $i, j = 1, 2, \dots, n$.

$$\mathbf{S}^{(r)} = \begin{pmatrix} 1 & a_{12}^{(r)} & \dots & a_{1n}^{(r)} \\ \vdots & & \ddots & \vdots \\ a_{n1}^{(r)} & a_{n2}^{(r)} & \dots & 1 \end{pmatrix},$$

where

$$a_{ij} = \begin{cases} 1 & \text{for } i = j \text{ pre } i, j = 1, 2, \dots, n \\ 1/q_{ij} & \text{for } q_{ij} > 0; i = 1, 2, \dots, n; j = i + 1, \dots, n \\ |q_{ij}| & \text{for } q_{ij} < 0; i = 1, 2, \dots, n; j = i + 1, \dots, n \\ \frac{1}{a_{ji}} & ; i = 2, \dots, n; j = 1, \dots, i - 1 \end{cases}$$

For the sample value $q_{12} = -3$ from the previous example, we get the Saaty matrix elements $a_{12} = 3$ and $a_{21} = \frac{1}{3}$.

However, the priorities calculated from pairwise comparisons only have meaning, if they are derived from consistent or almost consistent matrices. In the next step, we verified whether the answers were sufficiently consistent, i.e. whether any inconsistencies exist within the pairwise comparison of individual criteria.

The comparison of matrix **S** is consistent if $a_{ij} a_{jk} = a_{ik}$ for all values i, j, k ($i, j, k = 1, 2, \dots, n$). Such an ideal state does not happen for several reasons. Our scale is limited by the value 9, therefore, we cannot assign values greater than 9. Another source of inconsistency arises because we are dealing with human judgment, and even a simple lack of concentration can cause inconsistency. When we do not have sufficient information to make consistent comparisons, we use our judgment, and sometimes our judgment is not as accurate as we would like. Therefore, we have to use one of the consistency verification methods. Several methods have been proposed to measure consistency (Ishizaka & Labib, 2011, Golden & Wang, 1989). We will use a procedure presented by Saaty (1977), who proposed the Consistency Index (CI)

$$CI = \frac{\lambda_{max} - n}{n - 1},$$

where λ_{max} is the largest eigenvalue of the Saaty matrix **S** and n is the number of criteria. We evaluate the consistency of responses using the Consistency Ratio (CR), which is a comparison between the Consistency Index (CI) and the Random Consistency Index (RI)

$$CR = \frac{CI}{RI},$$

where CI is the consistency index and RI is the Random Consistency Index (Saaty & Tran, 2007). In the article, we will use RI values according to Saaty (1977). The RI values derived from the simulations of different authors are given by Franek & Kresta (2014).

Judgments that have a CR lower than 0.1 are reasonable; lower than 0.2 is tolerable, and higher than 0.2 should be revised or discarded (Saaty, 1980). If the value of CR is larger than required, we can do the following (Saaty & Tran, 2007): We find the most inconsistent judgment in the matrix; we then determine the range of values to which this judgment can be changed, according to which the inconsistency would be improved, and we ask the expert to consider, if possible, to change the judgment to a plausible value in that range. If the expert is not willing, we then try with the second most inconsistent judgment. It may occur that the knowledge of experts does not allow consistency to be improved, and more information is needed to improve consistency. We were unable to apply this procedure, as the questionnaires we used were anonymous. Therefore, we used Harker's procedure for automatic inconsistency correction, but only for those assessments for which the Consistency Ratio (CR) is tolerable (lower than 0.2) or at most 0.22. We excluded the others from further processing.

Often it is difficult to achieve consensus with a large number of persons or persons distant in interest. AHP can be applied to group evaluations. The evaluation of several experts will avoid any bias that may be present in the assessment of a single expert (Ishizaka & Labib, 2011). The

individual assessments of the evaluating experts can be aggregated into one aggregated matrix \mathbf{G} . Aczel & Saaty (1983) proved a theorem that group judgments can be synthesised suitably with the geometric mean. The elements of the aggregate matrix \mathbf{G} represent the geometric mean of the relevant elements of the Saaty comparison matrices $\mathbf{S}^{(1)}, \mathbf{S}^{(2)}, \dots, \mathbf{S}^{(k)}$, i. e.

$$g_{ij} = \sqrt[k]{\prod_{r=1}^k a_{ij}^{(r)}}.$$

Pairwise comparison is used to estimate the preference values of the final alternatives with respect to a given criterion. Choo and Wedley (2004) discuss 18 methods for deriving preference values from pairwise judgment matrices. The main challenge is how to harmonise the inevitable inconsistency of the comparison matrix. The indicator weights and rankings for the individual experts are the normalised values of the eigenvector v corresponding to the largest eigenvalue λ_{max}

$$(\mathbf{S} - \lambda_{max}\mathbf{I}).v = 0,$$

where \mathbf{S} is the Saaty matrix, \mathbf{I} is the unit matrix.

Using the Pearson correlation coefficient (Gupta, & Kapoor, 2020), we assess the dependence of competitiveness and quality of public administration in EU countries.

We performed the calculations in the R environment.

4 RESULTS AND DISCUSSION

The value of the Pearson correlation coefficient between GSCI and WGI for EU countries is high at 0.7475 and is significant (the p-value is 7.45E-06). This means that in EU countries there is a strong linear dependence between competitiveness, as measured by GSCI, and the quality of public administration.

Hybrid threats represent a serious risk to the security and stability of a state. They can be used for destabilising a political system, disrupting economic growth or endangering national security. Therefore, public administration must be resistant to hybrid threats.

Not all factors that are necessary for the functioning of public administration so that it is able to effectively face hybrid threats and support the competitiveness of the country have the same weight. In order to identify the importance of the factors, we contacted 15 experts from Slovakia, 9 of whom agreed to participate. Their results are given in the following Tab. 2.

Tab. 2 – Results of a questionnaire survey of nine experts (\mathbf{Q} matrix)

Expert	CS_RI	CS_LS	CS_DG	RI_LS	RI_DG	LS_DG
Expert 1	-5	5	-5	3	-3	-5
Expert 2	-3	1	3	3	3	1
Expert 3	-3	1	3	3	5	1
Expert 4	-9	1	-9	9	-7	-9
Expert 5	-5	5	3	7	7	-3
Expert 6	1	7	7	7	5	1
Expert 7	-5	1	7	5	7	1
Expert 8	-5	1	1	5	7	1
Expert 9	1	-5	-7	7	7	-9

Source: own processing

The Saaty matrix for Expert 1 is

$$S^{(1)} = \begin{pmatrix} 1 & 5 & 1/5 & 5 \\ 1/5 & 1 & 1/3 & 3 \\ 5 & 3 & 1 & 5 \\ 1/5 & 1/3 & 1/5 & 1 \end{pmatrix}.$$

We created the other Saaty matrices analogously. We then calculated the Consistency Ratio CR values, which are presented in Tab. 3.

Tab. 3 – Values of the Consistency Ratio (CR)

Expert1	Expert2	Expert3	Expert4	Expert5	Expert6	Expert7	Expert8	Expert9
0.2168	5.82e-02	4.35e-02	0.1911	9.07e-02	5.35e-03	0.1625	5.35e-03	0.5316

Source: own processing

Due to the high Consistency Ratio value (0.53164), we excluded Expert 9 from further processing, as we consider his answers to be inconsistent. The answers of Expert 1, Expert 4 and Expert 7 were inconsistent (greater than 0.10), but acceptable; therefore, we applied the Harker procedure (1987) and acquired a Q matrix with the following values.

Tab.4 – Results of the questionnaire survey of experts after Harker's modification (Q matrix)

	CS_RI	CS_LS	CS_DG	RI_LS	RI_DG	LS_DG
Expert 1	-1.1425	5	-5	3	-3	-5
Expert 2	-3	1	3	3	3	1
Expert 3	-3	1	3	3	5	1
Expert 4	-9	1	-9	9	-1	-9
Expert 5	-5	5	3	7	7	-3
Expert 6	1	7	7	7	5	1
Expert 7	-5	1	7	5	7	3.5997
Expert 8	-5	1	1	5	7	1

Source: own processing

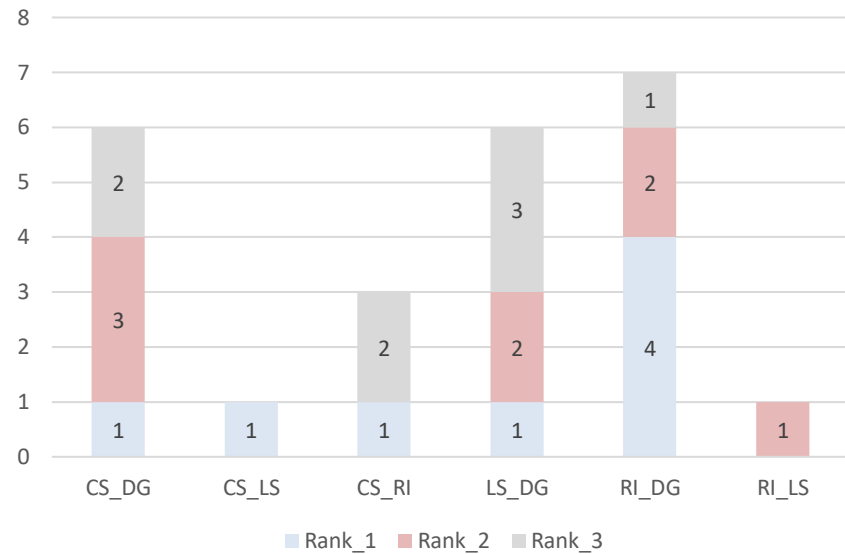
All the values of the Consistency Ratio are less than 0.10; we can thus conclude that the answers modified in this way are consistent (Tab. 5).

Tab. 5 – Values of the Consistency Ratio CR for the adjusted matrix Q

Expert1	Expert2	Expert3	Expert4	Expert5	Expert6	Expert7	Expert8
8.58e-02	5.82e-02	4.35e-02	3.35e-16	9.07e-02	5.35e-03	9.62e-02	5.35e-03

Source: own processing

Fig. 1 contains the data framework of the three most inconsistent pairwise comparisons made by each expert. The most inconsistent pairwise comparisons occurred in the Net debt of general government (DG). It was difficult for experts to compare this economic indicator with the other indicators. By far the fewest problems occurred with the comparison of the importance of Compliance with laws and safety (LS).



Source: own processing

Fig. 1 – The most inconsistent pairwise comparisons made by experts

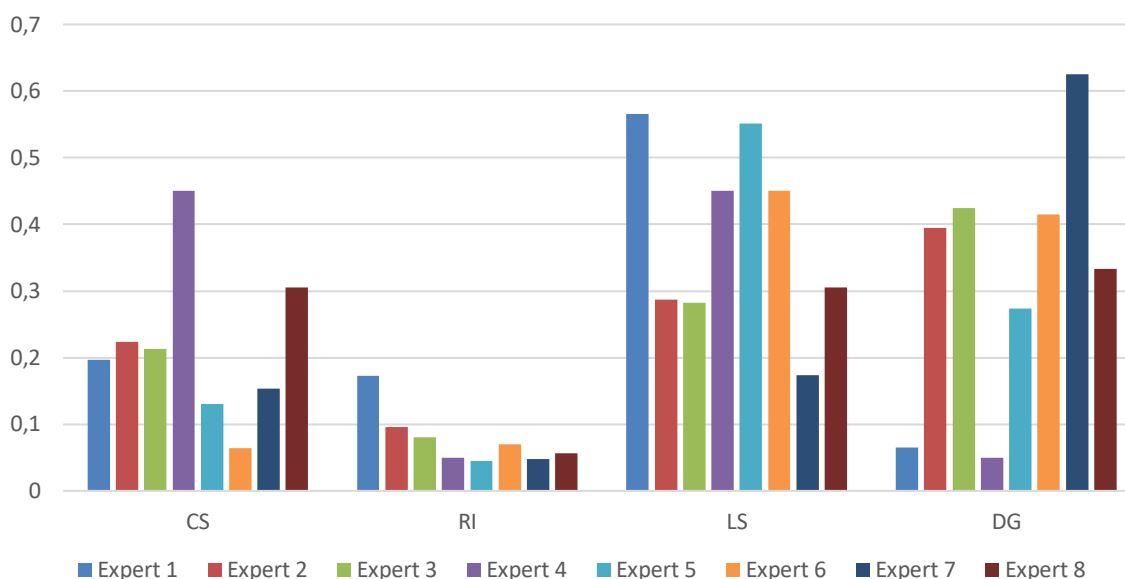
In the next step, we determined the weights of individual indicators. These are presented in Tab. 6, including their rank.

Tab. 6 – Indicator weights and order of indicators for individual experts

Expert	Weight				Rank			
	CS	RI	LS	DG	CS	RI	LS	DG
Expert 1	0.1968	0.1723	0.5658	0.0651	2	3	1	4
Expert 2	0.2234	0.0956	0.2867	0.3943	3	4	2	1
Expert 3	0.2132	0.0802	0.2820	0.4246	3	4	2	1
Expert 4	0.4500	0.0500	0.4500	0.0500	1.5	3.5	1.5	3.5
Expert 5	0.1307	0.0444	0.5511	0.2737	3	4	1	2
Expert 6	0.0643	0.0702	0.4502	0.4152	4	3	1	2
Expert 7	0.1538	0.0475	0.1736	0.6250	3	4	2	1
Expert 8	0.3052	0.0563	0.3052	0.3333	3	4	2	1

Source: own processing

In Fig. 2 we see the weights of the individual indicators for all eight experts. Cyber security (CS) was considered to be the most important by expert 4, though it was not ranked first by any expert. In the case of expert 4, the first and second places were shared by Cyber security and Compliance with laws and safety (LS). The answers suggest to us that the issue of Cyber security (CS) in public administration is underestimated.



Source: own processing

Fig. 2 – Weights of individual indicators for all eight experts

The issue of cyber security, however, does not only affect highly specialised workplaces or institutions with sensitive data. Every district office, regional directorate or other public administration authority with an Internet connection represents a potential target for hybrid threats. The vulnerability of public administration grows continually in the context of moving the means of communication and management processes in almost all spheres of life from the real to the virtual world, especially in the area of critical infrastructure management, Industry 4.0 concepts, the Internet of Things and others. Public administration workplaces are becoming an attractive target for cybercriminals who can gain access to personal data files or gain control over intelligently operated city resources. Therefore, public administration should adopt, implement and maintain protective systems (resources, processes and management of interested participants) for state security as soon as possible, according to Sivák (2019). Sivák (2019) also says that Slovakia can improve cyber security in public administration mainly by ensuring regular cyber security audits, improving the strong connection of the legal system in the field of cyber security to the field of critical infrastructure and supplementing it with other elements of information security while raising the level information and cyber security.

It is interesting that the weight of Resistance to disinformation (RS) was low for all experts and has a rank of 3 or 4, though Expert 1 gave it the highest weight of all the experts.

Compliance with laws and safety (LS) has a high weight in case of the individual evaluations of all the experts. Compliance with legal provisions is the process by which a society adheres to complex rules, policies and procedures. Public administration represents one of the crucial components by which the state and its power are exercised. In public administration, public authorities make decisions on the rights, legally protected interests and obligations of natural persons and legal entities, and regulations, both legal and administrative, determine behaviour within and outside government. How regulations are implemented and enforced is important. Corruption is a phenomenon that deforms the work of public administration and violates the principles underlying the legal actions of public administration and its bodies. The key is creating such a legislative, personnel and material environment that corruption has no chance to be applied, thus ensuring the safety of persons and property. Security is one of the defining aspects of any society governed by the rule of law and is a fundamental function of the state. It

is also a prerequisite for application of the rights and freedoms that the rule of law seeks to advance.

Aside from Expert 1 and Expert 4, all the experts, according to the AHP, place high importance on the net general government debt (DG). When compiling the questionnaire, we were a little worried about the inclusion of an economic indicator, but from a theoretical point of view it is very important. The experts were truly excellent, and we can see in their answers that they did not defend narrowly focused interests. They made their evaluations with insight. Indeed, examples from history show that a national debt crisis can result in civil unrest. Lazarou & Stanicek (2021) say that a high level of debt affects the state's ability to provide basic means of public services, which in turn are a key source of government legitimacy. Exceptionally high debt, particularly foreign debt, means increased exposure for the country to global market risks and creditor decisions, making the state very vulnerable to external economic shocks (Weltwirtschaftsforum & Zurich Insurance Group, 2019). Unsustainable borrowing and debts can worsen the basis of societal division, especially when real or perceived inequalities increase and result in civil unrest.

The consistency ratio (CR) for Saaty's matrix of aggregated individual judgements is 0.0076, i.e. the aggregate matrix is consistent.

From the above calculations, we can conclude that Slovak experts consider the following to be the most important factors for the functioning of public administration to be able to effectively face hybrid threats :

- Ensuring compliance with laws and security (LS) – weight 41.62%,
- Avoiding a sovereign debt crisis (DG) – weight 28.23%,
- Ensuring cyber security (CS) – weight 22.02%,
- Ensuring resistance to disinformation (RI) – weight 8.13%.

5 CONCLUSION

The strong linear dependence (significant Pearson coefficient) between competitiveness and the quality of public administration means that these two parameters are closely interconnected and that a change in one parameter leads to a change in the other in the same direction. In the specific case of EU countries, this means that countries with a higher quality of public administration tend to be more competitive. There are several reasons why there is such a strong correlation between these two quantities. Quality public administration is necessary to create and maintain a suitable business environment. Public administration is responsible for providing basic services, such as infrastructure, education and health care, which are important for business, and is also responsible for creating and implementing policies that support competition and innovation. High quality public administration can help businesses reduce costs and increase productivity. For example, transparent and efficient government institutions can lower the costs of doing business simplifying regulatory processes and improving the protection of property rights. Good quality public administration can help businesses access new markets and thus opportunities. For example, effective government institutions can help businesses export their products and services abroad. All of these factors contribute to the fact that countries with a higher quality of public administration as a rule are more competitive. There are, of course, other factors that influence a country's competitiveness, such as the quality of human resources, the level of innovation and the openness of the economy, but the quality of public administration is an important factor that needs to be considered when assessing a country's competitiveness.

Underestimating disinformation (weight 8.13%) can have many negative consequences. Disinformation can undermine people's trust in public institutions, such as governments, the

media, and this can subsequently have a negative impact on democracy and governance. Disinformation can be used to spark violence and hatred against certain groups of people, leading to social tension and conflict. Disinformation may lead to worsening economic outcomes by damaging confidence in business and investment.

Ensuring cyber security (CS) has a weight of 22.02%. It should be noted that a cyberattack can have serious consequences for public administration. A cyberattack, for example, can result in a blackout of electricity, water supply or a disruption of health care. It can lead to a loss of public confidence in the public administration if the public believes that the public administration cannot protect its systems and information. A cyberattack can lead to economic damage, if business operations are disrupted.

It is important that public administration takes measures to ensure its own cyber security. These measures should include investments in security software and technology, educating employees about cyber security, implementing security procedures and policies and cooperation with other organisations, such as the private sector and civil society.

For public administration, the **prevention of a sovereign debt crisis** (28.23%) is important for the several reasons.

A sovereign debt crisis may lead to economic recession. If the state gets into a situation where it is unable to repay its debt, this can lead to an increase in interest rates and a decrease in investment, which can then lead to a slowdown in economic growth and an increase in unemployment. A sovereign debt crisis can lead to social unrest. If the public believes that the state is unable to provide basic services, this can lead to social unrest, which may in turn lead to violence, unrest and destabilisation of the state.

Ensuring compliance with the law and security is the role of all public administration authorities, including the police, courts and security elements. These authorities must cooperate to ensure that laws are followed and that citizens are kept safe. According to the study, the most important matter for public administration is **ensuring compliance with laws and security** (41.62%). Laws and safety measures are necessary for the functioning of society. Without them, it would be difficult to maintain order and peace. It is important that public administration pay sufficient attention to ensuring compliance with the law and security.

The research carried out in the V4 countries confirmed that the results for other countries may be different (article in the stage of preparation for publication). This may occur due to a different current situation, particularly in the economic, political, legislative areas and in the assessment of domestic experts of the most important factors necessary for the functioning of public administration.

Acknowledgement

The contribution was created within the national project “Increasing Slovakia’s resilience to hybrid threats by strengthening public administration capacities”, project code ITMS2014+:314011CDW7. This project is supported by the European Social Fund.

References

1. Ali, S. E. A., Lai, F. W., Aman, A., Saleem, M. F., & Hamad, S. (2022). Do Information Security Breach and Its Factors Have a Long-Run Competitive Effect on Breached Firms. Equity Risk? *Journal of Competitiveness*, (1), 23-42. <https://doi.org/10.7441/joc.2022.01.02>

2. Bhamra, R., Dani, S., & Burnard, K. (2011). Resilience: the concept, a literature review and future directions. *International Journal of Production Research*, 49(18), 5375-5393. <https://doi.org/10.1080/00207543.2011.563826>
3. Borgonovi, E., Bianchi, C., & Rivenbark, W. C. (2019). Pursuing community resilience through outcome-based public policies: Challenges and opportunities for the design of performance management systems. *Public Organization Review*, 19, 153-158 <https://doi.org/10.1007/s11115-017-0395-1>
4. Costa, I. P. D. A., Costa, A. P. D. A., Sanseverino, A. M., Gomes, C. F. S., & Santos, M. D. (2022). Bibliometric studies on multi-criteria decision analysis (mcda) methods applied in military problems. *Pesquisa Operacional*, 42, e249414.
5. Cullen, P., Juola, C., Karagiannis, G., Kivisoo, K., Normark, M., Rácz, A., Schmid, J., & Schroefl, J. (2021). *The landscape of Hybrid Threats: A Conceptual Model* (Public Version), Giannopoulos, G., Smith, H., & Theocharidou, M. (eds). EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, <https://doi.org/doi:10.2760/44985>. Available on https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf.
6. Dalgaard-Nielsen, A. (2017). Organizational resilience in national security bureaucracies: Realistic and practicable?. *Journal of Contingencies and Crisis Management*, 25(4), 341-349. <https://doi.org/10.1111/1468-5973.12164>
7. EUGS. (2016). *Shared Vision, Common Action: A Stronger Europe*. A Global Strategy for the European Union's Foreign and Security Policy. Available on https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf
8. Golden, B. L., & Wang, Q. (1989). An Alternate Measure of Consistency. In: Golden, B.L., Wasil, E.A., Harker, P.T. (eds) *The Analytic Hierarchy Process*. Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-642-50244-6_5
9. Gupta, S. C., & Kapoor, V. K. (2020). *Fundamentals of mathematical statistics*. Sultan Chand & Sons.
10. Gökce, O. (2017). Definition and scope of hybrid threats. *Inquiry-Sarajevo Journal of Social Science*, 3(1), 19-30.
11. Harker, P. (1987). Incomplete pairwise comparisons in the analytic hierarchy process." *Mathematical Modelling*, 9(11), 837- 848. Available on <http://www.sciencedirect.com/science/article/pii/0270025587905033>
12. Hildebrandt, M. (2018). Algorithmic regulation and the rule of law. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 376(2128), 20170355. <http://dx.doi.org/10.1098/rsta.2017.0355>
13. Ince, H., Imamoglu, S. Z., Karakose, M. A., & Turkcan, H. (2017). The Search For Understanding Organizational Resilience. In M. Özşahin (Ed.), *Strategic Management of Corporate Sustainability, Social Responsibility and Innovativeness*, vol 34. European Proceedings of Social and Behavioural Sciences. 230-243. Future Academy. <https://doi.org/10.15405/epsbs.2017.12.02.20>
14. Ishizaka, A., & Labib, A. (2011). Review of the main developments in the analytic hierarchy process. *Expert systems with applications*, 38(11), 14336-14345. <https://doi.org/10.1016/j.eswa.2011.04.143>
15. Lazarou, E., & Stanicek, B., (2023). *Mapping threats to peace and democracy worldwide: Normandy Index 2023*, EU Parliamentary Research Service. Belgium.

- Available on
https://policycommons.net/artifacts/4786168/eprs_stu2023751422_en/5622638/
16. Franek, J., & Kresta, A. (2014). Judgment scales and consistency measure in AHP. *Procedia economics and finance*, 12, 164-173. [https://doi.org/10.1016/S2212-5671\(14\)00332-3](https://doi.org/10.1016/S2212-5671(14)00332-3).
 17. Frankie Cho (2019). *ahpsurvey: Analytic Hierarchy Process for Survey Data*. R package version 0.4.1. <https://CRAN.R-project.org/package=ahpsurvey>
 18. Freelon, D., & Wells, C. (2020). Disinformation as political communication. *Political communication*, 37(2), 145-156. <https://doi.org/10.1080/10584609.2020.1723755>
 19. Kettl, Donald F. 2018. *Politics of the Administrative Process*. 7th ed. Los Angeles: CQ Press.
 20. McKay, S., & Tenove, C. (2021). Disinformation as a threat to deliberative democracy. *Political Research Quarterly*, 74(3), 703-717. <https://doi.org/10.1177/1065912920938143>
 21. Kulakowski, K. (2020). *Understanding the analytic hierarchy process*. CRC Press.
 22. Munier, N., & Hontoria, E. (2021). *Uses and Limitations of the AHP Method*. Cham, Switzerland: Springer International Publishing.
 23. Pawlak, P. (2017). *Countering hybrid threats: EU-NATO cooperation*, EPRS: European Parliamentary Research Service. Belgium. Retrieved from <https://policycommons.net/artifacts/1338529/countering-hybrid-threats/1947195/> on 01 Oct 2023. CID: 20.500.12592/j752bj.
 24. Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. *International Journal of scientific research and management*, 9(12), 669-710. <https://doi.org/10.18535/ijssrm/v9i12.ec04>
 - Profiroiu, A. G., & Nastaca, C. C. (2021). What strengthens resilience in public administration institutions?. *Eastern Journal of European Studies*, 12, 100-125 <https://doi.org/10.47743/ejes-2021-SI05>
 25. Pyankova, S., Troyanskaya, M. , & Tyurina, Y. (2021). Digital development and its impact on regions' competitiveness. *Global Economy Journal*, 21(02), 2150010. <https://doi.org/10.1142/S219456592150010X>
 26. Ronchi, A. (2020). Hybrid threats: defence line from the grassroots. *Journal of Defence & Security Technologies*, 84-98. . <https://doi.org/10.46713/jdst.003.5>
 27. R Core Team (2021). *R: A language and environment for statistical computing*. R Foundation for Statistical Computing, Vienna, Austria. URL <https://www.R-project.org/>
 28. Saaty, T.L., & Tran L.T. (2007). On the invalidity of fuzzifying numerical judgments in the Analytic Hierarchy Process. *Mathematical and Computer Modelling*, 46(7), 962 - 975. Decision Making with the Analytic Hierarchy Process and the Analytic Network Process, <https://doi.org/10.1016/j.mcm.2007.03.022>. Available on <http://www.sciencedirect.com/science/article/pii/S0895717707000787>.
 29. Saaty, T. (1977). A scaling method for priorities in hierarchical structures. *Journal of Mathematical Psychology*, 15 (3), 234-281. [https://doi.org/10.1016/0022-2496\(77\)90033-5](https://doi.org/10.1016/0022-2496(77)90033-5)
 30. Saaty, T. L. (1980). *The analytic hierarchy process: planning, priority setting, resource allocation*. New York: McGraw-Hill.
 31. Saaty, T. L. (1990). How to make a decision: the analytic hierarchy process. *European journal of operational research*, 48(1), 9-26. [https://doi.org/10.1016/0377-2217\(90\)90057-I](https://doi.org/10.1016/0377-2217(90)90057-I)

32. Sivák, J. (2019). *Hybridné hrozby na Slovensku*. Bratislava: Globsec. Available on https://www.globsec.org/sites/default/files/2018-01/Hybridne-hrozby-na-SR_6-tematickych-oblasti.pdf
33. Shu, K., Bhattacharjee, A., Alatawi, F., Nazer, T. H., Ding, K., Karami, M., & Liu, H. (2020). Combating disinformation in a social media age. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 10(6), e1385. <https://doi.org/10.1002/widm.1385>
34. Stoian, V. (2016). Corruption in the Defense Sector: Concepts, Practices and Implications for National Security. In *Countering Hybrid Threats: Lessons Learned from Ukraine*, 65-73. IOS Press. <https://doi.org/10.3233/978-1-61499-651-4-65>
35. Tittlova, M., Balog, B., & Kleniar, I. (2021). *Podvodné konania a korupcia vo verejnej správe*. Bratislava: PEVŠ. Available on https://www.paneurowni.com/wp-content/uploads/2021/09/br3_podvodne_konanie_vo_verejnej_sprave_web.pdf
36. Thijs, N., Hammerschmid, G., & Palaric, E. (2017). *A comparative overview of public administration characteristics and performance in EU28*. European Commission, Brussels. Available on https://www.dgaep.gov.pt/upload/Estudos/2018/Comp_overview_PA_characteristics_2018.pdf
37. Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security—what goes where?. *Information & Computer Security*, 26(1), 2-9. <https://doi.org/10.1108/ICS-04-2017-0025>
38. Wallden, P., & Kashefi, E. (2019). Cyber security in the quantum era. *Communications of the ACM*, 62(4), 120-120.
39. Wang, Z., Sun, L., & Zhu, H. (2020). Defining social engineering in cybersecurity. *IEEE Access*, 8, 85094-85115.
40. Weltwirtschaftsforum & Zurich Insurance Group. (2019). *Global risks 2019*. Insight report. Available on http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf
41. Zandee, D., van der Meer, S., & Stoetman, A. (2021). *Countering hybrid threats: Steps for improving EU-NATO cooperation*. Clingendael Institute. <https://www.clingendael.org/sites/default/files/2021-10/countering-hybrid-threats.pdf>

Contact information

prof. Ing. Antonín Korauš, PhD., LL.M., MBA

Academy of the Police Force in Bratislava
 Department of Informatics and Management
 Country: Slovak Republic
 E-mail: antonin.koraus@akademiapz.sk
 ORCID: <https://orcid.org/0000-0003-2384-9106>

prof. Mykola Palinchak, PhD.

Uzhorod National University
 Faculty of International Economic Relations
 Department of International Politics
 Country: Ukraine
 E-mail: f-intrel@uzhnu.edu.ua
 ORCID: <https://orcid.org/0000-0002-9990-5314>

Assoc. prof. Ing. Miroslav Gombár, PhD.

University of Prešov in Prešov

Faculty of Management and Business

Department of Management

Country: Slovak Republic

E-mail: miroslav.gombar@unipo.sk

ORCID: <https://orcid.org/0000-0002-8383-7820>

prof. RNDr. Beáta Stehlíková, CSc.

Slovak University of Technology

Institute of Management

Country: Slovak Republic

E-mail: stehlikovab2@gmail.com

ORCID: orcid.org/0000-0003-1064-6254