Acta Montanistica Slovaca
ISSN 1335-1788
actamont.tuke.sk

Index for Public Administration Resilience Against Hybrid Threats

Antonin KORAUS[1]*, Mykola PALINCHAK[2], Dagmar CAGANOVA[3], Beata STEHLIKOVA[4] *and* ***Miroslav GOMBAR[5]***

Authors' affiliations and addresses:
[1] Antonin Koraus, Academy of the Police force in Bratislava, Sklabinská 1, 835 17 Bratislava, Slovakia
e-mail: antonin.koraus@akademiapz.sk

[2] Mykola Palinchak, Uzhorod National University, Faculty of International Economic Relations, University Street 14, 880 00 Uzhorod, Ukraine
e-mail: mykola.palinchak@uzhnu.edu.ua

[3] Dagmar Caganova, Faculty of management, Comenius University in Bratislava; Odbojárov 10, 820 05 Bratislava, Slovakia
e-mail: dagmar.caganova@fm.uniba.sk

[4] Beata Stehlikova, Slovak University of Technology, Institute of Management, Vazovova 5, 812 43 Bratislava, Slovakia
e-mail: beata.stehlikova@stuba.sk

[5] Miroslav Gombar, University of Prešov, Faculty of Management and Business, 080 01 Presov, Slovakia
e-mail: miroslav.gombar@unipo.sk

***Correspondence:**
Anton Koraus, Academy of the Police force in Bratislava, Sklabinská 1, 835 17 Bratislava, Slovakia
tel.: +42196 105 7384
e-mail: antonin.koraus@akademiapz.sk

Funding information:
European Social Fund,
project code TMS2014+:314011CDW7.

Acknowledgment:
This research was supported by the European Social Fund as part of the project ITMS2014+:314011CDW7 Increasing Slovakia's resilience to hybrid threats by strengthening public administration capacities.

How to cite this article:
Koraus, A., Palinchak, M., Caganova, D., Stehlikova, B. and Gombar, M. (2023). Index for Public administration resilience against hybrid threats. *Acta Montanistica Slovaca*, Volume 28 (4), 1010-1024

DOI:
https://doi.org/10.46544/AMS.v28i4.17

Abstract

EU countries are dependent on the import of many raw materials. The geopolitical situation significantly impacts the European Union's raw materials policy. Hybrid threats are a serious challenge to security and stability in the world. They are very diverse in terms of actors, activities, or tools. The relationship between the EU's raw materials policy and hybrid threats is complex and influenced by a number of factors. In principle, however, it can be said that due to its dependence on importing raw materials from third countries, the EU is more prone to become the object of hybrid threats that these countries can use to promote their interests. The resistance of the public administration to hybrid threats is one of the important factors that can help the EU reduce the risk of threats to raw material policy by hybrid threats. The aim of the contribution is to create a new composite index, KAPA, which measures the resistance of public administration to hybrid threats. The proposed index has five dimensions – cybersecurity, resistance to disinformation, compliance with laws and security, protection against corruption, and prevention of a sovereign debt crisis. When constructing the KAPA index, we start from the apparatus of fuzzy sets. We have drawn all data from reputable, publicly available databases. According to the KAPA index, the countries ranked best are Estonia, Denmark, Finland, Sweden, and the Netherlands. The worst-ranked countries were Greece, Cyprus, Italy, Bulgaria, and Croatia. The results confirmed that fragile states, measured by the Fragile States Index FSI, are also more vulnerable to hybrid threats and have less resilient public administration.

Keywords

Raw material policy, public administration, resilience, hybrid threats, EU, composite index, fuzzy sets

Introduction

The security environment in Europe has seen significant changes in recent years. The rise of Russia as a military and political power is one of the most important changes in Europe's security environment in recent years. Growing Islamic radicalism is also a serious threat to Europe's security. Several terrorist attacks in Europe in recent years have claimed dozens of victims. Migration from Africa and the Middle East is another factor affecting Europe's security environment. Migration may pose a threat to public security as well as to EU security forces. Cybersecurity is an increasingly important component of Europe's security environment, as cyberattacks can have serious consequences for economies, infrastructure, and governments. Thus, Europe is facing new security challenges, one of the most important of them is hybrid threats.

We can define a hybrid threat as a set of coercive and subversive activities, conventional and non-conventional, military and non-military, which both state and non-state entities can use in a coordinated manner to achieve specific goals without a formal declaration of war and beneath the threshold of a typical reaction. Hybrid threats imperil the functioning of democratic societies and try to weaken them from the inside by exploiting their vulnerabilities but also their main achievements, including freedom of speech and expression, media independence, the rule of law, public control of institutions, and democratic political competition or the openness of the market economy. Often, their intention is to deepen social and political polarization at the national and international level, as well as political destabilization, the inciting of social tension, undermining the credibility of the state and public institutions, and an overall weakening of democratic decision-making and value orientation of society.

Hybrid threats can be used to manipulate commodity markets, which can lead to higher prices or shortages of raw materials. This could have serious economic consequences for the EU. In the EU, at least 30 million jobs depend on the availability of raw materials. Hybrid threats can be used to carry out cyber attacks on infrastructure needed for producing or transporting raw materials. This could cause serious disruptions in the supply of raw materials. Hybrid threats can be used to spread propaganda that can influence public opinion on the EU's raw materials policy. This could lead to the EU being less able to assert its interests in raw materials.

Hybrid threats constitute a serious risk to raw material policy. Cyber-attacks can disrupt the supply of raw materials because they can attack the systems needed to transport, process, or store them. Propaganda can be used to undermine trust in public institutions that are responsible for implementing raw materials policy. Economic sanctions can be used to disrupt the supply of raw materials or to increase their prices.

The resilience of public administration to hybrid threats includes the ability of public administration to identify, evaluate, and respond to hybrid threats. This also includes the ability of the public administration to restore its functions in the event that the hybrid threat weakens it. Rapid identification and response, vulnerability reduction, and damage repair are some concrete ways in which public administration resilience to hybrid threats can help the EU reduce the risk that hybrid threats would threaten its raw materials policy.

To the best of our knowledge, no index in the available literature would measure resilience to hybrid threats, nor specifically the resilience of public administration. The aim of the contribution is to create a new composite index, KAPA, which measures the resilience of public administration to hybrid threats. The second goal of the paper is to prove that fragile states, i.e., countries that are vulnerable to conflict, violence, and state collapse, are also more vulnerable to hybrid threats and, at the same time, have less resilient public administration.

Literature Review

Glenn (2009) defines a hybrid threat as a combination of political, military, economic, social, and information means and conventional, irregular, catastrophic, terrorist, and criminal methods of warfare. However, it cannot be said that there is consensus on how hybrid threats should be defined. For this reason, Gökce's (2017) study focuses on creating the framework for the conception of hybrid threats, which are gradually gaining importance in international conflicts. Definitions within the EU and NATO also differ (Zandee, van der Meer & Stoetman, 2021). The article by Pawlak (2017) outlines new areas of practical cooperation between the EU and NATO, especially in relation to hybrid threats, building resilience in cybersecurity, and strategic communication. Bajarūnas and Keršanskas (2018) examine the theoretical debates concerning the definition of hybrid threats by singling out their main elements and, on their basis, comparing the definitions used by the European Union and NATO.

A study by the EU Joint Research Centre and the European Centre of Excellence for Countering Hybrid Threats identified 13 different areas of possible hybrid threats: infrastructure, cyberspace, space, the economy, military/defense, culture, social/society, public administration, the legal area, intelligence services, diplomacy, politics, and the information field. In our view, this is the most comprehensive overview of hybrid threats. Hybrid threats can also be directed at public administration. Hybrid threats will continue to evolve based on the success of their application, ongoing technological development, changes in the vulnerabilities of potential antagonists, and the evolution of countermeasures.

Hybrid threat actors are state and non-state entities that conduct activities related to hybrid threats. State hybrid threat actors are states or their representatives that carry out these activities within the framework of their state policy. Non-state hybrid threat actors are entities that are not states but that conduct hybrid threat activities. Non-state hybrid threat actors include, for example, extremist groups, such as terrorist organizations, which may conduct hybrid threat activities to undermine trust in the state or society, or hacker groups, which carry out cyberattacks that are also part of hybrid threats. Propaganda groups can also be hybrid threat actors, as they can spread disinformation, which is an element of hybrid threats.

The international system has great difficulty dealing with illegitimate non-state actors, such as transnational terrorist groups and organized crime syndicates. The analyst Pollard (2002) proposes tools that should be incorporated into the structure of international law and treaties to maintain credibility regarding illegal non-state actors and to hold sponsors of illegality accountable.

Hybrid threat tools are the means that hybrid threat actors use to achieve their aims. The use of hybrid threat tools can serve to achieve specific aims even without a formal declaration of war.

Typical hybrid threat tools are disinformation campaigns. Their aim is to spread false or misleading information that can undermine the credibility of the targeted government or company. Disinformation campaigns can employ various channels, such as social media, traditional media, or personal contacts.

Cyberattacks are another typical hybrid threat tool, as they can target critical infrastructure such as power plants, financial systems, or communication networks.

At present, economic pressure is one of the most commonly used tools for hybrid threats. The aim of economic sanctions is to cripple the economy of the targeted state. Economic sanctions can lead to an economic crisis, which may, in turn, cause unrest and instability. Economic pressures can be used to force a target country or organization to alter its policies to suit the interests of the hybrid threat actors. The manipulation of markets can lead to a fall in stock prices or a decline in the value of a currency because it can cause uncertainty and panic.

Another important tool is the weakening of legal institutions, i.e., reducing their ability to conduct their duties according to the law. Hybrid threats can disrupt the functioning of courts, the police, or other law enforcement agencies, which can lead to the failure of information systems, the release of sensitive information, or the impossibility of the administration of justice.

Corrupt practices can also be used as a tool for hybrid threats. Bribery and corruption can serve to gain influence over politicians, businessmen, or other public actors, to spread the influence of such actors, and can lead to the misuse of public funds, the reduction of competitiveness, and an overall weakening of the economy.

The Internet of Things (IoT) (Maryska et al., 2018) can potentially transform many aspects of our lives, including how we live, work, and communicate. IoT devices could be used in hybrid threats.

Another tool is diplomacy, which puts pressure on the target government. This also includes propaganda, i.e., spreading information intended to influence public opinion, including the propaganda of violence, which spreads information to incite violence.

We can also include terrorism, which can be characterized as a violent act intended to cause fear or chaos, among hybrid threat tools. Treverton (2023) presents a summary of hybrid threat tools: propaganda, fake news, strategic information leaks (e.g., via e-mails), support for political parties, organized protests, cyber tools, espionage, attacks on critical infrastructure, disinformation, economic leverage, and paramilitary operations.

Hybrid threat activities are sets of coordinated activities that both state and non-state actors use to achieve concrete goals without a formal declaration of war and that run below the threshold of a customary response. The basic characteristic of a hybrid attack is that it is designed to exploit a country's weaknesses.

Hybrid-type activities are especially complex and aim to threaten, intimidate, destabilize, and destroy a target or disrupt services with the aim of keeping the adversary in a state of political, economic, military, and social imbalance while keeping the initiative on the side of the attacker to decide on the development of events (Drent, Hendriks & Zandee, 2015), without the target even realizing that it is being attacked and without the possibility of easily identifying the source and the real target of the attack and the means of taking countermeasures. This intimidation, often through violence, "has the aim of creating chaos, national instability, and a general sense of insecurity among ordinary citizens. The state of insecurity over time becomes unbearable, and the 'accusing finger' of public resentment points at governing bodies that fail to provide the necessary protection" (Bojor, 2012).

We adopt the resilience definition that encompasses a system's ability to resist disruption, maintain operations during disruption, and recover to full operational capacity after disruption (Bhamra et al., 2011; Amer et al., 2023; Yarveisy et al., 2020; Pawar et al., 2022). An organization's ability to cope with environmental uncertainties, hybrid threats, crises, and unexpected events depends on its resilience (Ince et al., 2017). Strong institutions are more capable of responding to hybrid threats.

Good public policies (Idsø et al., 2018; Hasanov, Mammadov & Al-Musehel, 2018) can play an important role in preventing hybrid threats.

Public administration is purposively understood in the broadest possible sense as "the process of transforming public policies into results" (Kettl, 2018). The dichotomy between politics and administration is emphasized as a fundamental attribute of European societies (Wallace, Pollack & Young, 2015). Giannopoulos, Smith, and Theocharidou (2021) state that the role of public administration is the implementation of laws and regulations.

Ensuring resilience with an emphasis on eliminating the effect of hybrid threats is an important role for public administration (Koraus et al., 2021; Koraus et al., 2023a; Koraus et al., 2023b; Korauš et al., 2023c). Public and state authorities remain informed about hybrid threats, and that they know how to identify them and respond to them. The added value of the work of Koraus et al. (2023d) is identifying factors important for the resistance of public administration to hybrid threats, including the importance of these factors in the Slovak Republic.

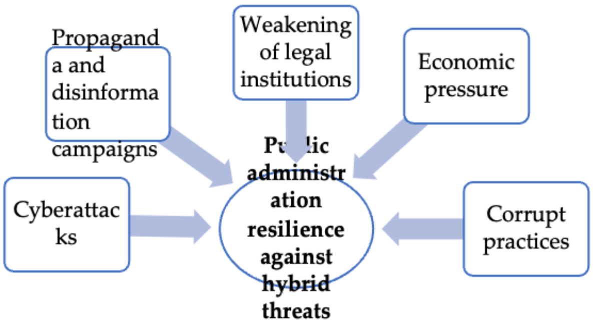
Propaganda and disinformation campaigns
Weakening of legal institutions
Economic pressure
Cyberattacks
Public administration resilience against hybrid threats
Corrupt practices

Fig. 1. Factors (hybrid threats tools) affecting public administration resilience against hybrid threats

Material and methods

Individual indicators characterize one measurable or observable aspect of the investigated phenomenon (Gao et al., 2023). A large set of individual indicators could serve as a comprehensive profile of the phenomenon under consideration (Wang, 2023). Compared with a set of individual indicators, a composite index not only characterizes multidimensional sustainability but also simplifies regional and secular comparisons, integration into decision-making, and public communication (Gao et al., 2023). Building a composite index consists of several steps. The first is the selection of indicators characterizing the investigated phenomenon. The second is to assign weights, which is usually a methodologically problematic and highly controversial process. The last step is to aggregate the indicators (Gao et al., 2023).

According to Mecatti, Crippa, and Farina (2012), a number of subtopics in which the macrotheme may be split should be first identified to represent the measurable dimensions of the latent dimension under study. Then, a pool of descriptive observable variables, interpreting these dimensions and suitably measuring them within every sub-topic, should be identified to quantify each component of the macrotheme.

Composite indicators are increasingly recognized as useful policy-making and public communication tools for conveying information about a country's performance in various areas, such as the environment, economy, society, or technological development (Nardo et al. 2005).

Building resilience is paramount when it comes to countering hybrid threats. A good understanding of the underlying causes of exploitable vulnerabilities is required (Hybrid CoE, 2020).

Identification of relevant aspects

The identification of relevant resilience indicators for a given risk is the first critical step in measuring resilience (Amer et al., 2023). Public administration is responsible for providing basic services to citizens and businesses, such as protection, education, healthcare, and infrastructure. The construction of the KAPA index is based on the thesis that if a state is resistant to various hybrid threats, its public administration will likely be able to continue providing services to citizens and businesses. The novel composite indicator KAPA has five dimensions corresponding to different aspects of public administration resilience against hybrid threats.

The composite index provides relatively concentrated information derived from a certain number of partial indicators. The aim of our contribution is to construct a novel composite index - the Public Administration Resilience Against Hybrid Threats Index (KAPA).

The proposed index has five dimensions – cybersecurity, resistance to disinformation, compliance with laws and security, protection against corruption, and prevention of a sovereign debt crisis. In the following sections, we will clarify the reasons for selecting these individual dimensions as well as indexes of renowned institutions, with the help of which we will quantify them and then compile a new index from the quantified dimensions.

Cybersecurity

The first conflicts of the 21st century showed that information technologies and cyberspace could be used with malicious intent for designing and executing influential operations targeting mass audiences and specific communities (Mazzucchi, 2022). The battle against cyber information threats is more difficult to achieve because the virtual space is free from any real control, and any violent intervention by the authorities may be interpreted as an attempt to limit the right to expression and access to information.

We will assess cybersecurity using the National Cybersecurity Index (NCSI). The NCSI is a global index that measures countries' preparedness for preventing cyber threats and handling cyber incidents. The NCSI can help countries identify their cybersecurity strengths and weaknesses and can also help countries monitor their progress in improving their cybersecurity over time. The NCSI helps countries identify areas in which they need to improve their cyber cooperation with other countries and assists countries in raising cybersecurity awareness among citizens and businesses.

Ensuring cybersecurity is a critical task for all countries in the framework of the resilience of public administration to hybrid threats. Public administration is vulnerable to cyber threats, which can affect its ability to provide services to citizens and businesses. Therefore, we included cybersecurity as one of the pillars of public administration's resilience to hybrid threats. The higher the cyber security of a specific country, the more resistant the public administration is to cyberattacks.

Disinformation

Duberry (2022) states that disinformation on Facebook is deliberate and often strategic in that it is aimed at specific demographic groups and embeds false stories and coordinated efforts from real and fake accounts with the aim of engaging the public (Bennett & Livingston, 2018).

Disinformation campaigns are part of a large strategy to cast doubts on common understandings of the advantages, relevance, and resilience of European liberal democracies, thereby contributing to a global geopolitical power game (Duberry, 2022).

The Media Literacy Index (MLI) is a tool used to measure an individual's. This is an important skill in today's world, where we are exposed to a huge amount of ability to understand and critically evaluate media information from various sources. The Media Literacy Index measures media literacy based on 10 criteria, including an individual's ability to recognize different types of media and their purposes, to understand how the media operates and what its assumptions are, to critically evaluate information from the media, to identify bias and errors in the media, to create one's own opinion based on information from the media, to understand how the media affects society, to understand how we can engage with the media, and to understand how we can protect ourselves from the harmful effects of the media.

Disinformation is a tactic to undermine trust in democratic institutions. Disinformation campaigns and propaganda are activities aimed at influencing, destabilizing, and disrupting the carrying out of public administration. We included the ability of individuals to understand and critically assess information from the media, i.e., be resilient to misinformation, in the composite index KAPA.

Compliance with Laws and Security

Security is one of the defining aspects of any society governed by the rule of law and is a basic function of the state. It is also a prerequisite for realizing the rights and freedoms that the rule of law seeks to promote.

Public administration represents one of the crucial components by which a state and its power are exercised. In it, public authorities decide on the rights, legally protected interests, and obligations of natural persons and legal entities. Legal and administrative regulations determine behavior both in and outside government. How regulations are implemented and enforced is important.

The rule of law is defined as the observance of laws, the independence of the courts, and the presence of transparent and effective institutions. The rule of law is an important aspect of governance, as it ensures that people are dealt with fairly and equally in accordance with the law.

The rule of law is important for public administration for several reasons - it ensures that the public administration operates in harmony with the law; protects the rights of citizens, who have the right to a fair trial and equality before the law; and creates a stable and predictable environment for business, which need to know that their rights will be protected to invest and grow. The rule of law ensures that public administration is transparent and accountable, that citizens have the right to access information about public administration activities, and that they have the right to demand accountability from public officials.

The rule of law is a complex concept that is difficult to measure precisely. The Worldwide Governance Indicators (WGI) project reports aggregate and individual governance indicators for over 200 countries and territories for six dimensions of governance.

The rule of law has strong institutions. Strong institutions (i.e., strong public administration) are more capable of better responding to hybrid threats. We will measure the Compliance with Laws and Security dimension using the Rule of Law dimension of the WGI index.

Corruption

Corruption in public administration can be defined as the misuse of public administration apparatus with the goal of personal or group favoritism or direct enrichment, whereby the means is the corruption of officials, local politicians, and local representatives of political parties by various persons or interest groups. We can, therefore, speak about corruption in public administration or define this as an action that is not in line with the standards on whose basis and in line with which public authorities and public functions operate, namely due to the prioritizing of individual (private) interest, i.e., interest concerning an individual to achieve personal benefit.

The European Quality of Government Index (EQI) measure of institutional quality available at the regional level in the EU. Institutional quality is defined as a multidimensional concept consisting of high impartiality, quality of public service delivery, and low corruption. The EQI is based on three dimensions – Perceptions and experiences with public sector corruption, Impartiality, and Quality.

The World Bank rescaled the regional data to national data ranging from 0 to 1. The higher the values, the better the quality of public administration is evaluated.

The negative effect of corruption in public administration is the weakening of citizens' trust in the law, the rule of law, and its institutions. This is the creation of parallel, unelected, undemocratic power decision-making structures, which weakens the power of public administration and thus also resilience to hybrid threats.

Avoiding a sovereign debt crisis

General government debt to GDP ratio measures the gross debt of the general government as a percentage of GDP. A sovereign debt crisis can have different consequences. It can lead to a reduction in economic growth and to a rise in unemployment. When governments are forced to reduce public spending, this can also lead to a reduction in spending on social programs and public services and, thus, a drop in living standards. A sovereign debt crisis can lead to rising inflation, as governments may be compelled to print more money to meet their obligations. It can also lead to a decrease in confidence in the economy, which can make it difficult for the government to obtain new loans and investments from private investors. People can become frustrated with economic problems and reduced living standards; thus, a sovereign debt crisis can lead to unrest and social tension. The ability to avert a sovereign debt crisis can be measured using the general government debt ratio to GDP.

Composite Indicator KAPA

The structure of the composite indicator KAPA, according to the methodology of Mecatti, Crippa, and Farina (2012), is in Tab. 1. We quantify individual dimensions with values from world-renowned databases. Data were used from public databases for the year 2021. A description and the source of the indicators is in Tab. 2.

Tab. 1. Macro subject: Public Administration Resilience Against Hybrid Threats

	Sub-topic 1	Sub-topic 2	Sub-topic 3	Sub-topic 4	Sub-topic 5
Dimensions	Resilience against cyberattacks	Resilience to disinformation	Legal resilience	Resilience against corruption	Resilience against sovereign debt crisis
Indicators	National Cybersecurity Index (NCSI)	Media Literacy Index (MLI)	Dimension Rule of Law (in Worldwide Governance Indicators (WGI))	Dimension Perception of corruption in the public sector (in the European Quality of Government Index (EQI)	The ratio of general government debt to GDP

Tab. 2. Source and description of indicators

Indicator	Source	Minimum	Maximum	Direction: better is
NCSI	e-Governance, Estonia	0	100	higher
MLI	European Policies Initiatives	0	100	higher
Dimension Rule of law (WGI)	World Bank, National Resource Governance Institute	-2.5	2.5	higher
Dimension Perception of corruption in the public sector (EQI)	University of Gothenburg*/	0	100	higher
General government debt to GDP	OECD, International Monetary Fund	15	225	lower

**/ World Bank rescaled the regional data to national data with a range from 0 to 1*

We construct the new KAPA index using the fuzzy sets apparatus. Fuzzy sets were introduced by Lotfi A. Zadeh in 1965 as an extension of the classical notion of a set. The central idea of fuzzy set theory is that an object simultaneously belongs to more than one set. The closeness of the object to a set is indicated by membership degrees (Peters, 2009). More mathematically, consider a classical set A of the universe U. A fuzzy set $\mathscr{A}$ is defined by a set of ordered pairs, a binary relation:

$$\mathscr{A} = \{ (x, \mu_{\mathscr{A}}(x)) : x \in A, \mu_{\mathscr{A}}(x) \in \langle 0,1 \rangle \} \quad (1)$$

where $\mu_{\mathscr{A}}$ (x) is a membership function. The value $\mu_{\mathscr{A}}$ (x) specifies the grade or degree to which any element x in A belongs to the fuzzy set $\mathscr{A}$. The membership functions play a pivotal role in fuzzy representation. The trapezoidal membership function (Fig. 2.) is defined by four parameters: a, b, c, and d:

$$\mu_{\text{trapeziodal}}(x;\ a,\ b,\ c,\ d) = \max\ (\min\ ((x - a)/(b - a);\ 1;\ (d - x)/(d - c));\ 0). \tag{2}$$

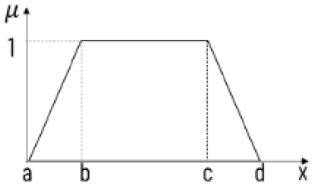

Fig. 2. The trapezoidal membership funYAon

We use two special forms of trapezoidal function based on the openness of the function. They are known as the R-function (Open right) and the L-function (Left open). When higher indicator values are desired, we use L-functions. An L-function has $c = d = +\infty$. Conversely, when lower indicator values are desired, we use R-functions. An R-function has $a = b = -\infty$.

Given a fuzzy set $\mathscr{A}$ on universe U, their α-cuts ($\alpha \in \langle 0,1 \rangle$) are defined as follows:

$$\mathscr{A}_{\alpha} = \{\ (x\text{: } \mu_{\mathscr{A}}\ (x) \geq \alpha\}. \tag{3}$$

α-cut of a fuzzy set $\mathscr{A}$ is a crisp set. This simple but important relationship applies to α-cuts of a fuzzy set $\mathscr{A}$*:* If $\alpha \leq \beta$ then $\mathscr{A}_{\beta} \subseteq \mathscr{A}_{\alpha}$.

A linguistic variable is characterized by a quintuple (X, T(X), U, G, M), where X is the name of the variable, T(X) is the set of terms of X, U is the universe of discourse, G is a syntactic rule for generating the name of the terms, and M is a semantic rule for associating each term with its meaning, that is, a fuzzy set defined on U (Peters, 2009). In our case, X is "resilience against the analyzed factor", T(X) is a set of terms used in the discussion of resilience against the analyzed factor, i.e., {resilient, very resilient, more or less resilient, nonresilient, very nonresilient, more or less nonresilient}. Universe U is the range of indicator values. The syntactic rule G that generates the terms of T (resilience against the analyzed factor) is T^(i+1)={resilient}∪{very T^i }. Semantic rule M associated with the linguistic term resilient with its meaning is

$$\text{M(resilient)} = \{u,\ \mu_{\text{resilient}}\ (u);\ u \in \langle 0,100 \rangle\}$$

where $\mu_{\text{resilient}}(u)$ is a membership function. Linguistic hedges can be used to modify linguistic variables. Assume that the meaning of a linguistic value X is defined by the membership function μ_{X} (u) of U, then linguistic hedges "very" and "more or less" are constructed by mathematical representations (Huynh, Ho and Nakamori**,** 2002) as follows:

$$\begin{aligned}
&\text{Very X = CON(X), where } \mu_{\text{CON(X)}}\ (u) = (\mu_{\text{X}}\ (u))^2\ ;\\
&\text{More or less X = DIL(X), where } \mu_{\text{DIL(X)}}\ (u) = (\mu_{\text{X}}\ (u))^{0.5}\ ;\\
&\text{Not X = NEG(X), where } \mu_{\text{NEG(X)}}\ (u) = 1 - \mu_{\text{X}}\ (u).
\end{aligned}$$

Weighting is the most important step and should be handled with great care. However, existing approaches to applying weights have been subject to severe criticism, as weighting is typically a methodologically problematic and highly controversial process (Gao et al., 2023). A simple case that we use is equal weighting, where all indicators are attached with the same importance.

Aggregation functions combine input values into a single output value, which represents all the inputs. Radko, Kolesárová, and Komorníková (2015) give a list of basic examples as well as some peculiar examples of aggregation functions.

An OWA operator of dimension n is a mapping F : $\text{R}^n \rightarrow \text{R}$, that has an associated vector $\boldsymbol{w} = (w_1, w_2, \ldots, w_{\text{n}}\ )^{\text{T}}$ such as $w_{\text{i}} \in \langle 0,\ 1 \rangle$ and $\sum w_{\text{i}} = 1$. Then $\text{F}(a_1,\ a_2,\ \ldots,\ a_{\text{n}}\ ) = \sum w_{\text{j}}b_{\text{j}}$, where b_{j} is the j-th largest element of the $\{a_1,\ a_2,\ \ldots,\ a_{\text{n}}\}$. We use a special type of OWA aggregation operator - averaging operator $\boldsymbol{w}_{\text{A}} = (1/n,\ 1/n,\ \ldots,\ 1/n)^{\text{T}}$. Then $\text{F}(a_1,\ a_2,\ \ldots,\ a_{\text{n}}\ ) = \sum a_{\text{j}}\ 1/n$. OWA operators appear to be particular cases of Choquet integral with respect to a suitable fuzzy measure (Grabisch, 1997).

The Fragile States Index

Concluding we will compare the ranking of states according to our new KAPA index with the ranking of states according to Fragile States Index (FSI). The FSI is a tool that measures the vulnerability of countries to conflict, violence, and state collapse. It is published by the Fund for Peace, a nonprofit organization that prevents conflict and promotes peace. The FSI is scored on a scale of 0 to 120, with a higher score indicating a higher vulnerability to fragility.

States with lower FSI ratings are usually less resilient to hybrid threats. This is because such states often have weaker institutions, less cooperation between different actors, and a lower level of transparency, making them more vulnerable to being targeted by hybrid threats. A state with a low FSI evaluation may be more susceptible to disinformation campaigns, a typical tool of hybrid threats. This is because such a state often has weaker institutions that are less able to identify and respond to disinformation campaigns. States with a lower FSI evaluation are more often the target of cyberattacks because they often have weaker institutions that have less funding and are less capable of identifying and responding to such attacks.

Results and discussion

We included five indicators in the analysis, the selection of which is based on a literature review; their descriptive statistics are shown in Table 2. The largest variability measured by the coefficient of variation is General government debt to GDP (62.7661). The second largest variability is the Dimension Rule of Law (54.6184). The third largest variability is the MLI (23.1326). Skewness measures the distortion of symmetrical distribution or asymmetry in a data set. Data distribution is for the three indicators nearly symmetrical (skewness between -0.5 and 0.5) – Rule of law, MLI, and Perception of corruption in the public sector (EQI). Others are skewed. All indicators except general government debt to GDP have a negative skew. This means most of the data distribution will be on the right side of the mean, while the lower-ranging values will be on the left side of the curve.

Tab. 3. Descriptive statistics

Indicator	Minimum	Maximum	Mean	Standard deviation	Median	Coefficient of variation	Skewness
NCSI	50.6500	94.8100	81.3856	11.1555	84.4200	13.7070	-1.1698
MLI	29	78	55.1481	12.7572	56	23.1326	-0.1566
Dimension Rule of law (WGI)	-0.0439	2.0579	1.0722	0.5856	1.1099	54.6184	-0.0712
Dimension Perception of corruption in the public sector (EQI)	0.6708	0.9148	0.8138	0.0733	0.8128	9.0033	-0.4469
General government debt to GDP (%)	17.6900	212.4000	70.7648	44.4163	55.3100	62.7661	1.6073

In the first step of KAPA index construction, we fuzzify the values of individual dimensions. In Tab. 4. the linguistic variables associated with the dimensions of the KAPA index are described.

Tab. 4. Linguistic variables

Dimension	Linguistic variable X	Universe U	Membership function $m_{\text{resilient }(u)}$
Resilience against cyberattacks	Resilience against cyberattacks	⟨0, 100⟩	max (min (u/100; 1); 0)
Resilience to disinformation	Resilience to disinformation	⟨0, 100⟩	max (min (u/100; 1); 0)
Legal resilience	Resiliency in complying with the law and ensuring safety	⟨-2.5, 2.5⟩	max (min ((u + 2.5)/5; 1); 0)
Resilience against corruption	Resilience against corruption	⟨0, 1⟩	max (min (u; 1); 0)
Resilience against sovereign debt crisis	Resilience against sovereign debt crisis	⟨15, 225⟩	max (min ((225 - u)/210; 1); 0)

Countries that belong to the 0.80-cut of the fuzzy set "very resilient" are very resilient against cyberattacks. These are Belgium, Estonia, Lithuania, Czech Republic, Germany, Greece, Portugal, and Romania (Fig. 3). Countries that belong to the 0.80-cut of the fuzzy set "resilient" are resilient against cyberattacks, i.e., the very resilient countries plus Spain, Poland, Austria, Finland, Denmark, France, Sweden, Croatia, the Netherlands, and the Slovak Republic. Countries that belong to the 0.80-cut of the fuzzy set "more or less resilient" are more or less resilient against cyberattacks, i.e., all resilient countries plus Italy, Ireland, Latvia, Bulgaria, Hungary, Cyprus, and Luxembourg. Slovenia and Malta belong to indefinite countries because they do not belong to the 0.80-cut of any fuzzy set.

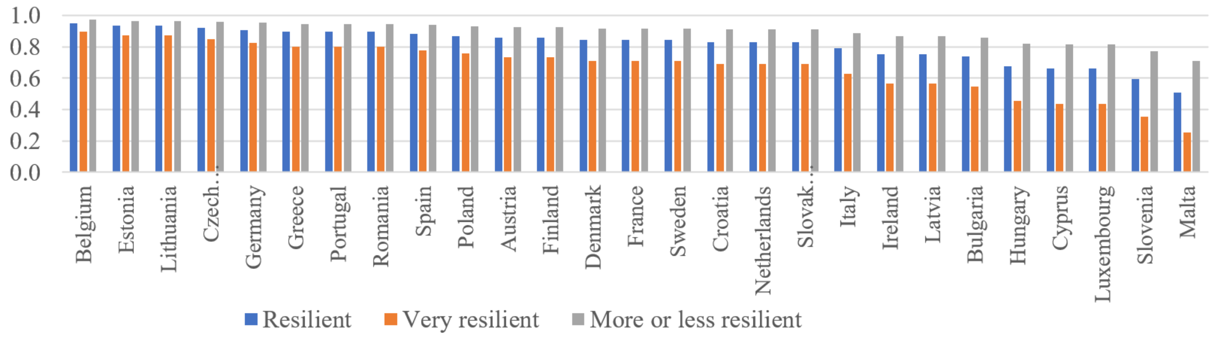

Fig. 3. Resilience against cyberattacks

Finland, Denmark, Estonia, Sweden, Ireland, the Netherlands, and Belgium are more or less resilient to disinformation (Fig. 4). Romania and Bulgaria are more or less nonresilient to disinformation. The remaining states are indefinite countries because they do not belong to the 0.8 cut of any fuzzy set. Resistance to disinformation is the weakest point of vulnerability to hybrid threats.

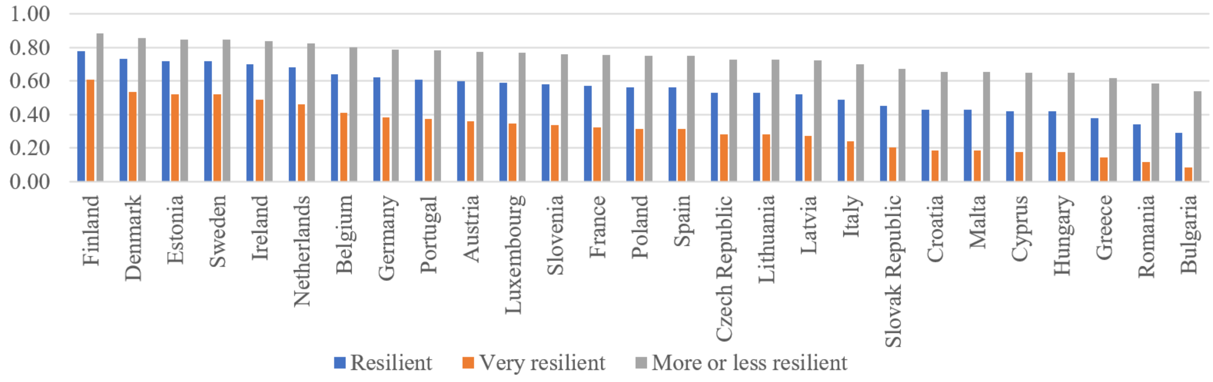

Fig. 4. Resilience to disinformation

Only Finland is very resilient in complying with the law and ensuring safety (Fig. 5). Resilient are Finland, Denmark, Austria, Luxembourg, the Netherlands, Sweden, Germany, and Ireland. More or resilient are the resilient countries plus Estonia, Belgium, France, Portugal, the Czech Republic, Lithuania, Slovenia, Latvia, Spain, Malta, and the Slovak Republic.

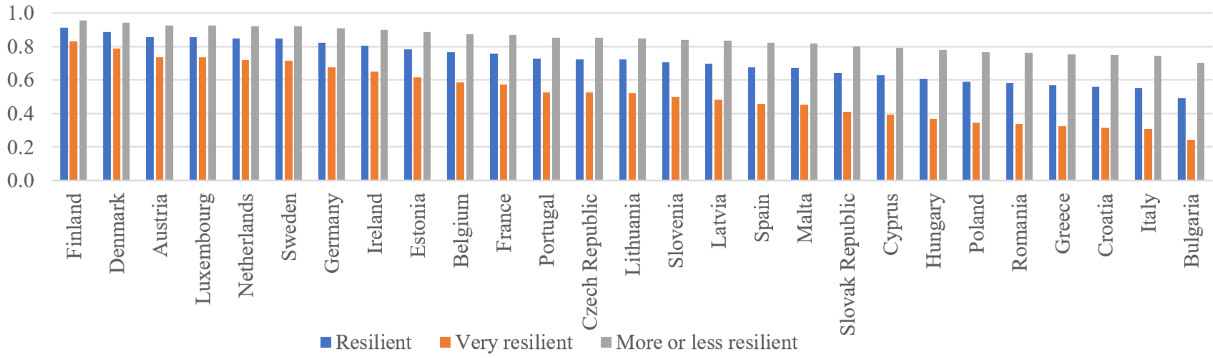

Fig. 5. Resilience in complying with the law and ensuring safety

Four countries are very resilient to corruption – Finland, the Netherlands, Estonia, and Ireland (Fig. 6). Resilient are the very resilient countries and Denmark, Sweden, Germany, Luxembourg, Belgium, Austria, the Czech Republic, Slovenia, France, Spain, Italy, and Malta. All EU countries are more or less resilient.

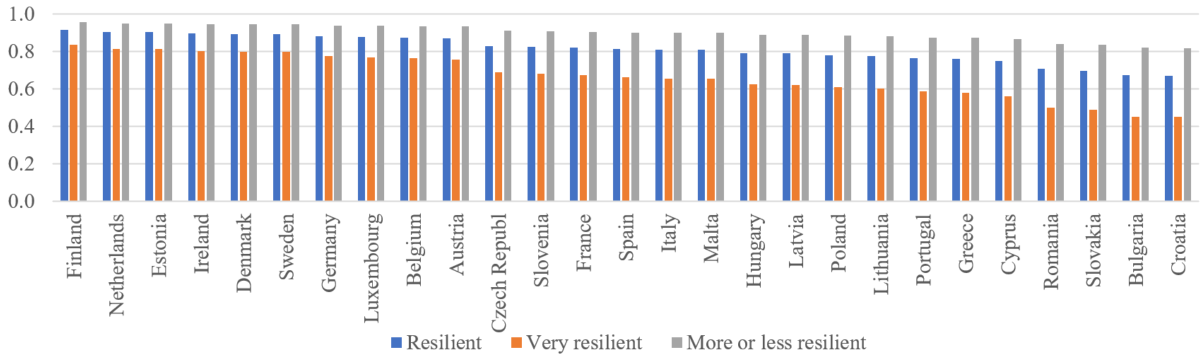

Fig. 6. Resilience against corruption

Estonia, Luxembourg, Denmark, and Bulgaria are very resilient against a sovereign debt crisis (Fig. 7). Resilient countries are the very resilient, plus Sweden, Lithuania, Poland, the Czech Republic, Germany, Latvia, Romania, the Netherlands, Malta, and Finland. Greece is very nonresilient, with a ratio of general government debt to GDP higher than 200 percent. More or less resilient are very resilient countries, resilient countries, and Ireland, Austria, the Slovak Republic, Slovenia, Hungary, and Croatia. Belgium, France, Spain, Portugal, Cyprus, and Italy are indefinite countries because they do not belong to the 0.80 cut of any fuzzy set. All have a very high ratio of general government debt to GDP.

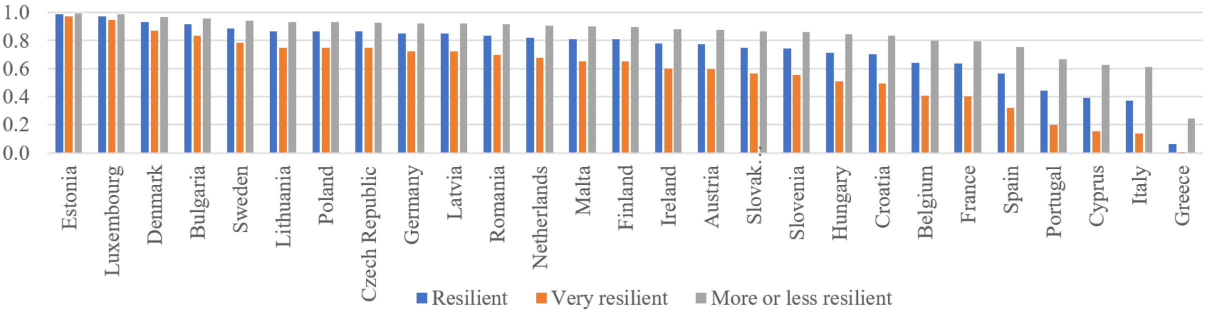

Fig. 7. Resilience against a sovereign debt crisis

In the second step, we aggregate the membership functions. We use a special type of OWA aggregation operator – averaging operator $\boldsymbol{w}_A$. The higher the value of the KAPA index, the higher the resilience of public administration to hybrid threats.

Table Tab. 5 contains the values of the membership functions and the resulting KAPA index. When we notice the asymmetry of the distribution of the values of the membership functions, their median is greater than the mean, and thus, most of the values are greater than the mean.

Tab. 5. Values of the membership functions and the resulting KAPA index

Country	CS	RD	LS	PC	DC	KAPA	Rank
Austria	0.8571	0.6000	0.8576	0.8705	0.7719	0.7914	8
Belgium	0.9481	0.6400	0.7652	0.8736	0.6395	0.7733	11
Bulgaria	0.7403	0.2900	0.4912	0.6721	0.9150	0.6217	24
Croatia	0.8312	0.4300	0.5605	0.6708	0.7012	0.6387	23
Cyprus	0.6623	0.4200	0.6274	0.7482	0.3913	0.5698	26
Czech Republic	0.9221	0.5300	0.7252	0.8291	0.8640	0.7741	10
Denmark	0.8442	0.7300	0.8873	0.8937	0.9332	0.8577	2
Estonia	0.9351	0.7200	0.7855	0.9024	0.9872	0.8660	1
Finland	0.8571	0.7800	0.9116	0.9148	0.8080	0.8543	3
France	0.8442	0.5700	0.7578	0.8203	0.6345	0.7254	14
Germany	0.9091	0.6200	0.8217	0.8814	0.8511	0.8167	6
Greece	0.8961	0.3800	0.5700	0.7612	0.0600	0.5334	27
Hungary	0.6753	0.4200	0.6062	0.7913	0.7133	0.6412	22
Ireland	0.7532	0.7000	0.8060	0.8956	0.7768	0.7863	9
Italy	0.7922	0.4900	0.5539	0.8102	0.3736	0.6040	25
Latvia	0.7532	0.5200	0.6963	0.7891	0.8503	0.7218	15
Lithuania	0.9351	0.5300	0.7220	0.7763	0.8648	0.7656	12
Luxembourg	0.6623	0.5900	0.8574	0.8770	0.9744	0.7922	7
Malta	0.5065	0.4300	0.6729	0.8086	0.8088	0.6454	21
Netherlands	0.8312	0.6800	0.8479	0.9026	0.8219	0.8167	5
Poland	0.8701	0.5600	0.5889	0.7808	0.8648	0.7329	13

Portugal	0.8961	0.6100	0.7267	0.7651	0.4432	0.6882	18
Romania	0.8961	0.3400	0.5815	0.7075	0.8366	0.6723	20
Slovak Republic	0.8312	0.4500	0.6411	0.6978	0.7506	0.6742	19
Slovenia	0.5974	0.5800	0.7060	0.8261	0.7442	0.6907	17
Spain	0.8831	0.5600	0.6752	0.8128	0.5656	0.6993	16
Sweden	0.8442	0.7200	0.8468	0.8936	0.8842	0.8378	4

Comment: CS -Resilience against cyberattacks, RD-Resilience to disinformation, LS-Resiliency in complying with the law and ensuring safety, PC-Resilience against corruption, DC-Resilience against the sovereign debt crisis

The countries with the lowest KAPA values (Fig. 8) have problems, especially with Resilience to disinformation (RD) and Resilience against a sovereign debt crisis (DC).

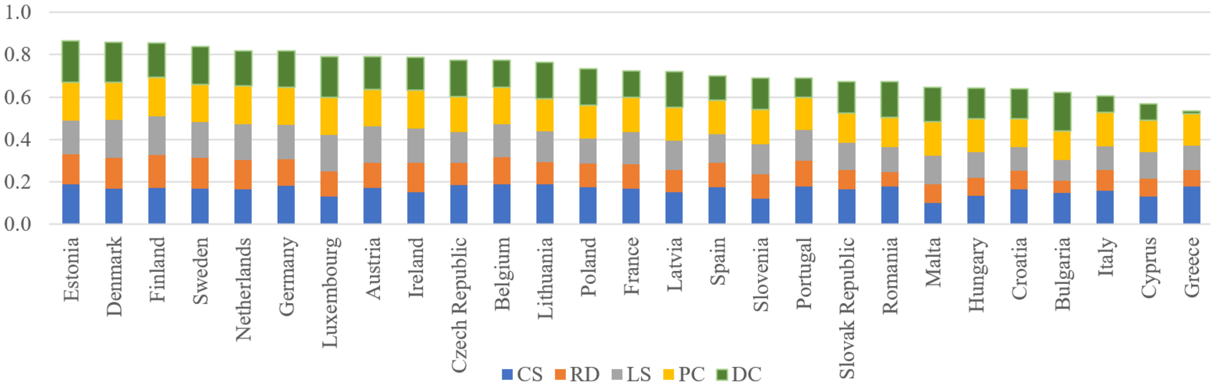

Fig. 8. Structure of the index KAPA

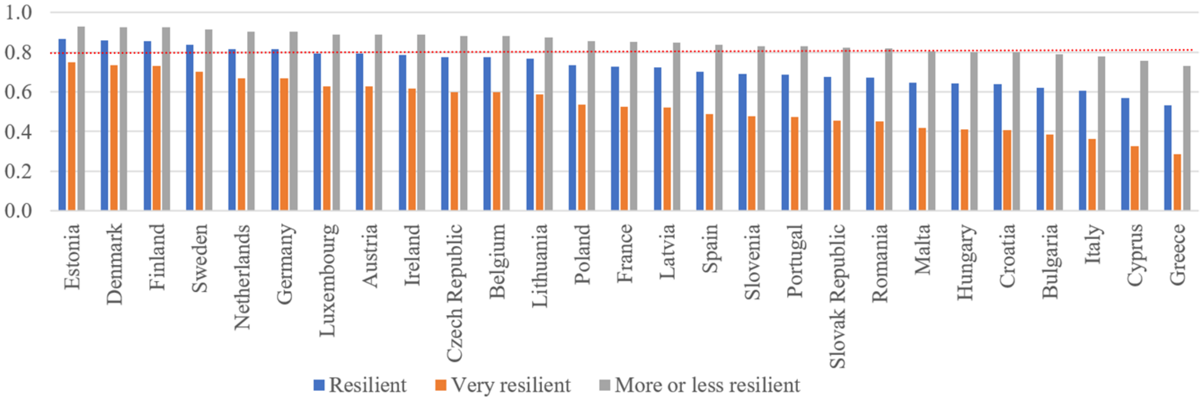

Fig. 9. Resilience of public administration against hybrid threats

No EU country has a very resilient public administration against hybrid threats (Fig. 9). Only six countries are resilient: Estonia, Denmark, Finland, Sweden, the Netherlands, and Germany. These are countries that are intensively focused on solving problems related to hybrid threats in universities or institutions. Except for Estonia, these are countries with a high GDP per capita value. France placed 14th in the ranking. At the bottom of the ranking are the countries of the former socialist bloc, except for the Czech Republic, which took an excellent 10th place. More or less resilient public administration against hybrid threats has the countries that are resilient as well as 16 others. There are also countries that are indefinite in terms of resilience in public administration against hybrid threats – Croatia, Bulgaria, Italy, Cyprus, and Greece. All the listed states have membership function values among the worst-ranked states in at least three value dimensions.

All dimensions of the KAPA index show statistically significant dependence (Fig. 11) on the value of the KAPA index, except for the cyber threat dimension measured by the NCSI. The choice of NCSI over other indices measuring resilience to cyber threats is based on the index's methodology. The results would not significantly change even if the widely used Global Cybersecurity Index (GCI) were used. The GCI measures countries' commitment to cybersecurity at a global level – to raise awareness of the importance and different dimensions of the problem. Resilience against cyber-attacks is not statistically dependent, with no dimension of the KAPA index. The statistical methods did not confirm our assumption that the higher the cybersecurity of a particular country, the more resistant its public administration is to cyberattacks. Nevertheless, we argue that resilience against cyber threats is important to resilience against hybrid threats. The virtual space is free from any real control, and any violent intervention by authorities may be interpreted as an attempt to limit the right to expression and access to information. Creating an effective cybersecurity management system that will ensure implementation and compliance with legislation is necessary.

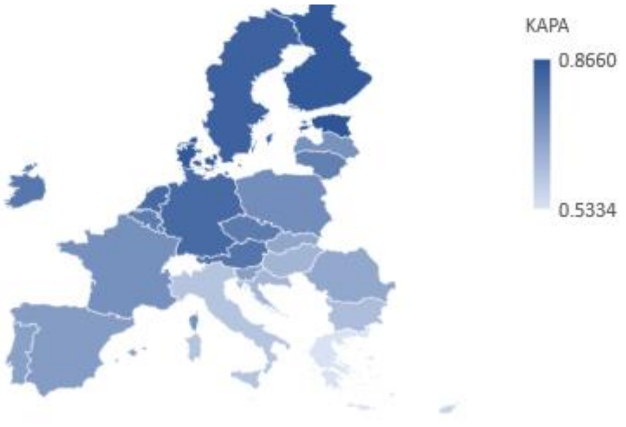

Fig. 10. Values of the KAPA index in EU countries

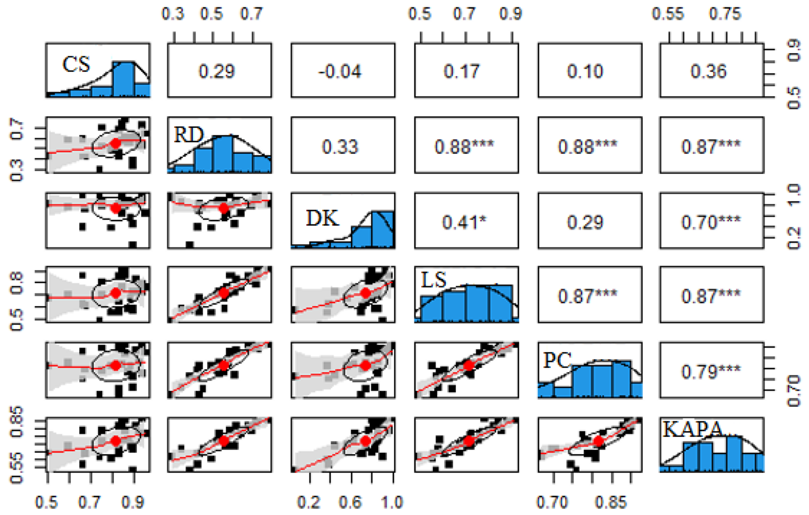

Fig. 11. Dependencies of the dimension with the KAPA index

Now, let us measure the dependence between the new KAPA index and the FSI index. The Pearson correlation coefficient between the FSI and the new public administration resilience to hybrid threats index KAPA is -0.7894 (p-value is 6.023e-07). This means an indirect linear relationship exists between the KAPA and FSI indices. This dependence is described even better by Spearman's correlation coefficient of -0.8052503 (p-value is 2.114e-06), which is a measure of monotonic dependence. Both coefficients are high and significant.

Dependence exists between the Fragile States Index (FSI) and the resilience of public administrations to hybrid threats KAPA. Weak states (as assessed using the FSI) have weak state institutions that are less capable of facing the complex challenges of hybrid threats. They often have higher levels of corruption and crime, creating an environment where hybrid threats can spread more easily. They often have high levels of social tension and instability, which can create opportunities for hybrid threats to spread disinformation as well as incite unrest.

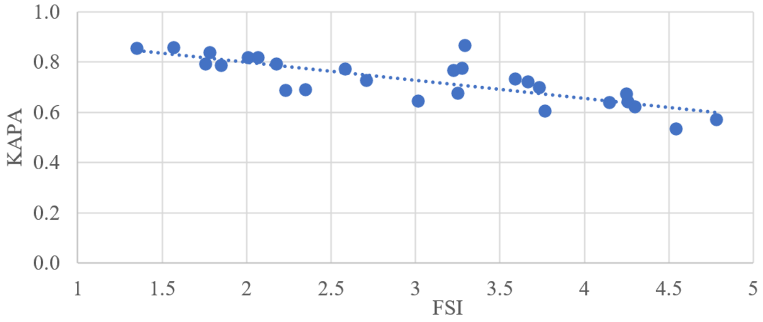

Fig. 12. Dependence between the new KAPA index and the FSI index.

Conclusions

Quality public administration and country management are key factors in its economic performance. There are several instruments by which the public administration supports the raw materials policy of the European Union. These are legislative instruments when the public administration implements and complies with European laws and regulations related to raw materials policy. The public administration uses economic instruments such as taxes, fees, subsidies, and other financial incentives to support the efficient and sustainable use of raw materials in accordance with EU policy. The public administration supports research and development in the field of raw materials policy, for example, in the field of new technologies for extraction and processing of raw materials or in the field of recycling and secondary use of raw materials. Public administration can support the business environment so that fundamental technological breakthroughs in the field of reducing raw material dependence are translated into real products with real commercial potential. Another tool is the support of education and awareness in the field of the EU's raw materials policy to increase public awareness of the importance of the efficient and sustainable use of raw materials. We can also include the implementation and use of European programs and funds that are intended to support raw materials policy.

Hybrid threats can affect public administration and thus threaten its support for resource policy in several ways. Hybrid threats can exploit weaknesses in public administration, such as weaknesses in management and control systems, corruption, or lack of transparency. Hybrid threat actors can use disinformation and propaganda to influence public opinion and decision-making in public administration. This can lead to wrong decisions in the area of raw materials policy or resistance to the necessary measures. Hybrid threat actors can use cyber-attacks to disrupt public administration information systems, which can impact the ability of public administration to manage and support resource policy effectively. Hybrid threat actors can abuse legal rules and processes to achieve their goals, for example, through legal disputes or manipulation of regulatory processes. They can also influence electoral processes in order to achieve results that are beneficial to them. This can have a negative impact on political decision-making in the area of raw materials policy. Hybrid threats require a comprehensive response that includes improving security measures, strengthening transparency and accountability, fighting corruption, improving cyber security, and strengthening corporate resilience.

The aim of the paper was to create a new composite KAPA index, which measures the resistance of public administration to hybrid threats. No EU country has a very resilient public administration against hybrid threats. Only six countries are resilient: Estonia, Denmark, Finland, Sweden, the Netherlands, and Germany. The worst-ranked countries were Greece, Cyprus, Italy, Bulgaria, and Croatia. Although resilient countries are also dependent on oil and gas imports, they also have significant coal and renewable energy resources, which makes them vulnerable to price fluctuations and political instability in these regions and provides them with a higher degree of security. According to KAPA, the differences between the countries at the beginning and at the end of the ranking are also dependent on rare earths.

The supply of raw materials has become a real geopolitical tool. The Critical Raw Materials Act (CRMA) from 2022 should provide a shared understanding of which critical raw materials can be considered as particularly strategic. Targeted amendments and harmonization to existing legislation, notably on waste, would promote quality recycling of strategic raw materials and an efficient market for secondary raw materials, which is in line with our circular economy objectives. By fulfilling the CRMA, the public administration has the opportunity to contribute to securing the future of European industry. CRMA can help European businesses withstand price fluctuations and political uncertainties and ensure they have access to the critical raw materials they need for their production.

The FSI is used to measure the vulnerability of states to internal and external challenges that may threaten their stability and reduce their ability to follow the law and provide basic services to their citizens. Our study also confirmed that there is a clear link between the Fragile States Index (FSI) and the resilience of public administrations to hybrid threats measured by the KAPA index. Powerful states have a public administration that is resistant to hybrid threats.

References

Amer, L., Celik, N. and Andiroglu, E. (2023). Operationalizing resilience: A deductive faultdriven resilience index for enabling adaptation. *Process Safety and Environmental Protection,* 177, 1085-1102. doi:10.1016/j.psep.2023.07.082

Bajarūnas, E. and Vytautas, K. (2018). Hybrid threats: analysis of content, challenges posed and measures to overcome. *Lithuanian annual strategic review,* 16, 123–170. doi: 10.2478/lasr-2018-0006

Bennett, W. L. and Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. *European journal of communication,* 33(2), 122-139.

Bhamra, R., Samir, D. and Burnard, K. (2011). Resilience: the concept, a literature review and future directions. *International journal of production research* 49(18): 5375-5393. doi: 10.1080/ 00207543.2011.563826

Bojor, L. (2012). The Hybrid type of conflict – future challenge for military frameworkof actions. The 18th International Scientific Conference "The Knowledge Based Organization", Sibiu, 24.

Drent, M., Hendriks, R. J. and Zandee, D. (2015). *New threats, new EU and NATO Responses.* The Hague, Netherlands: Clingendael Institute. Available online: https://www.clingendael.org/sites/default/files/pdfs/New%20Threats_New%20EU_Nato%20Responses_Clingendael_July2015.pdf (accessed on 11 June 2023).

Duberry, J. (2022). AI and the Weaponization of Information: Hybrid Threats Against Trust between Citizens and Democratic Institutions. In *Artificial Intelligence and Democracy*, 158–194. Edward Elgar Publishing

e-Governance Academy. *National Cyber Security index NCSI*. Available online: https://ncsi.ega.ee/methodology/ (accessed on 10 May 2023).

Fund for Peace. (2021). *Fragile States Index*. Available online: https://fragilestatesindex.org/wp-content/uploads/2021/05/fsi-2021.xlsx (accessed on 10 May 2023).

Gao, P., Wang, Y., Wang, H., Song, Ch., Wang and Y.S. (2023). A Pareto front-based approach for constructing composite index of sustainability without weights: A comparative study of implementations. *Ecological Indicators*, 155,110919. doi:10.1016/j.ecolind.2023.110919

Giannopoulos, G., Smith, H. and Theocharidou, M. (2021). *The Landscape of Hybrid Threats: A Conceptual model.* Public version. European Centre for Excellence for Countering Hybrid Threats. Publications Office of the European Union, Luxembourg, doi:10.2760/44985

Glenn, R. W. (2009). Thoughts on hybrid conflict. *Small Wars Journal* 2(1), 1-8.

Gökce, O. (2017). Definition and scope of hybrid threats. *Inquiry-Sarajevo Journal of Social Science* 3(1), 19–30.

Grabisch, M. (1997). Alternative Representations of OWA Operators. pp. 73-85 In: Yager, R. R., Kacprzyk, J. (eds.) *The Ordered Weighted Averaging Operators*. Springer, Boston, MA. doi:10.1007/978-1-4615-6123-1_7

Hasanov, F., Fuad, M. and Al-Musehel, N. (2018). The effects of fiscal policy on non-oil economic growth. *Economies* 6(2), 27.

Huynh, V. N., Ho, T.B. and Nakamori, Y. (2002). A parametric representation of linguistic hedges in Zadeh's fuzzy logic. *International Journal of Approximate Reasoning* 30(3), 203-223.

Hybrid CoE. (2020). *Vulnerability and resilience of COI*. https://www.hybridcoe.fi/coi-vulnerabilities-and-resilience/

Charron, N., Lapuente, V., Bauhr, M. and Annoni, P. (2022). Change and Continuity in Quality of Government: Trends in subnational quality of government in EU member states. *Investigaciones Regionales-Journal of Regional Research*, 53, 5-23. doi:10.38191/iirr-jorr.22.008

Idsø, J., Torbjørn, Å. and Bhatta, B.P. (2018). The income equalization system among municipalities in Norway: Strengths and implications. *Economies* 6(2), 34.

Ince, H., Imamoglu, S. Z., Karakose, M. A. and Turkcan, H. (2017). The Search For Understanding Organizational Resilience. In Özşahin, M. (Ed.), Strategic Management of Corporate Sustainability, Social Responsibility and Innovativeness. *European Proceedings of Social and Behavioural Sciences*, 34, 230-243. Future Academy. doi:10.15405/epsbs.2017.12.02.20

Kacprzyk, J. and Pedrycz, W. (eds). (2015). *Springer handbook of computational intelligence*. Springer. doi:10.1007/978-3-662-43505-2

Kettl, D. F. (2018). *Politics of the Administrative Process*. 7th ed. Los Angeles: CQ Press.

Koraus, A., Lukac, J., Mihalcova, B. and Kurilovska, L. (2023a). HDI index dimensions in the context of hybrid threats. *Entrepreneurship and Sustainability Issues*, 11(2), 452-465. doi: 10.9770/jesi.2023.11.2(30)

Koraus, A., Krasna, P., Sisulak, S. and Veselovska, S. (2023b). Integrated security strategies in the context of hybrid threats in the Slovak Republic. *Entrepreneurship and Sustainability Issues*, 11(1), 233-250. doi: 10.9770/jesi.2023.11.1(14)

Koraus, A., Kurilovska, L., Sisulak, S. and Krasna, P. (2021d) Cyberbullying as a modern phenomenon of the present time and its impact on youth. In: RELIK. Langhamrova, J., Vrabcova, J. (eds). Praha : Prague University of Economics and Business, 353-362. ISBN 978-80-245-2429-0.

Koraus, A., Palinchak, M., Gombar, M. and Stehlikova, B. (2023d). The resilience of public administration to hybrid threats in the context of sustainable competitiveness of a country. Sent to *Journal of Competitiveness.*

Maryska, M., Doucek, P., Nedomova, L. and Sladek, P. (2018). The energy industry in the Czech Republic: On the way to the Internet of Things. *Economies* 6(2), 36. doi:10.3390/economies6020036

Mazzucchi, N. (2022). *AI-based technologies in hybrid conflict: The future of influence operations.* Hybrid CoE Paper 14. Available online: https://www.hybridcoe.fi/wp-content/uploads/2022/06/20220623-Hybrid-CoE-Paper-14-AI-based-technologies-WEB.pdf

Mecatti, F., Franca, C. and Farina, P. (2012). A special gen(d)re of statistics: Roots, development and methodological prospects of gender statistics. *International Statistical Review* 80(3), 452-467. doi:10.1111/j.1751-5823.2012.00186.x

Mihalcova, B., Koraus, A., Sisulak, S., Gallo, P. and Lukac, J. (2023). The risks of misusing social networks in the context of hybrid threat. *Entrepreneurship and Sustainability Issues*, 10(4), 357-371. http://doi.org/10.9770/jesi.2023.10.4(22)

Nardo, M., Saisana, M., Saltelli, A. and Tarantol, S. (2005). *Tools for composite indicators building*. European Comission, Ispra 15(1), 19-20.

Novak, V. (1990). *Fuzzy množiny a jejich aplikace*. Praha: SNTL.

Pawar, B., Huffman, M., Khan, F. and Wang, Q. (2022). Resilience assessment framework for fast response process systems. *Process Safety and Environmental Protection*, 163, 82-93. doi:10.1016/j.psep.2022.05.016

Pawlak, P. (2017). *Countering hybrid threats: EU-NATO cooperation*. Available online: https://policycommons.net/artifacts/1338529/countering-hybrid-threats/1947195/

Peters, G. (2009). Granular Computing. *Encyclopedia of Artificial Intelligence*. IGI Global, 74-780.

Pollard, N. A. (2002). Globalization's Bastards: Illegitimate Non-State Actors in International Law. *Low Intensity Conflict & Law Enforcement* 11, 210-238 doi:10.1080/0966284042000279009

OSIS: *Media Literacy Index*. (2021). Available online: https://osis.bg/?p=3750&lang=en

Mesiar, R., Kolesarová, A., Komornikova, M. (2015). Aggregation Functions on [0,1]. In: Kacprzyk, J., Pedrycz, W. (eds) *Springer Handbook of Computational Intelligence*. Springer Handbooks. Springer, Berlin, Heidelberg. doi:10.1007/978-3-662-43505-2_4

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/.

Revelle, W. (2022). *psych: Procedures for Personality and Psychological Research*, Northwestern University, Evanston, Illinois, USA, https://CRAN.R-project.org/package=psych Version = 2.2.5.

Treverton, G. F. (2021). *An American view: Hybrid threats and intelligence. Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. By Mikael Weissmann, Niklas Nilsson, Björn Palmertz and Per Thunholm. London: I.B. Tauris, 36–45. Bloomsbury Collections.

University of Gothenburg. (2018). *European Quality of Government Index*. Available online: https://nicholascharron.files.wordpress.com/2018/08/eqi-data-qog-webpage.xlsx

Wallace, H., Pollack, M.A. and Youn, A.R. (2015). *Policy-Making in the European Union*. 7th ed. Oxford: Oxford University Press.

Wang, Y., Song, C., Cheng, C., Wang, H., Wang, X. and Gao, P. (2022). Modelling and evaluating the economy-resource-ecological environment system of a third-polar city using system dynamics and ranked weights-based coupling coordination degree model. *Cities* 133,104151. doi:10.1016/j.cities.2022.104151

World Bank: *WGI*. Available online: https://www.govindicators.org/

Yarveisy, R., Gao, C. and Khan, F. (2020). A simple yet robust resilience as-sessment metrics. *Reliability Engineering & System Safety.* 197, 106810. doi:10.1016/j.ress.2020.106810

Zandee, D., van der Meer, S. and Stoetman, A. (2021). *Countering hybrid threats: Steps for improving EU-NATO cooperation.* Clingendael Institute, 2021. Available online: https://www.clingendael.org/sites/default/files/2021-10/countering-hybrid-threats.pdf