

## Article

# Novel Index for Public Administration Resilience Against Hybrid Threats

Antonin Koraus <sup>1\*</sup>, Mykola Palinchak<sup>2</sup>, Beata Stehlikova<sup>3</sup>, Miroslav Gombar<sup>4</sup>

<sup>1</sup> Academy of the Police force in Bratislava, Sklabinská 1, 835 17 Bratislava, Slovak Republic; [antonin.koraus@akademiapz.sk](mailto:antonin.koraus@akademiapz.sk)

<sup>2</sup> Uzhorod National University, Faculty of International Economic Relations, University Street 14, 880 00 Uzhorod, Ukraine; [mykola.palinchak@uzhnu.edu.ua](mailto:mykola.palinchak@uzhnu.edu.ua)

<sup>3</sup> Institute of Management of the Slovak University of Technology, Vazovova 5, 812 43 Bratislava, Slovak Republic; [beata.stehlikova@stuba.sk](mailto:beata.stehlikova@stuba.sk)

<sup>4</sup> Department of Management, Faculty of Management and Business, University of Prešov, 080 01 Presov, Slovakia; [miroslav.gombar@unipo.sk](mailto:miroslav.gombar@unipo.sk)

\* Correspondence: [antonin.koraus@akademiapz.sk](mailto:antonin.koraus@akademiapz.sk)

## Abstract

Hybrid threats are a serious challenge to security and stability in the world. They are very diverse in terms of actors, activities, or instruments. Composite indices, which are created from several indicators, make it possible to describe the multidimensional nature of phenomena. 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, 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 Fragile States Index FSI) are also more vulnerable to hybrid threats and have less resilient public administration.

**Keywords:** public administration; resilience; hybrid threats; EU; composite index; fuzzy sets

**Citation:** To be added by editorial staff during production.

Academic Editor: Firstname Last-name

Received: date

Revised: date

Accepted: date

Published: date



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

## 1. Introduction

The 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. Another factor affecting Europe's security environment is migration from Africa and the Middle East. 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. Europe is thus facing new security challenges, and 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 state and public institutions and an overall weakening of democratic decision-making and value orientation of society.

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. It cannot be said, however, that there is consensus on how hybrid threats should be defined. For this reason, the study of Gökce (2017) 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 and 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 entities, whether state and non-state, which 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 those entities that are not states but which 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.

V súčasnosti je ekonomický tlak = economic pressure jedným z najčastejšie používaných nástrojov hybridných hrozieb. The aim of economic sanctions is to cripple the economy of the targeted state. Ekonomické sankcie môžu viesť k ekonomickej kríze, ktorá môže spôsobiť nepokoj a nestabilitu. Ekonomické tlaky môžu byť použité na to, aby cieľová

krajina alebo organizácia zmenila svoju politiku tak, aby vyhovovala záujmom aktérov hrozby. Manipulácia s tržmi môže viesť k poklesu cien akcií, k poklesu hodnoty meny, pretože môže spôsobiť neistotu a paniku.

Ďalším významným nástrojom je oslabenie právnych inštitúcií, t.j. zníženie ich schopnosti vykonávať svoje úlohy podľa zákona. Hybridné hrozby môžu narušiť fungovanie súdov, polície alebo iných orgánov činných v trestnom konaní. To môže viesť k výpadku informačných systémov, k úniku citlivých informácií alebo k znemožneniu vykonávania spravodlivosti.

Korupčné praktiky môžu byť použité ako nástroj hybridných hrozieb. Úplatky a korupcia môžu slúžiť na získanie vplyvu na politikov, podnikateľov alebo iných verejných činiteľov, na šírenie vplyvu aktérov, môžu viesť k zneužívaniu verejných zdrojov, k zníženiu konkurencieschopnosti a k celkovému oslabeniu ekonomiky.

IoT (Maryska et al. 2018) has the potential to transform many aspects of our lives, including the way we live, work, and communicate. IoT devices could be used in hybrid threats.

Another tool is diplomacy, the aim of which is to put pressure on the target government. This also includes propaganda, i.e., the spreading of information intended to influence public opinion, including the propaganda of violence, which spreads information aiming 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 which 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 and Zandee 2015, p. 30), 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).

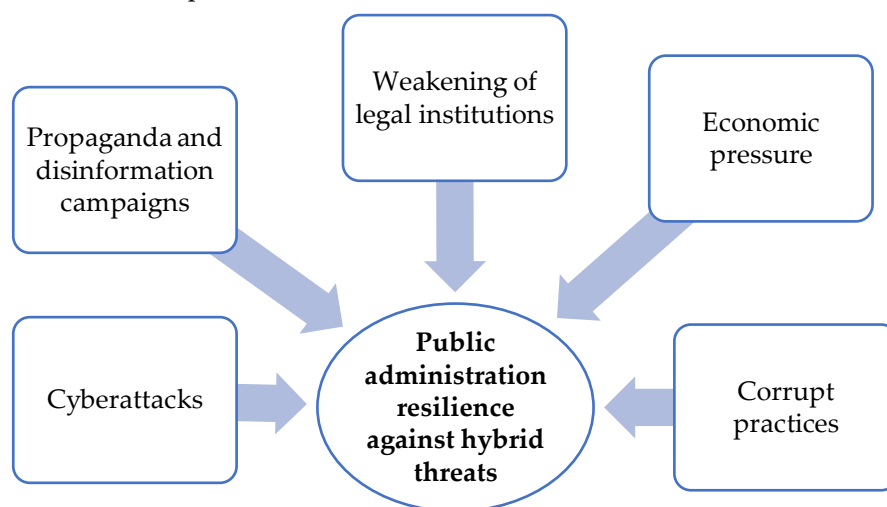
We adopt the *resilience* definition that encompasses a system's ability to resist disruption, maintain operations during disruption, and recover to full operational capacity after disruption (Bhamra et al. 2011, Amer et al. 2023, Yarveisy et al. 2020, Pawar et al. 2022). An organization's ability to 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, and 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 and Young 2015). Giannopoulos, Smith and Theocharidou (2021) state that role of the public administration is the implementation of laws and regulations.

Ensuring resilience with an emphasis on eliminating the effect of hybrid threats is the important role for public administration. 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. (2023) is the identification of factors important for the resistance of public administration to hybrid threats, including the importance of these factors in the Slovak Republic.



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

To the best of our knowledge, there is no index in the available literature that 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.

## 2. 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, integrations 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 step is to assign weights. Weighting is usually a methodologically problematic and highly controversial process. The last step is the aggregation of indicators (Gao et al. 2023).

According to Mecatti, Crippa, and Farina (2012) a number of sub-topics in which the macro-theme may be split should be first identified—representing measurable dimensions of the latent dimension under study. Then a pool of descriptive observable variables, interpreting these dimensions and to be suitably measured within every sub-topic, should be identified, with the purpose of quantifying each component of the macro-theme.

Composite indicators are increasingly recognized as a useful policy-making and public communication tool for conveying information about countries' 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).

### 2.1 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 the state is resistant to various hybrid threats, it is likely that the public administration will be able to continue providing services to citizens and businesses. The novel composite indicator KAPA has five dimensions that correspond to different aspects related to 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 - 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, 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.

#### 2.1.1 Cybersecurity

The first conflicts of the 21st century showed that information technologies and cyberspace can 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 cyber-attacks.

#### 2.1.2 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 and 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.

### *2.1.3 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. Regulations, both legal and administrative, 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, 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 as well as 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.

### *2.1.4 Corruption*

Corruption in public administration can be defined as the misuse of the apparatus of public administration 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 with the aim of achieving 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 multi-dimensional concept consisting of high impartiality and quality of public service delivery, along with 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, which range 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, in the rule of law and in 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.

### 2.1.5 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 the 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 ratio of general government debt to GDP.

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

**Table 1.** Structure of a composite indicator KAPA (according to Mecatti, Crippa, Farina 2012)

Macro subject: Public Administration Resilience Against Hybrid Threats					
	Sub-topic 1	Sub-topic 2	Sub-topic 3	Sub-topic 4	Sub-topic 5
	Resilience against cyber attacks	Resilience to dis-information	Legal resilience	Resilience against corruption	Resilience against sovereign debt crisis
Dimensions				Dimension Perception of corruption in the public sector (in European Quality of Government Index (EQI))	
	National Cybersecurity Index (NCSI)	Media Literacy Index (MLI)	Dimension Rule of Law (in World-wide Governance Indicators (WGI))		Ratio of general government debt to GDP
Indicators					

**Table 2.** Source and description of indicators

Indicator	Source	Minimum	Maximum	Direction: better is
NCSI	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 range from 0 to 1

## 2.2 Fuzzification

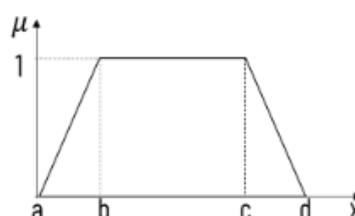
We construct the new index KAPA using the apparatus of fuzzy sets. Fuzzy sets were introduced by Lotfi A. Zadeh in 1965 as an extension of the classical notion of set. The central idea of fuzzy set theory is that an object belongs to more than one sets simultaneously. The closeness of the object to a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

$$A = \{(x, \mu_A(x)) : x \in A, \mu_A(x) \in (0,1)\},$$

where  $\mu_A(x)$  is a membership function. The value  $\mu_A(x)$  specifies the grade or degree to which any element  $x$  in  $A$  belongs to the fuzzy set  $A$ .

The membership functions play a pivotal role in fuzzy representation. The trapezoidal membership function (Figure 2) is defined by four parameters:  $a$ ,  $b$ ,  $c$ , and  $d$

$$\mu_{\text{trapezoidal}}(x; a, b, c, d) = \max\left(\min\left(\frac{x-a}{b-a}, 1, \frac{d-x}{d-c}, 0\right), 0\right)$$



**Figure 2.** The trapezoidal membership function

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

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

$$A_\alpha = \{(x : \mu_A(x) \geq \alpha)\}.$$

The  $\alpha$  – cut of a fuzzy set  $A$  is a crisp set. This simple but important relationship applies to  $\alpha$  – cuts of a fuzzy set  $A$ : If  $\alpha \leq \beta$ , then  $A_\beta \subseteq A_\alpha$

A crisp set of input data are gathered and converted to a fuzzy set using fuzzy linguistic variables, fuzzy linguistic terms and membership functions. This step is known as fuzzification.

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 analyzed factor”,  $T(X)$  is a set of terms used in the discussion of resilience against 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 analyzed factor) is  $T^{i+1} = \{\text{resilient}\} \cup \{\text{very } T^i\}$ . Semantic rule  $M$  associated with linguistic term of resilient with its meaning is

$M(\text{resilient}) = \{u, \mu_{\text{resilient}}(u); u \in \langle 0, 100 \rangle\}$  where  $\mu_{\text{resilient}}(u)$  is 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  $\mu_X(u)$  of  $U$ , then linguistic hedges “very” and “more or less” are constructed by mathematical representations as follows (Huynh, Ho, and Nakamori 2002)

Very  $X = \text{CON}(X)$ , where  $\mu_{\text{CON}(X)}(u) = (\mu_X(u))^2$ ;

More or less  $X = \text{DIL}(X)$ , where  $\mu_{\text{DIL}(X)}(u) = (\mu_X(u))^{0.5}$

Not  $X = \text{NEG}(X)$ , where  $\mu_{\text{NEG}(X)}(u) = 1 - \mu_X(u)$

### 2.3 Weighting

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, which we use, is equal weighting, where all indicators are attached with the same importance.

### 2.4 Aggregation

Aggregation functions combine input values into a single output value, which represents all the inputs. Radko, Kolesárová, 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  $F : R^n \rightarrow R$ , that has an associated vector  $w = (w_1, w_2, \dots, w_n)^T$  such as  $w_i \in \langle 0, 1 \rangle$  and  $\sum w_i = 1$ . Then  $F(a_1, a_2, \dots, a_n) = \sum w_j b_j$ , where  $b_j$  is the  $j$ -th largest element of the  $\{a_1, a_2, \dots, a_n\}$ . We use a special type of OWA aggregation operator - averaging operator  $w_A = ((1/n, 1/n, \dots, 1/n))^T$ . Then  $F(a_1, a_2, \dots, a_n) = \frac{1}{n} \sum a_j$ . OWA operators appear to be particular cases of Choquet integral with respect to a suitable fuzzy measure (Grabisch 1997).

### 2.5 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 works to prevent conflict and promote 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, and all of this makes 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. The reason for this is that 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.

## 3. Results and discussion

We included five indicators in the analysis, the selection of which is based on a literature review, and 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 Dimension Rule of Law (54.6184). The third largest variability is the MLI (23.1326). Skewness is a measurement of the distortion of symmetrical distribution or asymmetry in a data set. Data distribution is for three indicators nearly symmetrical (skewness between -0.5 and 0.5) – Rule of law, MLI, Perception of corruption in the public sector (EQI). Others are skewed. All indicators except General government debt to GDP, have negative skewness. This means majority 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.

**Table 3.** Descriptive statistics

Indicator	Min	Max	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

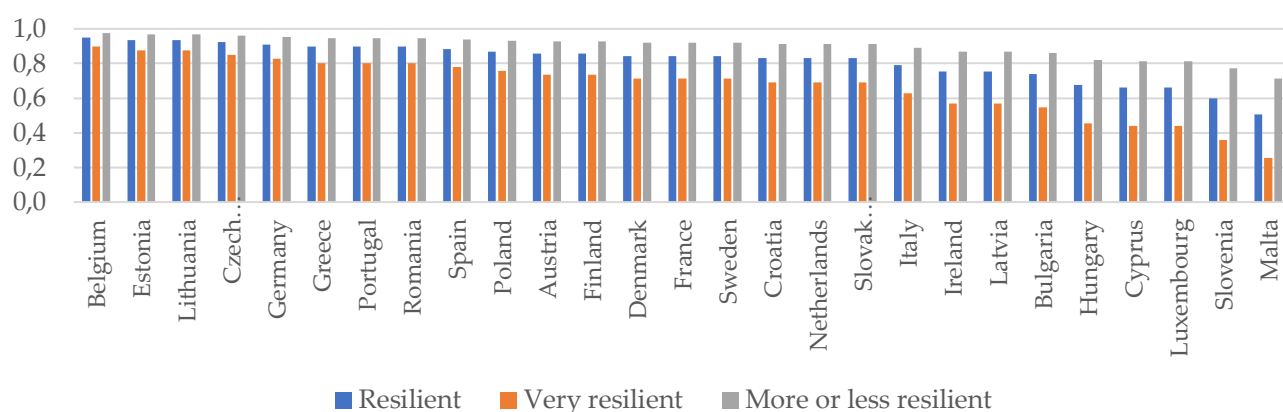
In the first step of KAPA index construction, we fuzzify the values of individual dimensions. In Table are described linguistic variables associates with dimensions of the index KAPA.

**Table 4.** Linguistic variable

Dimension	Linguistic variable X	Universe U	Membership function $\mu_{resilient}(u)$
Resilience against cyber attacks	Resilience against cyber attacks	$\langle 0, 100 \rangle$	$\max\left(\min\left(\frac{u}{100}, 1\right), 0\right)$
Resilience to disinformation	Resilience to disinformation	$\langle 0, 100 \rangle$	$\max\left(\min\left(\frac{u}{100}, 1\right), 0\right)$
Legal resilience	Resiliency in complying with the law and ensuring safety	$\langle -2.5, 2.5 \rangle$	$\max\left(\min\left(\frac{u + 2.5}{5}, 1\right), 0\right)$

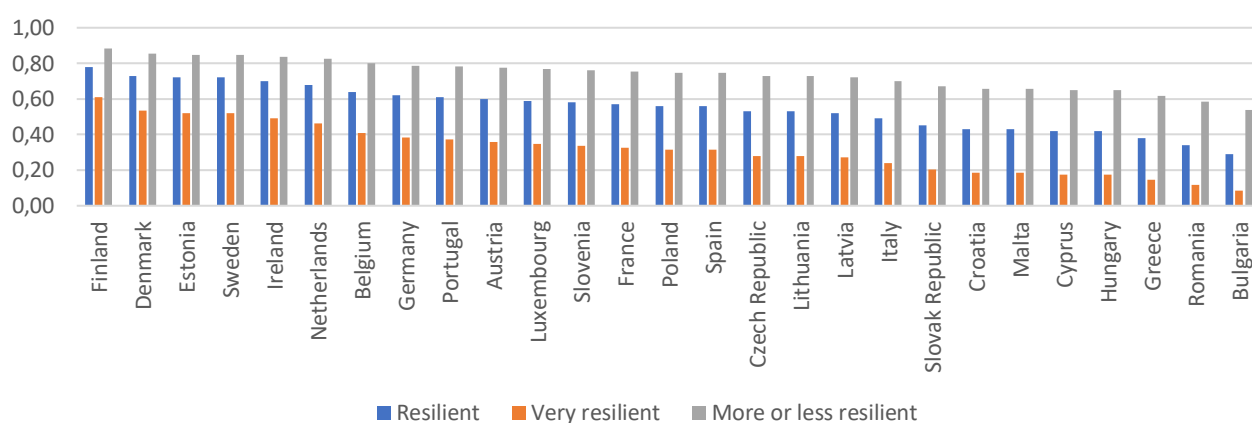
Resilience against corruption	Resilience against corruption	$\langle 0, 1 \rangle$	$\max(\min(u, 1), 0)$
Resilience against sovereign debt crisis	Resilience against sovereign debt crisis	$\langle 15, 225 \rangle$	$\max\left(\min\left(\frac{225 - u}{210}, 1\right), 0\right)$

Very resilient against cyber-attacks are countries that belong to 0.80-cut of a fuzzy set “very resilient”. They are countries Belgium, Estonia, Lithuania, Czech Republic, Germany, Greece, Portugal, Romania (Figure 3). Resilient against cyber-attacks are countries that belong to 0.80-cut of a fuzzy set “resilient” i.e., very resilient countries and countries Spain, Poland, Austria, Finland, Denmark, France, Sweden, Croatia, Netherlands, and Slovak Republic. More or less resilient against cyber-attacks are countries that belong to 0.80-cut of a fuzzy set “more or less resilient”, i.e., resilient countries and Italy, Ireland, Latvia, Bulgaria, Hungary, Cyprus, Luxembourg. Slovenia and Malta belong to indefinite countries, because they do not belong to the 0.80-cut of any fuzzy set.



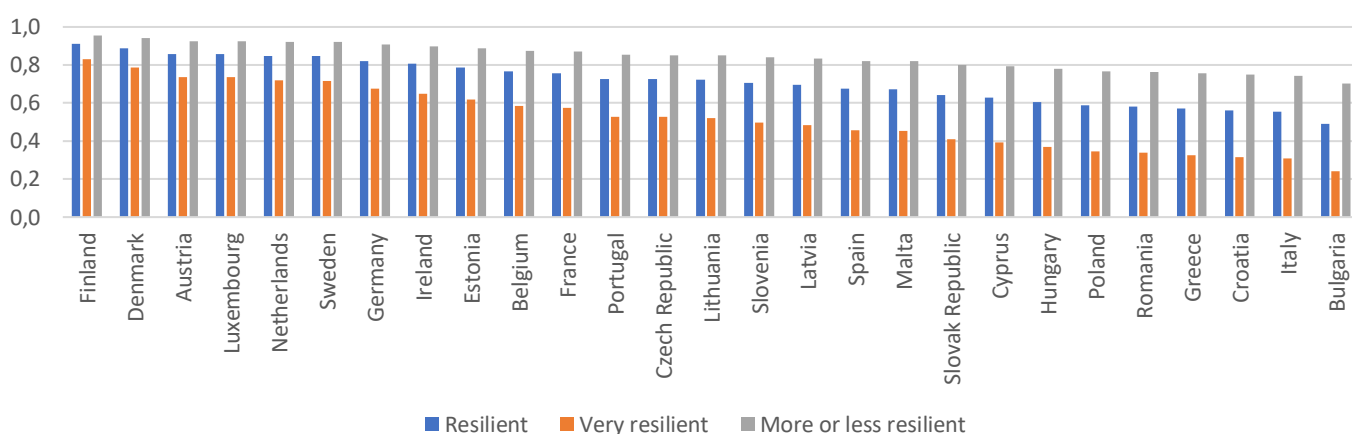
**Figure 3.** Resilience against cyber attacks

Finland, Denmark, Estonia, Sweden, Ireland, Netherlands, and Belgium are more or less resilient to disinformation (Figure 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.



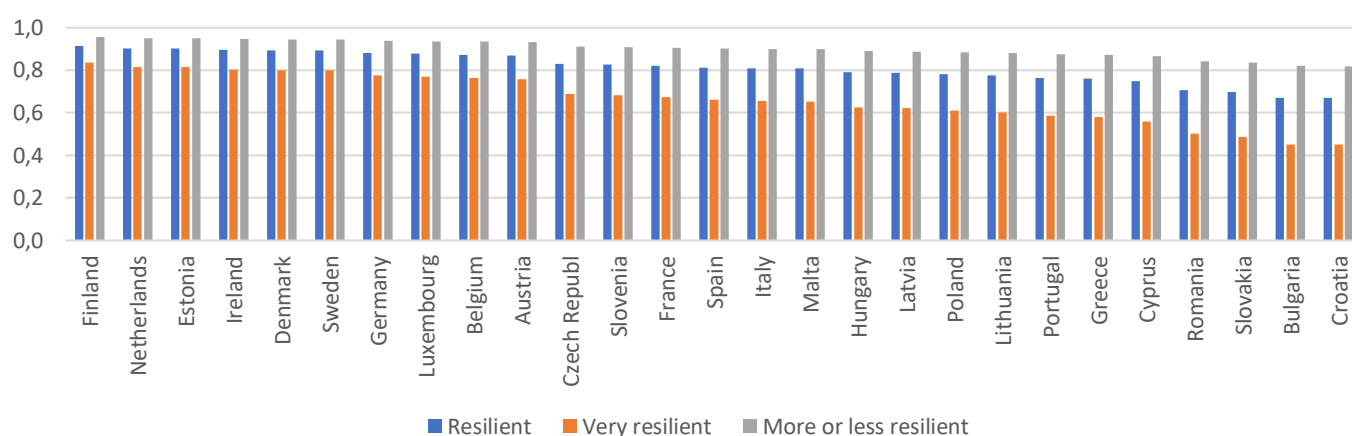
**Figure 4.** Resilience to disinformation

Very resilient in complying with the law and ensuring safety is only Finland (Figure 5). Resilient are Finland, Denmark, Austria, Luxembourg, Netherlands, Sweden, Germany, and Ireland. More or resilient are resilient countries and Estonia, Belgium, France, Portugal, Czech republic, Lithuania, slovenia, Latvia, Spain, Malta, and Slovak Republic.



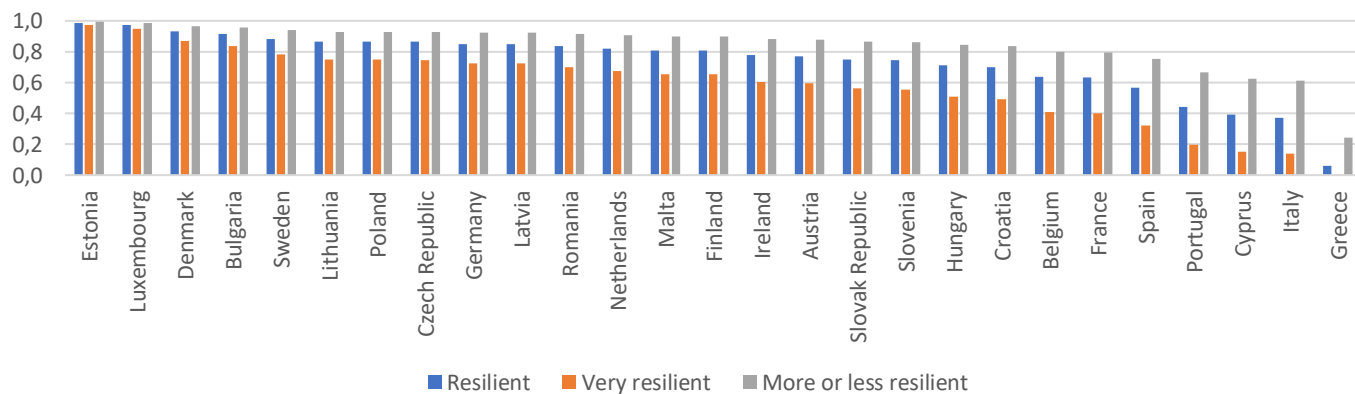
**Figure 5.** Resilience in complying with the law and ensuring safety

Very resilient to corruption are four countries - Finland, Netherlands, Estonia, and Ireland (Figure 6). Resilient are very resilient countries and Denmark, Sweden, Germany, Luxembourg, Belgium, Austria, Czech Republic, Slovenia, France, Spain, Italy and Malta. More or less resilient are all EU countries.



**Figure 6.** Resilience against corruption

Very resilient against sovereign debt crisis are countries Estonia, Luxembourg, Denmark, and Bulgaria (Figure 7). Resilient countries are very resilient and Sweden, Lithuania, Poland, Czech Republic, Germany, Latvia, Romania, Netherlands, Malta, and Finland. Very nonresilient is Greece with ratio of general government debt to GDP higher as 200 percent. More or less resilient are very resilient countries, resilient countries, and Ireland, Austria, Slovak Republic, Slovenia, Hungary, and Croatia. Countries 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 very high ratio of general government debt to GDP.



**Figure 7.** Resilience against sovereign debt crisis

In the second step we aggregate the membership functions. We use a special type of OWA aggregation operator - averaging operator  $w_A$ . The higher the value of the KAPA index, the higher the resilience of public administration to hybrid threats.

Table 4 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.

**Table 4.** 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 cyber-attacks, RD-Resilience to disinformation, LS-Resiliency in complying with the law and ensuring safety, PC-Resilience against corruption, DC-Resilience against sovereign debt crisis

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

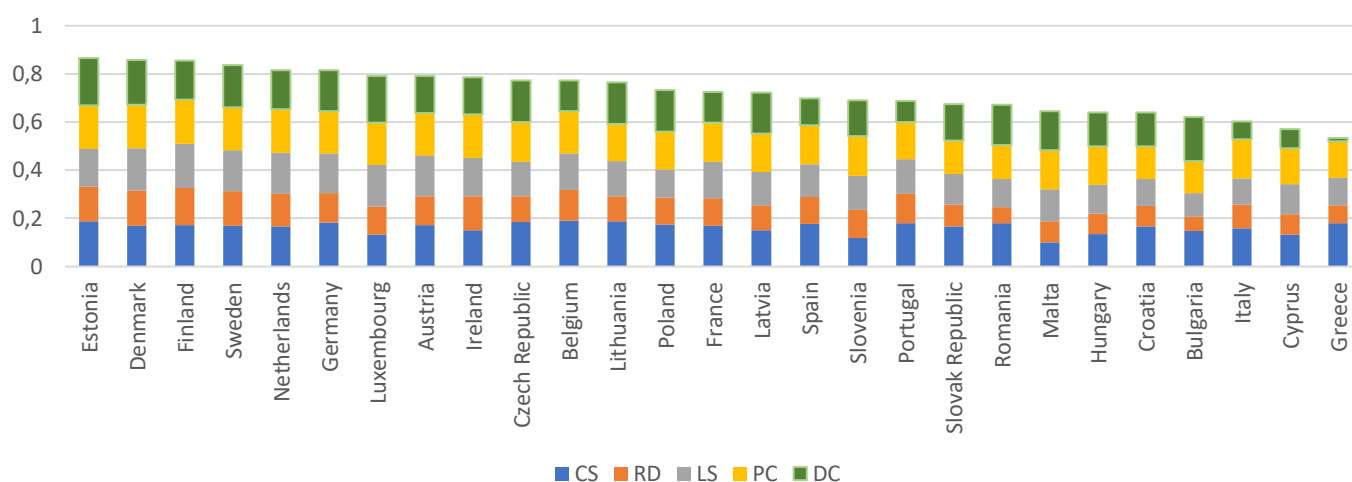


Figure 8. Structure of the index KAPA

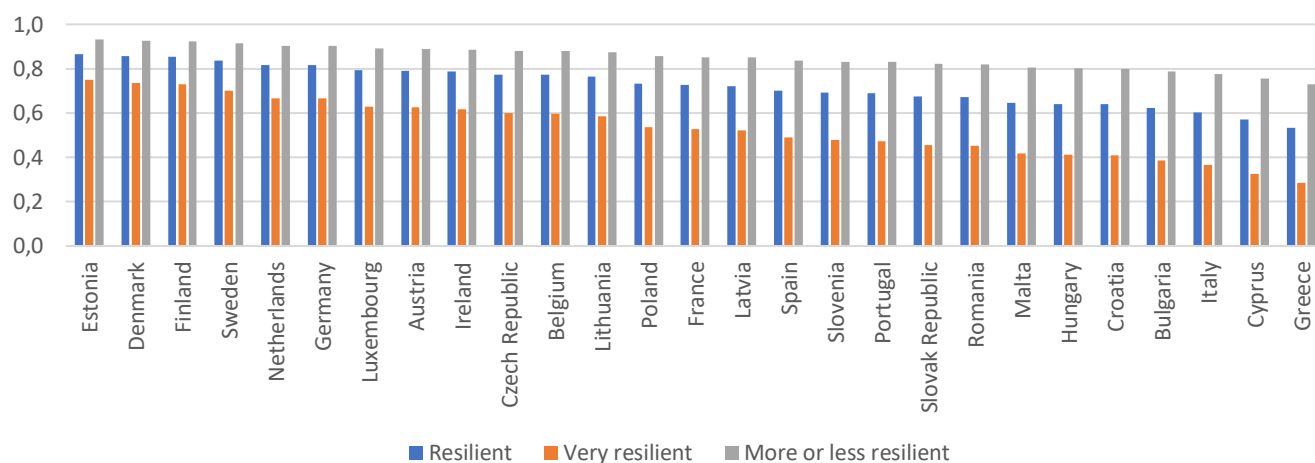


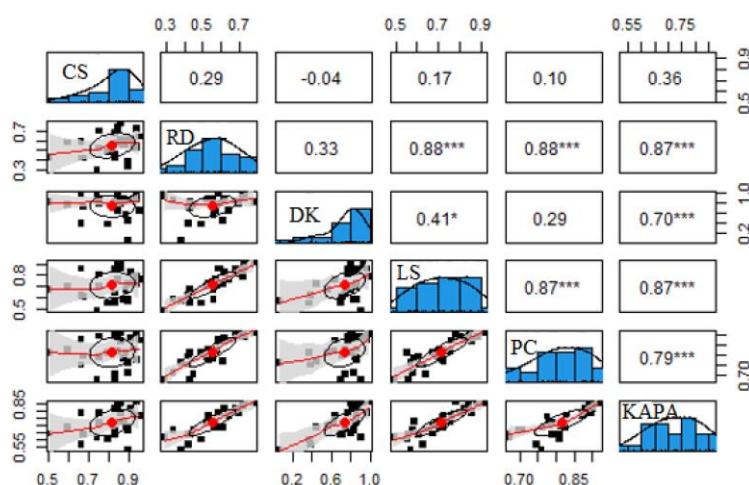
Figure 9. Resilience of public administration against hybrid threats

No EU country has a very resilient public administration against hybrid threats (Figure 9). Only six countries are resistant: Estonia, Denmark, Finland, Sweden, 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 value of GDP per capita. 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 countries that are resilient and 16 others. They are indefinite countries - Croatia, Bulgaria, Italy, Cyprus, and Greece in terms of resilience public administration against hybrid threats. All the listed states have membership function values in at least three value dimensions among the worst ranked states.



**Figure 10.** Values of the KAPA index in EU countries

All dimensions of the KAPA index show statistically significant dependence (Figure 3) 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 – with the aim of raising 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. Statistical methods did not confirm our assumption that the higher the cyber security of a particular country, the more resistant the public administration is to cyber-attacks. Nevertheless, we argue that resilience against cyber threats is an important part of resilience against hybrid threats. 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. It is necessary to create an effective cyber security management system that will ensure the implementation and compliance with the legislation.

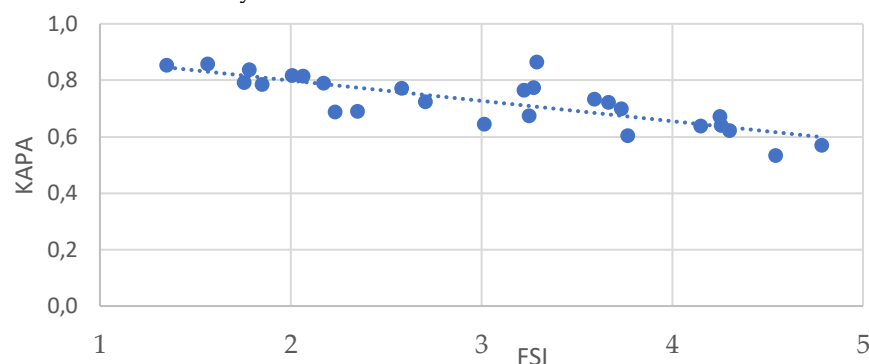


**Figure 11.** Dependencies of the dimension with the KAPA index

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  $6.023 \times 10^{-7}$ ). This means that there is an indirect linear relationship between the KAPA and FSI indices. This dependence is described even better by the 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.



**Figure 12.** Dependence between the new KAPA index and the FSI index.

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. Weak states (as assessed using the FSI) have weak state institutions which are less capable of facing the complex challenges of hybrid threats. They often have higher levels of corruption and crime, which creates an environment in which 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.

## 5. Conclusions

Europe is facing new security challenges. One of the most significant challenges is hybrid threats. To the best of our knowledge, there is no index in the available literature that would measure resilience to hybrid threats, nor specifically the resilience of public administration. The Public Administration Resilience Index Against Hybrid Threats (KAPA) is a novel index. The proposed index has five dimensions – cybersecurity, resistance to disinformation, compliance with laws and security, protection against corruption, prevention of a sovereign debt crisis. According to the KAPA index, countries ranked best are Estonia, Denmark, Finland, Sweden, and the Netherlands.

There are opportunities to improve the index using other aggregation methods. Further research may concern the determination of indicator weights. Another possibility in further research is the analogous creation of a general index of resistance to hybrid threats.

## Author Contributions

Conceptualization, A.K. and M.P.; Methodology, A.K. and B.S.; Software, S.B. and M.G.; Validation, A.K. and B.S.; Formal analysis, A.K. and M.G.; Investigation, M. P. and A.K.; Resources, B.S.; Data curation, S.B.; Writing—original draft, A.K. and B.S.; Writing—review & editing M.G.; Visualization, M.G. and B.S.; Supervision, A.K. and B.S.; Project administration, A.K. All authors have read and agreed to the published version of the manuscript.

## Funding

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.

## Informed Consent Statement

Not applicable.

**Data Availability**

The data supporting the results of the study are publicly available at the e-Governance Academy in Estonia, European Policies Initiative, World Bank, Fund for Peace, and Eurostat.

**Conflicts of Interest**

The authors declare no conflict of interest.

**References**

- Amer, Lamis, Celik, Nurcin, Andiroglu, Esber. 2023. Operationalizing resilience: A deductive fault-driven resilience index for enabling adaptation. *Process Safety and Environmental Protection* 177: 1085–1102. <https://doi.org/10.1016/j.psep.2023.07.082>
- Bajarūnas, Eitvydas, and Vytautas Keršanskas. 2018. Hybrid threats: analysis of content, challenges posed and measures to overcome. *Lithuanian annual strategic review* 16: 123–170. <https://doi.org/10.2478/lasr-2018-0006>
- Bennett, W. Lance, and Steven Livingston. 2018. The disinformation order: Disruptive communication and the decline of democratic institutions. *European journal of communication* 33: 122–139.
- Bhamra, Ran, Samir Dani, and Kevin Burnard. 2011. Resilience: the concept, a literature review and future directions. *International journal of production research* 49: 5375–5393. <http://dx.doi.org/10.1080/00207543.2011.563826>
- Bojor, Laviniu. (2012). The Hybrid type of conflict – future challenge for military framework of actions, *The 18th International Scientific Conference „The Knowledge Based Organization”, Sibiu*, 24.
- Drent, Margriet, Robert J. Hendriks, and Dick Zandee. 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](https://www.clingendael.org/sites/default/files/pdfs/New%20Threats_New%20EU_Nato%20Responses_Clingendael_July2015.pdf) (accessed on 11 June 2023).
- Duberry, Jérôme. 2022. AI and the Weaponization of Information: Hybrid Threats Against Trust between Citizens and Democratic Institutions. In *Artificial Intelligence and Democracy* (pp. 158–194). Edward Elgar Publishing. <http://dx.doi.org/10.4337/9781788977319>
- e-Governance Academy National Cyber Security index NCSI. Available online: <https://ncsi.ega.ee/methodology/> (accessed on 10 May 2023).
- Fund for Peace. Fragile States Index Available online: <https://fragilestatesindex.org/wp-content/uploads/2021/05/fsi-2021.xlsx> (accessed on 10 May 2023).
- Gao, Peichao, Wang, Yuanhui, Wang, Haoyu, Song, Changqing, Ye, Sijing Wang, Xiangyu. 2023. A Pareto front-based approach for constructing composite index of sustainability without weights: A comparative study of implementations. *Ecological Indicators*, 155: 110919. <https://doi.org/10.1016/j.ecolind.2023.110919>
- Giannopoulos, Georgios, Smith, Hanna, and Theocharidou, Marianthi. 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, 2021, <https://doi.org/10.2760/44985>
- Glenn, Russell W. 2009. *Thoughts on hybrid conflict*. *Small Wars Journal* 2: 1–8.
- Gökce, Orhan. 2017. Definition and scope of hybrid threats. *Inquiry-Sarajevo Journal of Social Science* 3: 19–30.
- Grabisch, Michel. 1997. Alternative Representations of OWA Operators. pp. 73–85 In: Yager, R.R., Kacprzyk, J. (eds) *The Ordered Weighted Averaging Operators*. Springer, Boston, MA. [https://doi.org/10.1007/978-1-4615-6123-1\\_7](https://doi.org/10.1007/978-1-4615-6123-1_7)
- Hasanov, Fakhri, Fuad Mammadov, and Nayef Al-Musehel. "The effects of fiscal policy on non-oil economic growth." *Economies* 6.2 (2018): 27.



- Huynh, Van-Nam, Tu Bao Ho, and Yoshiteru Nakamori. 2002. A parametric representation of linguistic hedges in Zadeh's fuzzy logic. *International Journal of Approximate Reasoning* 30: 203-223.
- Hybrid CoE . 2020. Vulnerability and resilience of COI. <https://www.hybridcoe.fi/coi-vulnerabilities-and-resilience/>
- Charron, Nicholas, Lapuente, Victor, Bauhr, Monika, and Annoni Paola. 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. <https://doi.org/10.38191/iirr-jorr.22.008>
- Idso, Johannes, Torbjørn Årethun, and Bharat P. Bhatta. 2018. The income equalization system among municipalities in Norway: Strengths and implications. *Economies* 6: 34.
- Ince, Huseyin, Imamoglu, Salih Zeki, Karakose, Mehmet Ali, and Turkcan, Hulya. 2017. The Search For Understanding Organizational Resilience. In M. Özşahin (Ed.), *Strategic Management of Corporate Sustainability, Social Responsibility and Innovativeness*, vol 34. *Euro-pean Proceedings of Social and Behavioural Sciences* (pp. 230-243). Future Academy. <https://doi.org/10.15405/epsbs.2017.12.02.20>
- Kacprzyk, Janusz, and Witold Pedrycz, eds. 2015. *Springer handbook of computational intelligence*. Springer. <https://doi.org/10.1007/978-3-662-43505-2>
- Kettl, Donald F. 2018. *Politics of the Administrative Process*. 7th ed. Los Angeles: CQ Press.
- Koraus Antonin, Palinchak Mykola, Gombar Miroslav, and Stehlikova Beata. 2023. The resilience of public administration to hybrid threats in the context of sustainable competitiveness of a country. Sent to *Journal of Competitiveness*.
- Maryska, Milos, Doucek, Petr, Nedomova, Lea, and Sladek, Pavel. 2018. The energy industry in the Czech Republic: On the way to the Internet of Things. *Economies* 6: 36. <https://doi.org/10.3390/economies6020036>
- Mazzucchi, Nicolas. 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> (accessed on 30 August 2023).
- Mecatti, Fulvia, Franca Crippa, and Patrizia Farina. 2012. A special gen (d) re of statistics: Roots, development and methodological prospects of gender statistics. *International Statistical Review* 80.3: 452-467. <https://doi.org/10.1111/j.1751-5823.2012.00186.x>
- Nardo, Michela, Saisana, Michaela, Saltelli, Andrea and Tarantol, Stefano. 2005. Tools for composite indicators building. *European Comission, Ispra* 15.1: 19-20.
- Novák, Vilém. 1990. *Fuzzy množiny a jejich aplikace*. SNTL, Praha
- Pawar, Bhushan, Huffman, Mitchell, Khan, Faisal , and Wang, Qingsheng. 2022. Resilience assessment framework for fast response process systems. *Process Safety and Environmental Protection*, 163: 82-93. <https://doi.org/10.1016/j.psep.2022.05.016>
- Pawlak, Patryk. 2017. *Countering hybrid threats: EU-NATO cooperation*. Available online: . <https://policycommons.net/artifacts/1338529/countering-hybrid-threats/1947195/> (accessed on 30 June 2023).
- Peters, Georg. 2009. Granular Computing. *Encyclopedia of Artificial Intelligence*. IGI Global, 74-780.
- Pollard, Neal A. 2002. Globalization's Bastards: Illegitimate Non-State Actors in International Law. *Low Intensity Conflict & Law Enforcement* 11: 210-238 <https://doi.org/10.1080/0966284042000279009>
- OSIS: *Media Literacy Index*. 2021. Available online: <https://osis.bg/?p=3750&lang=en>
- Mesiar, Radko, Kolesárová, Anna, Komorníková, Magda. 2015. Aggregation Functions on [0,1]. In: Kacprzyk, J., Pedrycz, W. (eds) *Springer Handbook of Computational Intelligence*. Springer Handbooks. Springer, Berlin, Heidelberg. [https://doi.org/10.1007/978-3-662-43505-2\\_4](https://doi.org/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/>. 668  
669
- Revelle, William. 2022. psych: *Procedures for Personality and Psychological Research*, Northwestern University, Evanston, Illinois, USA, <https://CRAN.R-project.org/package=psych> Version = 2.2.5. 670  
671  
672
- Treverton, Gregory 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. Web. 11 Apr. 2023. 673  
674  
675  
676
- University of Gothenburg. *European Quality of Government Index*. Available online: <https://nicholascharron.files.wordpress.com/2018/08/eqi-data-qog-webpage.xlsx> 677  
678
- Wallace, Helen, Mark A Pollack, and Alasdair R Young. 2015. *Policy-Making in the European Union*. 7th ed. Oxford: Oxford University Press. 679  
680
- Wang, Yuanhui, Song, Changqing, Cheng, Changxiu, Wang, Haoyu, Wang, Xiangyu, and Gao, Peichao. 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. <https://doi.org/10.1016/j.cities.2022.104151> 681  
682  
683  
684  
685
- World Bank: WGI Available online: <https://www.govindicators.org/> 686
- Yarveisy, Rioshar, Chuan Gao, and Faisal Khan. 2020. A simple yet robust resilience assessment metrics. *Reliability Engineering & System Safety*. 197: 106810. <https://doi.org/10.1016/j.res.2020.106810> 687  
688  
689
- Zandee, Dick, Sico van der Meer, and Adája Stoetman. 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> (accessed on 15 June 2023). 690  
691  
692  
693

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content. 694  
695  
696  
697

698

699