Tomasz Chłoń
Robert Kupiecki

Towards FIMI Resilience Council in Poland

Research and Progress

Łukasiewicz PORT

Faculty of Political Science and International Studies
University of Warsaw

Tomasz Chłoń
Robert Kupiecki

Towards FIMI Resilience Council in Poland

Research and Progress

Reviewers:
Onno Hansen-Staszyński
Wojciech Dzięgiel

Publishers:
Faculty of Political Science and International Studies, University of Warsaw
Łukasiewicz – PORT Polish Center for Technology Development

Warszawa – Wrocław 2025

ISBN 978-83-969186-4-2

ISBN 978-83-974215-0-9

Funded by
the European Union

This report has been prepared under Project SAUFEX
(Secure Automated Unified Framework for Exchange) financed
by the European Union under the HORIZON EUROPE program.
Grant Agreement no: 101132494

Saufex

Łukasiewicz
PORT

Faculty of Political Science
and International Studies
University of Warsaw

Table of Contents

Summary

Aim of the report

This report constitutes a deliverable within the SAUFEX project. It contains research offering inferences and lessons-learned from existing resilience councils as a multi-stakeholder approach (public-private-NGO) to address challenges to a societal resilience. The report also strengthens the rationale for establishing a Resilience Council (RC) in Poland as a critical component in addressing Foreign Information Manipulation and Interference (FIMI). It seeks to develop a coordinated, multi-stakeholder approach that integrates expertise from government, academia, civil society, and the private sector to enhance societal resilience against the evolving threats of disinformation. This report also aims to universalize this instrument as a possible way forward for the European Union to act against disinformation and foreign manipulation in the information space.

Implementation and innovation

This document presents a framework for the formation and operationalization of resilience councils, emphasising a holistic approach that includes public consultation, stakeholder engagement, and interdisciplinary collaboration. The approach builds on social science research, technological development, and policy innovation to create resilient structures capable of mitigating the impact of FIMI. Resilience, which is a key element of the proposed resilience councils, is defined for the SAUFEX project as: (1) anticipating, preventing, detecting, and evaluating FIMI incidents and campaigns; combating and removing its effects; and restoring society to its previous state after a major FIMI event; and (2) supporting efforts to empower citizen resilience and strengthen the system to make it more resistant to damage.

Methodology and approach

The methodology of SAUFEX integrates multiple work streams. Social science research informs its understanding of disinformation's societal impacts and guides community-based interventions; technological development supports the detection, analysis, and counteraction of disinformation; community involvement ensures that the Resilience Councils are rooted in local and regional contexts, benefiting from broad-based public support; and policy engagement serves to align with and influence existing regulatory frameworks, ensuring the sustainability of resilience initiatives. This document outlines the process of public consultation and stakeholder involvement, which are a key aspect of ensuring the relevance and effectiveness of resilience councils. It also details the creation of structured frameworks and protocols that will guide the councils' operations.

Anticipated utility of major findings and recommendations

This deliverable is expected to yield important findings on the operational effectiveness of resilience councils in combating FIMI. Recommendations will likely focus on strengthening collaboration among governmental, non-governmental, and private entities; enhancing data-sharing mechanisms to improve transparency and coordination; and refining policy frameworks to better support the operational goals of resilience councils.

Potential shortcomings and limitations

The project may face several challenges, including balancing the diverse interests of stakeholders involved in resilience councils, addressing technological limitations that may impede the development of effective countermeasures, and navigating complex policy and regulatory environments that could affect the implementation of recommended actions.

Conclusion

This report sets out a detailed plan for the establishment of resilience councils as part of a broader EU effort to counteract FIMI. The document emphasises the importance of interdisciplinary collaboration, public consultation, and stakeholder engagement in building robust defences against disinformation. While the project acknowledges potential challenges, it remains focused on creating resilient and adaptable structures capable of withstanding and countering FIMI threats across the EU.

Abbreviations and acronyms

Abbr.	Meaning	Description
ABCDE	Actors, Behaviour, Content, Degree, and Effect	This tool for analysing disinformation breaks down disinformation into the ABCDE categories to improve coordination and communication among stakeholders.
ACR	Alliance for Climate Resilience	A coalition focused on enhancing climate resilience through collaborative efforts and policy development.
AIDR	Australian Institute for Disaster Resilience	An institute dedicated to improving disaster resilience and management in Australia.
ARC	Alabama Resilience Council	A state-level council focused on enhancing community resilience in Alabama.
BCI	Business Continuity Institute	An organisation that provides education and resources for business continuity and resilience planning.
BENSRC	Business Executives for National Security Resilience Council	A council of business leaders working to enhance national security through resilience initiatives.
BRC	Business Resilience Council	A council focused on improving business resilience against various threats.
BRIC	Building Resilient Infrastructure and Communities	A programme aimed at supporting communities in enhancing resilience through infrastructure investments.
C40	40 Cities Climate Leadership Group	A network of the world's megacities committed to addressing climate change and resilience challenges.
CDRI	The Coalition for Disaster Resilient Infrastructure	A global partnership that aims to promote the resilience of infrastructure systems to climate and disaster risks.
CEPI	Coalition for Epidemic Preparedness Innovations	An organisation working to accelerate the development of vaccines against emerging infectious diseases.
CGIAR	Consultative Group on International Agricultural Research	A global partnership focused on agricultural research for development.

DERC	Digital Europe Resilience Council	A council dedicated to improving digital resilience within the European Union.
DSC	Digital Service Coordinators	Officials supported by resilience councils who are responsible for overseeing compliance of digital service providers with regulations and coordinating enforcement actions against FIMI.
DSA	Digital Services Act	EU legislation that sets rules for digital services and platforms to ensure a safer and more accountable online environment.
EEAS	European External Action Service	The diplomatic service and combined foreign and defence ministry of the European Union.
EMoD	European Master of Disinformation	Proposed training course within SAUFEX aimed at educating Digital Service Coordinators on FIMI and related challenges.
EU	European Union	A political and economic union of 27 European countries that are located primarily in Europe.
FAO	UN Food and Agriculture Organization	An agency of the United Nations that leads international efforts to defeat hunger and improve agriculture.
FBDRC	Fiji Business Disaster Resilience Council	A council in Fiji focused on enhancing business resilience to disasters.
FEMA	Federal Emergency Management Agency	A U.S. government agency responsible for coordinating the federal response to disasters and emergencies.
FIMI	Foreign Information Manipulation and Interference	Acts of manipulating or interfering with information by foreign entities aimed at undermining democratic processes and national security.
FIMI RC	Resilience Council against FIMI	A council focused on addressing and mitigating FIMI threats.
FIMI RC PL	Resilience Council against FIMI Poland	The Polish branch of the FIMI Resilience Council focused on combating FIMI threats.
FSC	Global Food Security Cluster	A coordination body aimed at ensuring food security in emergency situations.
GCA	Global Cyber Alliance	An international coalition working to reduce cyber risk and improve global cybersecurity.
GFCE	The Global Forum on Cyber Expertise	A global platform that promotes cyber capacity building and expertise sharing among countries.

GHS	Global Health Security	Initiatives and measures aimed at protecting global public health from threats and crises.
GHSA	Global Health Security Agenda	A global initiative to strengthen the world's ability to prevent, detect, and respond to infectious disease threats.
GRC	Global Resilience Council	A council dedicated to improving global resilience against various threats, including climate change and cyber risks.
GRI	Global Resilience Institute	An institute focused on research and education in global resilience and disaster risk reduction.
GRP	Global Resilience Partnership	A partnership that aims to build resilience in vulnerable communities affected by climate change and disasters.
GTTRC	Global Travel and Tourism Resilience Council	A council focused on enhancing resilience in the global travel and tourism industry.
GWPSA	Global Water Partnership Southern Africa	A partnership focused on water resource management and resilience in Southern Africa.
GYRN	Global Youth Resilience Network	A network aimed at empowering young people to contribute to global resilience efforts.
ICLEI	Local Governments for Sustainability	A global network of local governments committed to sustainable urban development.
IFRC	The International Federation of Red Cross and Red Crescent Societies	A global humanitarian network that provides assistance without discrimination during emergencies.
MEN	Ministry of Education	The government department responsible for a country's primary and secondary education.
MFA	Ministry of Foreign Affairs	The government department responsible for a country's foreign relations and diplomacy.
MPS	Ministry of Social Policy	The government department responsible for a country's social and family issues.
NAC	National Advisory Council	A body that provides advice and recommendations on national security and resilience issues.
NASK	Naukowa i Akademicka Sieć Komputerowa	A Polish research and development organisation that operates the national research and education network.

NGO	Non-governmental organisation	An independent organisation that operates without government control, typically focused on humanitarian or social issues.
OEC	Office of Electronic Communications	The national regulatory authority responsible for communications and electronic services in a country.
RA	Resilience Alliance	A global network focused on enhancing resilience through collaborative research and innovation.
RAN	Resilient Agriculture Network	A network focused on improving agricultural resilience to climate change and other threats.
RCs	Resilience Councils	Bodies within SAUFEX that coordinate strategic and political responses to FIMI threats, providing a standardised EU-wide solution space and improving intra-EU coordination.
RRC	Resilience Research Centre	A research centre dedicated to studying and improving resilience in various domains, including disaster management and climate adaptation.
SAUFEX	Secure Automated Unified Framework for Exchange	A project endorsed by various international bodies, aiming to advance the state-of-the-art in combating FIMI.
SOP	Standard Operating Procedure	A set of step-by-step instructions compiled by an organisation to help workers carry out complex routine operations.
TTPs	Techniques, tactics and procedures	A wide range of techniques, tactics and procedures used to harm and disrupt societies.
ULI	Urban Land Institute	A global non-profit organisation that provides leadership in the responsible use of land and creating and sustaining thriving communities.
USRC	U.S. Resiliency Council	A U.S. organisation focused on promoting resilience in buildings and infrastructure against natural disasters.
VBRC	Vanuatu Business Resilience Council	A council in Vanuatu focused on improving business resilience to disasters and economic shocks.
WFP	World Food Programme	The food assistance branch of the United Nations that provides food security and nutrition in emergencies and works to eradicate hunger.

Part A

Introductory remarks

Foreign Information Manipulation and Interference (FIMI), or international disinformation, poses a threat to social cohesion, stability, and the internal order of democratic states (Brandt, 2022). As stated in the G7 Foreign Ministers' Statement of April 2024, "FIMI negatively affects the ability of citizens to make rational, informed decisions, which lies at the very heart of our democratic institutions and aims at undermining confidence in democratic governments and societies. Disinformation can be used to polarise society; it often supports violent extremist activities and is fuelled by malicious foreign players. Online disinformation campaigns are widely used by various malign actors to create and exacerbate tensions" (G7 Foreign Ministers' Statement, 2024).

Adopted by the European Union in 2022, the strengthened Code of Practice on Disinformation refers to previous declarations by the European Commission, similarly stating that: "The exposure of citizens to large-scale disinformation, including misleading or outright false information, is a major challenge for Europe. Our open democratic societies depend on public debates that allow well-informed citizens to express their will through free and fair political processes. The dissemination of disinformation has many facets, both online and offline, and is facilitated by and impacts a broad range of actors, and that all stakeholders in the ecosystem have roles to play in countering its spread" (2022 Strengthened Code of Practice on Disinformation).

The code of practice contains 44 commitments and 127 specific measures that encourage cooperation between experts and NGO and state institutions to increase the transparency and effectiveness of activities aimed at detecting disinformation and enhancing social resilience. These measures also aim to strengthen the monitoring and reporting framework with qualitative and quantitative information at the EU and Member State level. At the same time, the European Union declares that it is "mindful of the fundamental right to freedom of expression, freedom of information, and privacy, and of the delicate balance that must be struck between protecting fundamental rights and taking effective action to limit the spread and impact of otherwise lawful content".

Disinformation is therefore one of the threats addressed by EU policies on building social and institutional resilience. A broad approach to this problem is required, as noted in one of the recommendations of the joint document prepared by the EU Parliament and the Council, which proposes a strategic approach to resilience in the EU's external action. It states that: "Identifying and building upon existing positive sources of resilience is as important as tracking and responding to vulnerabilities. Such factors may take the form of institutionalised or informal democratic and good governance or justice systems, non-state institutions and organisations, embedded cultural norms and practices, or ad hoc community-driven solutions that complement state capacities or compensate for their absence. Resilience has to be addressed at multiple levels – state, society and community. Local governments and civil society are often the basis on which resilience can take root and grow at community level" (Joint Communication to the European Parliament and the Council, 2017).

This suggestion is right in all respects and retains its relevance today, particularly as European Union Member States and their citizens continue to face significant challenges in detecting and effectively combating FIMI in their own information space (Adler & Drieschova, 2021). It notably concerns the strategic "foreign" component of FIMI – namely the ability to attribute acts of

disinformation to specific perpetrators regardless of the techniques and means used by them. This translates to difficulties at the technical and operational levels of combating FIMI, including analytical processes regarding the tactics and techniques and procedures used by hostile actors in disinformation campaigns. Consequently, it also impacts the effectiveness of punitive action and regulatory precautions, which are essential to ensuring systemic social resilience. The maintenance of a "healthy infosphere" determines the actions of individuals, social groups, and states based on true and verified information and the reliability of the means, producers, and broadcasters of its message.

Resilience against FIMI-related risks and impacts requires multifaceted continuous action against inherently dynamic problems that are both complex and difficult to predict.

It must therefore go beyond the traditional general understanding of resilience as a systemic ability to withstand shocks and restore functionality after crises that result from them.

Combatting FIMI, which encompasses a wide range of techniques, tactics and procedures (TTPs) used to harm and disrupt societies, should include anticipatory and long-term preventive thinking, including adequate threat intelligence, an understanding of the information environment, a set of preparatory measures, and an understanding of the need for their continuous use. This necessitates an adaptive approach and cooperation between the state and civil society structures in any threat-mitigation action.

The purpose of such operational resilience is the social ability to withstand disturbances of the infosphere, including harmful information operations undertaken by hostile states against the freedoms and standards of a democratic society, so that state institutions remain capable of fulfilling their tasks and citizens can fulfil their aspirations. This serves as the working definition of resilience against FIMI adopted for the purposes of this report.

Such resilience is the responsibility of European Union Member States, permeating into all spheres of public life. Effective implementation requires the involvement of a social factor in activities conducive to reducing systemic vulnerabilities, particularly in such complex spheres as:

- Setting, evaluating, and validating resilience standards.
- Verification and measurement of the effectiveness of resilience levels.
- Cooperation of actors involved in fighting disinformation and maintaining the resilience of the infosphere.
- Improving the synergy and effectiveness of measures to combat FIMI in all manifestations.
- Understanding the interdependence of civil society organisations and government structures.
- Understanding the role of the technological factor as a source of disinformation threats as well as a tool to combat them.

Therefore, in line with the nature of the problem and the European Union's approach to tackling it, a modern understanding of resilience to FIMI-derived threats taken by hostile state and non-state actors to harm democratic societies must include three integral components:

1. An awareness that goes beyond the traditional understanding of resilience as a systemic readiness to withstand shocks and restore functionality after a crisis that results from them. This awareness must not be confined to silos defined by organisational frameworks or by the nature of entities bringing together individuals and organisations active in

the field. **Moreover, breaking down the "silos of knowledge and competence" should become an important demand in the development of the European Union's approach to combating disinformation.**

2. A propensity for systematic preventive actions resulting from relevant and up-to-date knowledge of the nature of threats and an understanding of the information environment and operational capacity. This includes a set of measures ready to be applied in different phases of actions to limit the effectiveness of FIMI. The systemic effectiveness of these actions and the optimal use of available resources and funds can only take place if the silos typical of state and non-governmental entities active in the field of combating disinformation are dismantled.

3. A structured "stakeholders' community" that brings together individuals, social organisations, and state institutions operating within a common mission and benefiting from a common pool of knowledge, experience, and material support measures. On the latter point, the state should take a leading role. This is also the logic behind Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act) (Regulation (EU) 2022/2065 (Digital Services Act)). It acts as a "legal constitution" to tackle illegal content online, including disinformation. To achieve the objectives enshrined in this document, legislators have indicated the need for cooperation between state institutions and independent civil society organisations, researchers, auditors, and experts.

Synergies between governmental structures and civil society are needed to optimise work to strengthen the systemic resilience of the infosphere and its users and reduce the gap between state authorities' activities and the expectations of society. This conclusion is consistent with the European Union's strategies, which approach the concept of resilience as the result of actions referred to as a "360 degrees approach" (Tocci, 2019). This approach is also reflected in the EU's strategic approach to security as reflected in the 2022 Strategic Compass for Security and Defence. It includes building strategies, policies, and models of conduct that consider the broadest possible spectrum of issues and perspectives for their assessment. This also applies to the fight against disinformation.

Applying this approach to the fight against FIMI and its effects therefore means accepting the need to involve the broadest possible community of actors and a multifaceted set of competences in a system that strengthens societal resilience and combats information pathologies. On the actors' side, a cross-sectoral cooperation of governmental regulators with a social factor that can increase the spectrum of good practices and expand expertise through training and exchange of information is particularly desirable.

Such a practice of breaking organisational, sectoral, and competence silos has long been a successful tactic used in various spheres of public life, economic sectors, and organisations representing industry interests (including public health, environmental protection, crisis management, construction, tourism, and engineering safety standards). It has been implemented by organisations with different ownership structures and operating models.[1] However, these practices always share a common feature focusing their operations on a collective goal of strengthening resilience against threats of a critical nature. They have considerable achievements, and their examination in terms of organisation and setting goals, operational strategies, and standards of public-private cooperation allows for the formulation

1 The term "resilience" often appears in their names.

of certain generalisations and conclusions. These may prove useful for collective resilience-oriented action in other policy sectors, like countering FIMI. The empirical examination of existing resilience councils prompts a general understanding of their "operational philosophy" as: **an effective modus operandi across the globe as a mechanism for sectoral, national, or international governance in different fields of activity with a common goal of increasing resilience, organised as a state-sponsored, community-led, or locally-led not-for-profit or commercial entity.[2]**

Their experience can serve as a premise for thinking about organised, state-supported, and widely legitimised actions (i.e., preventive, operational, consultative, regulatory, and educational) to fight disinformation in democratic countries. Nevertheless, the concept of establishing the FIMI Resilience Council (FIMI RC) and the actions already taken in Poland to implement it are an original project stemming from the above-mentioned premises, as well as the belief that resilience councils can solve the main structural problems and gaps in knowledge, cooperation, and good practices that are instrumental to upholding a resilient information ecosystem.

We therefore propose the establishment of a FIMI Resilience Council (FIMI RC) as a public consultative and advisory body that will bring together relevant stakeholders to improve systemic effectiveness in preventing and combating FIMI incidents as well as maintaining a "healthy infosphere" as part of a more general policy of empowering citizen resilience.

Based on the findings of case studies of structured resilience efforts across various sectors, the authors of this report assert that the combination of such institutional and expert competences could be strengthened through the establishment and accreditation of the FIMI RC as a social body supporting the legislative and executive powers, including the National Digital Services Coordinator. The council will gather experts and knowledge from relevant subject areas in the fight against disinformation, including state institutions, legal regulations, national security, the media and information space, education, psychology, and sociology.

The proposed FIMI RC's members would advise the national Digital Services Coordinator in all related fields using specialised tools, protocols, and knowledge to coordinate proactive and reactive strategic actions and policy implementation. This would aid in the prevention and combat of disinformation threats and promote uniform solutions across the EU while also improving internal coordination within the EU. As part of its consultative and advisory mission, the FIMI RC would also carry out research, empower citizen resilience, and advise on social control functions. Participation in the work of the council would therefore require expertise. The main objective of the establishment of the FIMI RC would be to decentralise and democratise processes related to the implementation of the Digital Services Act and their proper monitoring and allow for civil society to offer guidance and closely coordinate with the state. The FIMI RC would combine the state's efforts with those of the non-governmental sector, linking them more closely to the state's strategy. It would support actions for a resilient infosphere, including, but not limited to:

- Cooperation in the creation of regulations that enhance resilience and the implementation of adopted principles, rules of conduct, and codes of ethics.
- Building trust and standardising the expectations of various participants in these processes.
- Active monitoring of compliance with adopted standards of conduct.
- Continuous inflow of relevant expertise to improve the quality of stakeholder cooperation.

2 The above idea is the first author's attempt at a general conceptualisation of the phenomenon of resilience councils operating in the world.

The FIMI RC, representing a wide range of organisations and experts from civil society with experience working with legislative and executive bodies both in Poland and internationally, could play an important consultative role in developing the procedures for granting the status of "vetted researcher" or "trusted flagger" and certifying out-of-court dispute settlement bodies. The council could also advise the authorities on control and criminal proceedings.

Decentralising and democratising the processes for analysing and responding to FIMI risks and potentially high-impact or illegal content will offer significant societal benefits. By enabling greater transparency and civil society participation, these processes could lead to more informed decision-making and ultimately improve the resilience of democratic processes and institutions against hostile actions by foreign actors.

The establishment of a RC FIMI rooted in civil society will have the effect of strengthening overall social resilience. Thanks to the possibility of direct support from EU funds and potential funding through public-private partnerships, the council can become independent of shifting political will or modifications to the state budget. This model can transform the fight against foreign interference from a top-down approach to a peer-to-peer (if not bottom-up) approach, which could lead to a unique ecosystem for countering disinformation and other hybrid threats in the digital and information environment.

FIMI RC can play a key role in countering disinformation and building citizen resilience in Poland.

The council's activities in Poland could also serve as an example for the establishment of its counterparts in other EU Member States and associated countries, with the support of the Polish Presidency of the EU in 2025. The Polish FIMI RC also offers the potential to promote this model of cooperation as a precondition for the creation of an EU-wide FIMI RC as an independent entity, social organisation supported by an EU institution, or association of national organisations of a similar nature.

The authors of this report are convinced that due to the nature of the threat posed by FIMI, it is necessary to create common institutions guaranteeing synergy of goals of state actors and the NGO sector. This will allow for the aggregation of competences and resources, synergy of strategies and plans, and a systematic increase of relevant knowledge. This will only be possible through solid cooperation between stakeholders, development of a network for the exchange of knowledge and collaborative responses, and the elimination of communication barriers ("silos") to strengthen trust and better direct the energy of individual actors.

In this sense, this report attempts to present the essence of the resilience council as a model of building resilience that can be applied in the field of counteracting FIMI. It does this based on conclusions from the relevant literature and empirical studies of existing organisations of a similar nature. The ambition of the authors is to create solid conceptual and operational foundations for the creation of the first FIMI RC in Poland. The Polish resilience council's activities should be an important venue for analysis and a process led by lessons-learned, which will in turn could lead to the possible universalization of this solution and creation of an EU-wide RC FIMI. This body would play an important role in connecting state decision-makers, social activists, practitioners, and research communities, who must act together in the face of growing threats of international disinformation.

Why a FIMI RC?

1. To secure a healthy infospace that contains accurate and vital information, which allows societies, groups, and individuals to secure their needs and prospects for unhindered decision-making regarding personal choices and public policies.
2. To consolidate the "whole-of-stakeholders" community and an "all-FIMI-related -threats" approach.
3. To make cooperation a daily practice that synergizes efforts, raises the legitimacy of action, and optimises results.

Countering FIMI requires networking across government and NGO sectors. The prevalence of incidents below the detection or attribution threshold is indicative of the weakness of prevention and countermeasures within institutional or sectoral silos.

Methodological note

FIMI RC is an innovative project in the field of countering disinformation that uses existing resilience building operational patterns from other public policy sectors, business domains, and local governments. These existing organisations operate in various geographical regions under differing ownership and organisational settings with diversified socio-economic contexts and subject areas. The authors of this report have studied over 100 such cases of structures that combine the efforts of diverse actors linked by a common goal and operational principles of action related to building resilience. This sample appears to be quantitatively representative, both for the generalisations made and the search for their application to the proposed FIMI RC. Out of these, the authors have selected 43 cases that meet the set criteria characteristic for resilience councils.[3]

During their research, the authors of the report observed two groups of criteria allowing the existing organisations to be categorised as resilience councils according to: their organisation's operational centre and ownership (criterion A) and the main areas of responsibility (criterion B).

Under criterion A, resilience councils are identified as organisations:

1. which are state structures that have invited entities from the NGO sector to cooperate,
2. are bottom-up initiatives of entities from specific sectors of the economy, or
3. are run by local governments.

The main comparable activities that fulfil criterion B relate to:

1. crisis prevention and management,
2. exchange of information and good practices, and
3. operational resilience (i.e. resulting from the adopted model of cooperation and its consolidation in stakeholders' practices).

Qualitative analysis of the declared missions and objectives of the organisations surveyed, which are explicitly referred to as "resilience councils" or operate under other names but meet the above criteria, allows the results obtained to be considered satisfactory. The empirical material was collected by examining content that is publicly available online, including official documents, strategies, and publications related to the organisations' policies. This report also utilizes data and observations from several publications to inform its operational recommendations, particularly on the issue of group (organisational) learning (Levitt & March, 1988; Huber, 1991).

In the case of the FIMI RC, collective learning can take place at three levels: basic (individual citizens), community (organisations), and strategic (regulations and policies). The natural challenge for the FIMI RC is to integrate

3 A list of the case studies examined is provided in Appendix 3.

these experiences and break siloed thinking and actions of social stakeholders and governmental actors. Siloed action presents a challenge to coordination between state and NGO actors operating under the common roof of the FIMI RC as well as the integration of their lessons learned and their translation into effective action patterns.

Despite organisational diversity, the varied nature of the control mechanism, and the areas of activity, the evaluated organisations are a valuable point of reference for the way the FIMI Resilience Council should operate. They share many similarities and a solid record of good practices, which should be considered when planning a structure focused on counteracting FIMI. They refer, inter alia, to the importance of resilience in a broad sense (as a preventive and regular future-oriented action aimed at systemic stability and survivability), as well as methods and forms of cooperation between stakeholders (regulators and private entities) and their productive interactions.

Bearing in mind the general concept of resilience presented earlier and the lack of a satisfactory detailed and universal definition of this concept, case studies allow us to look at ways of its operationalisation for the purpose and object of organised action of communities consisting of multiple stakeholders. This allows for the identification of recurring practices that can inform our generalisations for the needs of the FIMI RC.

This report is divided into two main parts. In the first, we define the broad context and purpose of our research, which is the pursuit of lessons learned resulting from the organised action of stakeholder communities interested in strengthening systemic resilience in their respective sectors. Next, we briefly characterise international disinformation (FIMI) as a problem for the solution of which we look for through these experiences and the related conceptual apparatus in the activities of the European Union and its Member States.

On this basis, we present conclusions from empirical research and evaluate strengths and weaknesses from the experience of national government, local government, business, and civil society entities involved in strengthening resilience. Subsequently, we formulate, among others, a working general definition of “resilience council” as a reference point for the first FIMI Resilience Council in Poland.

In the second part of the report, we present the assumptions, mission, vision, goals, planned structure, and first conclusions from the process of designing and creating the FIMI RC Poland. So far, the results of work on the Polish FIMI RC are highly promising. In their course, there was a de facto division into two structures operating under the common umbrella of the resilience council. The first of these, with a broader intent, is to advise the Polish Minister of Foreign Affairs in areas such as the state and its institutions, legal regulation, national security, education, and the psychology and sociology of disinformation. The second structure is aimed at supporting the National Digital Services Coordinator in the implementation of the EU Digital Services Act. The authors of this report are convinced of the reference value of this model to be replicated in other EU member states working to fight FIMI and strengthen societal resilience against FIMI-related threats. We also see a prospect for an EU-wide parent structure that will assist national FIMI RCs and improve overall EU resilience policies and actions.

In Appendix 3, we present the case studies examined, which serve as the basis for formulating the conclusions and generalisations presented in this report. Of the more than 100 entities surveyed, 43 entities met the defined criteria for a resilience council. These are presented in the form of a table that contains the name of the entity, its categorization, and a short description of its activities. We hope that the choice made will form the basis for further research into this interesting phenomenon.

The essence of the problem

In modern society, all spheres of life function based on a developed information structure. The security of the state, society, and individuals directly depends on the quality and resilience of national information processes and resources. This concerns not only the criterion of the truthfulness of information as a source of rationality and optimal decision-making but also the way in which the public uses information (Kupiecki, Bryjka, & Chłoń, 2022). Therefore, false information intentionally introduced by foreign actors with the aim of harming societies (disinformation), without the intention of harm (misinformation), or resulting from social interactions and false information codes (malinformation) have the ability to infiltrate public life and cause significant damage. "They provoke conflict, deepen polarisation, perpetuate stereotypes, and undermine general public trust in government" (Svintsytskyj et al., 2023, p. 428).

Resilience to FIMI is multilayered. At the social level, it refers to the ability to recognize, properly evaluate, and respond to information that may be false, misleading, or intentionally harmful (e.g., hate speech).

It includes knowledge-based education that enables individuals to effectively verify information before accepting it as true, as well as critical thinking skills and media literacy.

At the level of political institutions, the fight against disinformation beyond the regulatory efforts of states and the European Union requires the use of multiple and multifaceted actions. These should come from combined strategies involving the efforts of state institutions, information producers, operators of online media platforms, civil society groups, and informed citizens.

Such strategies can be based on multiple sectoral or combined approaches that benefit from synergies between state resources and the expertise and energy of the NGO sector. They should result from multifaceted continuous actions against problems that are repetitive, variable, and, although difficult to predict in detail, can be studied to accumulate knowledge useful in prevention, deterrence, defence, and the repair of damage caused by malicious foreign information activities. Resilience against FIMI-derived threats, rather than being a static objective, should be understood in terms of a strategic approach to evolving threats (Powley, Barker Caza, & Caza, 2020).

Resilience as a concept

Resilience is a useful metaphor that describes many phenomena related to the functioning of individuals and societies (Norris et al., 2008). For this reason, although present in scientific deliberations and public policies since the 1950s, the term does not have a satisfactory and exhaustive definition. It has been defined differently in the literature depending on the subject concerned, the scientific discipline in which the research is carried out, and the author's interest. Nevertheless, attempts are being made to unify this concept (Brand & Jax, 2007).

In general, the concept of resilience refers to a complex system with a principal purpose of protecting against harmful factors present in the environment of a given biological or social organism. The term therefore refers to the integrated operation of all subsystems capable of recognising and combating harmful influences, removing their effects, and restoring the functions of the system. Through learning processes, the concept is also proactive in nature and seeks to anticipate and prevent the emergence of new threats. Areas of consensus between researchers and practitioners on the concept of resilience are illustrated in the box below.

Defining resilience – consensus between researchers and practitioners

Characteristics of resilience as a subject of study:
- a system, community, or society exposed to a threat.

Resilience objectives:
- the ability to resist, absorb, accommodate, and recover from the effects of a threat/crisis in a timely and efficient manner;
- the preservation and restoration of essential basic structures and functions; and
- the ability to learn from experiences to improve future prevention efforts to fight and predict crises.

Effectiveness of resilience:
- A measurable persistence of systemic ability to:
  - » absorb changes and disruptions while retaining the same basic structure and ways of functioning as well as the capacity for self-organisation and adaption to the evolving environment;
  - » mitigate, adapt, and recover from shocks and stresses in a manner that reduces chronic vulnerability and facilitates inclusive growth; and
  - » manage changes and continue to develop.

The standard of resilience of democratic states includes:
- adaptability to changing contexts;
- survivability amidst large and unexpected shocks;
- the ability to recover to a desired state - either the previous one or a new one;
- functional and operational continuity; and
- learning from mistakes and transforming lessons learned into more effective resilience measures.

Source: own work based on existing literature.[4]

In addition to the natural context (i.e., biological immunity understood as the organisms' ability to defend itself against harmful environmental effects), there are concepts in circulation that refer to resilience as:

- **overall systemic resilience** – the ability to survive and maintain equilibrium.
- **organisational resilience** – the ability of an organisation to maintain continuity of operation and adaptation in the face of changes in its environment.
- **mental resilience** – an individual's ability to cope with life's hardships, stress, and other emotional problems.
- **resilience of IT systems** – an uninterrupted operational capability regardless of existing digital threats.
- **ecosystem resilience** – the ability to survive and maintain environmental functions in the face of adverse environmental impacts (e.g., climate change, human activity, or pollution).

4 A useful systematisation of the definition of resilience: Padan, C. and Gal, R., A Multi-Dimensional Matrix for Better Defining and Conceptualizing Resilience, 'Connections: The Quarterly Journal, no. 3 (2020), pp. 33-46, DOI:10.11610/Connections/19.3.02.

All these approaches point to the main characteristics of systemic resilience, which are survival, proactive and reactive protection from threats, adaptation and response to environmental changes, the ability to maintain integrity and function under all circumstances, and the capacity to restore lost functions after damage has occurred.

These general characteristics should be considered crucial, including when considering the resilience of democratic societies and states to hostile foreign information interference (FIMI).

The coherence of democratic societies is a key factor that must be protected from the harmful influences of FIMI. It is the basis of social resilience, which consists of the quality and strength of social bonds based on responsibility, trust, pluralism, and solidarity. Weakening these factors through harmful information hampers cooperation, problem-solving, and crisis response. Societies and states acting on their behalf must therefore develop a synergy of capacities to respond effectively to the dysfunctions of the information sphere. Those capacities encompass:

- **knowledge** – enables the identification of necessary actions for effective anticipation, response, prevention, and adaptation to difficult or crisis situations.
- **skills and competence** – allows for an analytical apparatus that can monitor risks, which leads to an improvement in the accuracy of forecasts and a reduction of uncertainty in the activities of individuals and communities.
- **effective communication** - ensures the growth of synergies and legitimacy of pro-resilience activities.

Knowledge-based resilience is therefore the "first line of defence" of any system against risks and threats undermining its integrity and survival. Competence-based resilience involves the planned, purposeful, and effective use of existing system resources in crisis prevention and response processes.

Third-level resilience requires systematic collection, analysis, and experience sharing, which is subsequently transformed into knowledge and procedures to improve preparations for future crisis situations. At all three levels, simultaneous processes identify objectives, link the available means and actions necessary to achieve them, and coordinate with social expectations. Progress achieved and systemic effects are as much related to real achievements as the ability to remove contradicting expectations. This is done by co-opting experts, coordinating strategies, and engaging the stakeholder community as widely as possible, which, in turn, strengthens trust and ownership.

The above-mentioned resilience-enhancing factors are more effective when they occur in an interconnected manner supported by cooperation and complementary actions of stakeholders. For example, identifying and understanding the nature of threats is a prerequisite for competent threat analysis and assessment, which consequently determines the development of effective crisis response algorithms. These, in turn, seem to be more effective when society understands and approves the course of action. The same informed actors can then be part of the crisis management performance assessment system.

Main attributes of systemic resilience (Survive-Solve Problem-Minimise Impact-Prevent Reoccurrence)	
Resistance	Resilience
Environmental monitoring	Adequate response
Defence against threats	Ability to restore functionality
Understanding of own vulnerabilities	Synergies between stakeholders' community and lessons learned
Recognition of environmental risks	Better knowledge-informed anticipation and prevention

Source: own work.

Resilience against FIMI – the operationalisation challenge

Given the complex nature and continuous evolution of the challenge of strengthening resilience against FIMI, it is not only essential that the concept is clear and up to date but also that it is operationalised into meaningful action. Resilience as a general objective of the organised activities of the state and the NGO sector must be subject to the rigour of understanding as: what should be achieved, how to achieve it, and what criteria should be used to measure progress.

Traditional definitions of resilience tend to associate it with the ability to assess, through qualitative and quantitative methods, a risk and the pace of systemic recovery. However, for the purposes of combating FIMI, this approach is too narrow and relates more to resistance and crisis management than the full spectrum of the resilience-building process, which includes anticipation, prevention, response, rehabilitation, and continuous improvement of systemic capacity. Therefore, the operationalisation of the objectives should be sought through a combination of many types of actions that are educational, analytical, legislative, and implementational. This also includes synergies of stakeholders' community efforts and their continuous expansion of access to key resilience-enhancing skills and capabilities. This involves fostering collaboration among government agencies, NGOs, private sector entities, and community groups, allowing for unity of purpose, shared responsibility, and the efficient use of tangible and intangible resources.

The operationalisation of resilience under such conditions must improve the understanding of the purpose and scope of necessary actions. This is essential in the process of shaping resilience strategies and plans. It must also contain indicators to estimate the effectiveness of their implementation, including the use of resources. Finally, it must shift the burden from responding to crises to continuously improving crisis prevention. The latter requires mobilisation of resources and expertise, which can only be achieved through synergetic action by a stakeholder community in the areas of education (i.e., raising public awareness), analysis (i.e., self-awareness and risk assessment), legislation (i.e., regulation and support) and implementation (i.e., resilience-oriented actions, execution of strategies, and plans).

Resilience councils – inferences from case studies

Just as the concept of resilience has gained significant attention among scholars and

practitioners of security and the development policies of EU member states in recent years, it has been followed by reflection on effective ways to strengthen it at the level of states, local governments, the business sector, and public policies. It has resulted in the creation of numerous organisations focused on this issue, which can be placed under a common conceptual umbrella of resilience councils. These have not been merged into a single globally coordinated structure. The number of sector-specific projects focused on building resilience and implemented in various ownership and organisational forms are numbered in the hundreds. However, they are more numerous in some sectors than in others.

Resilience councils represent an approach to tackling disinformation that is not yet well established. They deserve attention in this context because, as experts state, "A central distinction between authoritarian and democratic systems is their view of information. Democracies believe and depend on the open and free exchange of information that empowers citizens to make informed decisions to select their representatives and engage in political debates" (Rosenberger & Gorman, 2020, p. 1.).

Resilience councils most commonly exist in those sectors that have either experienced or, by nature, are vulnerable to environmental and social threats. The activity of local governments and cities in the sphere of crisis management in the face of threats resulting from climate change, accelerated urbanisation, or derivative civilization challenges demonstrate the above. Similarly, the sphere of public health or sustainable business development are also well represented. These sectors require coordinated and comprehensive strategies to increase resilience, including synergies stemming from resource pooling and collective learning to better anticipate threats, identify trends, and develop effective prevention measures.

In search of common criteria to define resilience councils

Based on the research of case studies presented below, one may be tempted to coin an original general working definition of a resilience council. For the RC FIMI created in Poland, it has a reference value.

Thus, the **resilience council is an interdisciplinary inclusive structure that brings together stakeholders representing different fields of activity: national governments, local governments, business, academia, and civil society around common goals to improve social resilience. It actively works to increase the legitimacy and effectiveness of joint efforts, including by breaking organisational and competence silos; it focuses on threat analysis, knowledge development and exchange, group learning, strategy shaping, and the development of policies and tailored solutions and their effective implementation.**

Positive criteria

A. Commonality of approach

Empirical examples illustrate that the basic criterion distinguishing resilience councils is **their inclusive collaborative nature and operational character** fostered by diverse entities willing and ready to implement shared missions. They are thus examples of a positive and proactive approach to strengthening resilience. Based on the examined case studies, it can be concluded that several factors are common in their activity:

1. A declared awareness of the need for a holistic integrated approach to resilience against threats occurring in statutory areas of engagement that, due to their complexity, require a cross-sectoral, multi-level, and comprehensive response.

2. A willingness to break siloed approaches to threats by facilitating the coordination of resilience-building efforts carried out by entities of different origins and management organisations (i.e., government-business-civil society).

3. A declared awareness of the need for political and social inclusivity regarding the inclusion of non-state actors.

4. A recognition that the process of strengthening resilience is an issue that exceeds the sole responsibility of governments and traditional top-down approaches. This involves understanding the need to increase the effectiveness and legitimacy of responses to threats through the involvement of knowledge and resources of a broader stakeholder community. It also recognizes the importance of integrating state (or local government) objectives with the sensitivity

and competence of civil society structures and the expert community.

5. The decentralisation of responses to threats achieved through community ownership of resilience initiatives. This fosters the development of best practices while strengthening communities.

B. Structural attributes

The case studies examined by the authors show a high convergence of features and properties organising the functioning of individual resilience councils, regardless of their area of operation. This allows us to conclude that these are entities where the similarity of structural attributes increases their legitimacy and effectiveness in the analysis and understanding of threats, the quality of responses, post-crisis rehabilitation, and preventative strengthening of systemic resilience.

Within this framework, the following key structural attributes of resilience councils can be identified:

1. **Clarity of objectives and missions**, which allows for mobilisation of resources, concentration of activities on key tasks, and assessment of their effects. All resilience councils we have examined have publicly available mission statements, definitions of major goals, priority objectives, and outlined plans to achieve them.

2. **An open management model**, which emphasises flexibility of procedures, effective communication within the stakeholder community, and efficient adaptation to emerging challenges and opportunities resulting from changes in the operational environment.

3. **A diverse stakeholder community** that includes multiple perspectives in strategizing and planning. This includes the desire to aggregate and strengthen the credibility of experts and practitioners from various fields of knowledge including the public, non-governmental, academic, and business sectors. For example, this would allow business experts to act within their understanding of the specifics of their sector; academics to provide methodological premises and current scientific knowledge; government representatives to add knowledge about the regulatory environment, public policies, and project financing opportunities; and the social factor to link the activity of the resilience council with the expectations and needs of stakeholder communities.

4. **Prioritisation of actions** and corresponding allocations. In the case of known resilience councils, funding is usually derived from government grants, private sector donations, or income from commercial projects.

5. **Continuity of good practices** of information sharing between participants of the resilience council, which increases the overall competence of a given structure.

6. **Openness to cooperation** with other relevant entities, including through formal methods (i.e., in the form of agreements and memoranda), or other inclusive approaches like traditional conferences, seminars, simulations, gaming, and other networking mechanisms.

7. **Professional development** through certification of qualifications and maintaining a knowledge-enhancing platform.

The most important action-oriented concepts of resilience councils	
Objectives	Means and ways
Enabling	Networking/synergy
Reducing	Education and inclusion
Fostering	Informed advice
Community building	Information sharing
Strengthening	Mutual learning
Anticipating	Methods/analysis, feedback loops, and formulating of testable hypotheses
Preventing	Regulation/implementation
Effectiveness	Breaking competency silos

Source: own work.

C. General criteria of utility (added value)

Existing resilience councils generate added value for public policies and civil society through the above-mentioned structural and functional attributes. This involves continuous improvement in the performance of a community of stakeholders in preparation and coordination of crisis activities, structured analysis and social education, institutional synergy, and resource management. This is due to the operational model of such structures, which emphasises adaptive, bottom-up, collaborative, and inherently inclusive approaches.

Key value-added criteria in this area relate to:

1. Regular knowledge exchange and cross-sectoral communication processes that contribute to an increased understanding of the nature of resilience-threatening problems and increased synergy and legitimacy of stakeholders' community activities.

2. Democratisation, integration, increased transparency, flexibility, financial efficiency, and creativity of resilience-enhancing processes through close cooperation between government, business, and NGO actors. The latter increases ownership and responsibility for the activities carried out. The governmental factor, in turn, improves the quality of public policies, broadening their information base and credibility while reducing costs and litigation risks.

3. Integrating knowledge and increasing opportunities for social education, which results in increased public awareness of threats and pro-resilience attitudes.

4. Provision of incentives for the responsible use of modern technologies to detect and reduce vulnerabilities.

5. A comprehensive approach to the problem of resilience and efforts to replicate good practices. By disseminating knowledge, resilience councils create opportunities for the universalization of good practices and their adaptation to the needs of specific sectors.

6. Political and regulatory support for social initiatives aimed at strengthening resilience. This increases the quality and legitimacy of regulation while correlating with social expectations.

Figure 1 Resilience Councils - added value. Source: own work.

Negative criteria and risk factors

The key to the effectiveness of resilience councils is both active and continuous stakeholder contributions to its overall mission and agenda ("Guidance for Stakeholder Engagement", 2019). In return, these stakeholders are given access to pooled resources that help them in their respective resilience-oriented activities while also increasing the resilience of the system as a whole. The basis of this engagement is the belief that sectoral, systemic, and operational resilience is a common interest and form of public good that will benefit all stakeholders.

While resilience councils bring added value in strengthening social and systemic resilience, two areas of concern for their effectiveness should also be noted:

A. the multiplicity of leadership and management patterns of such entities, and

B. the structural problems associated with their activities.

The first area has a relatively neutral impact on their effectiveness. The second one, on the other hand, involves many specific risk factors that could detract from the positive impact of resilience councils.

A. Leadership and management models

In an organisational sense, resilience councils can be both inclusive networks of organisations and forums that bring together state institutions, civil society actors, and businesses to strengthen resilience in areas of public life. Each management option, however, is characterised by a commonality of participants' objectives, a wide range of stakeholders, and parallel connectivity between governments

and businesses. Resilience councils serve as platforms for the exchange of information, best practices, and initiatives related to risk prevention, crisis preparedness and management, and group learning to strengthen resilience. Therefore, the leadership model should be considered a neutral/negative factor in examining resilience councils.

A1. Resilience council as a governmental structure

Comparative advantages associated with running a resilience council by government structures are associated primarily with access to decision-makers, potential formalisation of the council's activities, and access to relatively unlimited resources. Giving it a legal mandate promotes the formal definition of its powers and responsibilities and allows for inter-agency coordination, as well as the integration of resilience measures into other public policies. The state organiser of such activities may licence the involvement of experts and representatives of non-governmental sectors and the extent of their influence on the operation of the common structure. For its needs, the government can also mobilise the necessary financial and material resources, as well as integrated planning processes. However, this leadership model risks bureaucratisation, slow decision-making, "heavy" reporting requirements, and the impact of changing political priorities stemming from domestic and external pressure.

A2. Resilience council as a mixed structure

The mixed model of organisation and management of resilience councils is arguably the optimal form for such structures. Beyond the organisation itself and its decision-making structure, this also applies to the interaction of stakeholders in crafting an agenda of joint action. It combines strengths and compensates for individual weaknesses in the planning of the resilience council's strategy. It is linked to the strength of government structures and the legitimacy and flexibility of non-governmental sectors. This type of management model can successfully integrate diverse points of view, increasing the inclusiveness of decision-making processes and resulting in greater legitimacy.

Government funding, in turn, can unleash the energy and systematic use of the competence and innovation of social actors. Such structures, due to the decentralisation of the decision-making process and the reduction of bureaucracy, have the potential to be more adaptable than those managed centrally by the government. The primary risk factors for mixed resilience councils stem from a possible complexity of the processes involved in coordinating and agreeing on objectives of action, as well as the uneven distribution of resources. However, these risks can be mitigated by careful planning and effective communication within the stakeholder community.

A3. Resilience council as a non-governmental structure

A common case among working resilience councils is that they are run by non-governmental actors (e.g., business, local authorities, academia). They rely on the strength and funding of their participants while drawing on the inspiration and grant programmes offered by governments and international organisations. The source of their effectiveness is the minimization of bureaucracy and a narrower focus than those of governmental or mixed structures. Their leadership model is also associated with greater trust between participants who work to address issues of genuine concern and urgency. On the other hand, risk factors of this model include uncertainty of financing, potential collision with government policies, and the narrow legitimacy of actions taken that are "invisible" for the wider community.

B. Structural problems related to the activities of resilience councils

Resilience councils face several structural challenges. They concern problems with effective management, overcoming differences resulting from the varied organisational

cultures of stakeholders, limited availability of funds (which increases competition in this respect), and long-term maintenance of a consistent mission and the quality of activities undertaken.

For entities as complex as resilience councils, there is a potential for differences in strategic priorities and operational goals between stakeholders, which raises the risk of internal conflicts and decreased trust. The latter may also result from difficulties in integrating experiences, knowledge, and work cultures of stakeholders representing different sectors (e.g., continuity disruptions or differences in priorities of governments, businesses, and NGOs), as well as unequal representation in organisational management processes. This also affects the credibility of mechanisms for monitoring and improving the effectiveness of activities, as well as the ability to effectively communicate the mission of the organisation.

Why the state should be involved in the FIMI RC

FIMI poses a serious threat to social cohesion, public order, and the democratic processes of European Union Member States. Therefore, preventing and countering its impact is a key component of building the resilience of a community of democratic states. A FIMI Resilience Council that incorporates a wide spectrum of stakeholders can contribute to reducing related problems. This is an appropriate response to the recommendations contained in the EU's policies relating to a comprehensive approach that call for cooperation between governmental, business, and civic actors. This is demonstrated by the experience of many similar entities operating in multiple sectors of public life.

They suggest general tasks for the FIMI RC, including:

- strengthening national capacities to respond to the spread of foreign disinformation, including through joint multi-sectoral efforts by stakeholders;
- linking closer government security policies with the involvement of competences and expertise present among the NGO and business sectors;
- conducting research and analysis to identify harmful activities (i.e., TTPs) affecting social media and mapping sources and measuring the impact of disinformation;
- raising awareness through research and education that strengthens social resilience, media literacy, and critical thinking skills;
- contribution to policies protecting open democratic societies from targeted foreign disinformation campaigns that undermine public trust in free institutions, increase polarisation, and produce other harmful social consequences;
- cooperation of the NGO sector with government institutions to address systemic regulatory efforts aimed at combating FIMI in all its manifestations while protecting the free market and freedom of speech; and
- regular dialogue, education, and exchange of information with stakeholders.

The FIMI RC under construction in Poland will largely be a "defender community" organisation that operates under the umbrella of government institutions that are aware of the challenges of disinformation and the benefits of synergies provided by cooperation with the private sector and civil society. The authors see five key advantages of this structure, which will benefit from the government's ability to leverage its unique capabilities and responsibilities to create a comprehensive, trusted, and effective approach to strengthening resilience:

1. The activities of the FIMI RC will enhance the relevance of national security policy, including prevention, detection, and response to disinformation threats. At the same time, these activities will

gain stronger social legitimacy as the result of multi-stakeholder involvement.

2. Long-term resource allocation and regulatory activities will gain significant consultative potential, which may result in increased public trust.

3. The government will gain stronger support in crisis management, which requires rapid response and a broad social basis and reliance on competences and resources.

4. Access to knowledge, support for research, and the consolidation of information exchange practices will be democratised. This can be an important factor in increasing public awareness for more responsible public behaviour in the information sphere and strengthening democratic integrity.

5. The government will enhance its health security to give citizens access to reliable health information, which experience from the COVID-19 pandemic demonstrated is an issue of critical importance. This requires not only tackling disinformation in this area but also exploiting synergies with social organisations.

The list of areas in which resilience councils and related organisations operate is very rich. The categories of activities include: agricultural and food resilience, climate and environmental resilience, financial and economic resilience, global systemic resilience, health resilience, resilience of cities, resilience of infrastructure and transport systems, resilience through crisis management, and technological and cyber resilience.

In examining the case studies within these areas, it has become increasingly evident that a common and adaptable model for initiating and conducting cooperation intentionally oriented towards social resilience exists. There is therefore no reason why their experience should not be considered relevant for organised activities to prevent and combat FIMI-related risks and threats.

Figure 2 Resilience Councils: Lessons for FIMI RC Best Practices. Source: own work.

Part B

Creation of the FIMI Resilience Council

The process

SAUFEX began the process of establishing the FIMI Resilience Council (FIMI RC), guided by the following key principles:

1. Civil society councils are generally more effective if they are formally empowered and accredited as advisory-consultative bodies of legislative or executive bodies. This is also the objective pursued by SAUFEX. At the same time, the quality of the work and the usefulness of the councils are a function of the competence of its members.

2. The proposed FIMI RC should bring together representatives of organisations who are experts in areas such as the state and its institutions, legal regulation, national security, education, psychology, and the sociology of disinformation. Membership in the council therefore requires specific expertise.

3. This knowledge should also be based on lifelong learning. To this end, SAUFEX will create a European Master of Countering Disinformation (EMoD) as part of the project.

4. A reference point for the conceptual and organisational work of the council will be the provisions of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).

5. The resilience council will also require a minimum representation of 50% of women.

This project envisioned the development of the council's competences using simulations and tests carried out by consortium members at universities. This assumption has been verified. Such simulations could be carried out through real interactions on an ongoing basis between the government administration and third sector entities, namely the Ministry of Foreign Affairs and a wide range of NGOs involved in counteracting FIMI.

At the same time, SAUFEX has been involved in key consultation and legislative processes related to the implementation of the Digital Services Act: first, in the context of public consultations of the legislative draft, and second, in the context of inter-ministerial consultations of the draft law. Both paths are interrelated. The work was also guided by the results of initiatives and projects launched prior to the formal start of SAUFEX, including in the Polish Senate. On March 31, 2023 (after this grant application had already been submitted), a seminar of three commissions was held: Culture and Media; Human Rights, the Rule of Law, and Petitions; and Foreign and European Union Affairs. The discussion was based on the report "Tackling Disinformation in Poland. Systemic Recommendations" prepared by 40 experts, including researchers belonging to the SAUFEX consortium. During the session, a declaration on countering disinformation in Poland was adopted. The senators called on all political forces to endeavour to build the broadest possible consensus to fight disinformation, particularly in the face of the ongoing crisis of public trust in Poland and the war in Ukraine.

The declaration emphasised that disinformation has a negative impact on the security of citizens. To counter this threat to the democratic state and its institutions, systemic solutions are needed with the support of civil society and its involvement in the efforts of state institutions. The state's strategy for

dealing with this threat should cover such areas of public life as: education, media, security policy, civil society support, and legislation. It called for the urgent implementation of the European Union's Digital Services Act.

Public consultation

The implementation of the Digital Services Act is being coordinated by the **Ministry of Digital Affairs, which is responsible for ensuring the effective application of the provisions of this regulation into the Polish legal system** by amending the Act of July 18, 2002, on the Provision of Electronic Services (Journal of Laws of 2002, No. Journal of Laws 2020, item 344) and the Telecommunications Law Act of July 16, 2004 (Journal of Laws 2022, item 1648), as well as amending the relevant sectoral legislation.

During public consultations in January 2024, the presented assumptions of the draft act amending the Act on the Provision of Electronic Services and other acts in implementing the Digital Services Act drew attention, inter alia, to the following issues:

1. The regulation will become directly applicable and each Member State is required to ensure its effective application in its legal order by adopting appropriate internal provisions. The Digital Services Act provides for designation at the national level of a body that will act as a coordinator for digital services (i.e., a regulator responsible for compliance with the provisions of the regulation in Poland).

2. The legislative actions taken assumed that the amendment will concern only provisions that have been directly submitted by the EU legislator for regulation in national law or those in which the Digital Services Act has left regulatory freedom to the Member States. The following issues, which are reflected in the draft law, therefore need to be regulated by national law:

   a. institutional provisions on the appointment of the Digital Services Coordinator (President of the Office of Electronic Communications - OEC) and the competent authorities (President of the OEC, President of the Office of Competition and Consumer Protection), as well as the definition of their scope of competence.

   b. rules of procedure for authorities and cooperation between authorities, including those related to:

      i. conducting investigations, inspections, and proceedings related to a breach by providers of intermediary services of obligations under the regulation. The draft act provides for a uniform procedure for conducting proceedings for a breach of the provisions of the regulation and inspections, regardless of which authority conducts it.

      ii. procedural aspects for the imposition of penalties (with the maximum threshold for penalties being assigned based on Article 52 of the regulation).

      iii. procedural aspects for lodging complaints against providers of intermediary services (referred to in Article 53 of the regulation).

   c. issues requiring the establishment of procedures, considering the requirements and conditions set out in the regulation (i.e., the procedure that should be followed by the Digital Services Coordinator):

      i. granting the status of "vetted researcher" referred to in Article 8 of the regulation. The role of the vetted researcher is to carry out specific research based on the data processed by a specific provider of intermediary services. The status of a vetted researcher depends on

the fulfilment of certain conditions and is granted by the coordinator, which offers the provider confidence that its data will be shared with appropriate security rules.

ii. granting the status of "trusted flaggers" referred to in Article 22 of the regulation. These are independent entities whose notifications of content deemed illegal by providers of intermediary services are to be treated as a matter of priority by the providers.

iii. certification of out-of-court dispute resolution bodies.

d. the requirements for orders to act against illegal content or provide information issued by administrative authorities or courts based on EU or national law and in line with the requirements of the Digital Services Act.

e. rules on civil liability and proceedings before the courts in the event of a claim for damages for breach of the provisions of the regulation.

Of these, SAUFEX considered the following issues:

Certification of out-of-court dispute resolution entities

The Digital Services Act provides for Member States to engage in good faith in the out-of-court resolution of such disputes, including disputes that could not be satisfactorily resolved through internal complaint-handling systems. This should be done through certified bodies that have the necessary independence, means, and expertise to carry out their activities in a fair, timely, and cost-effective manner. The independence of out-of-court dispute settlement bodies should also be ensured at the level of natural persons in charge of dispute resolution, including through rules on conflicts of interest.

The vetted researcher

The draft law also provides for the procedure of granting the status of vetted researcher. Before granting the status of vetted researcher, the President of the OEC shall consult the authorities competent in matters related to the subject area represented by the entity applying for status.

Trusted flagger status

The Digital Services Act provides for the establishment of trusted flaggers that operate in designated areas where they have expertise. Through reporting and action mechanisms required under the regulation, they are expected to operate without prejudice and decide on all reports made under those mechanisms in a timely, diligent, and non-arbitrary manner. According to the regulation, the status of trusted flagger should be granted by the Digital Services Coordinator of the Member State where the applicant is established; this status should be recognised by all providers of online platforms falling within the scope of this regulation. Trusted flagger status should only be granted to entities who have demonstrated, inter alia, that they have specific expertise and competence in tackling illegal content and that they act in an accurate, objective, and diligent manner.

Before granting the status of trusted flagger, the President of the OEC shall consult the authorities competent in matters related to the subject areas represented by the entity applying for status. The provisions are constructed by analogy with the provisions on certification and with regard to the form of cooperation set out in Article 106 of the Code of Administrative Procedure. When determining the authority to request an opinion, the President of the OEC should be guided by their location in the Polish legal system and their expertise and experience, ensuring the possibility of adequate assessment of designated entities operating in a given sector. It should be emphasised that due to the critical nature of trusted flaggers' activities, the

President of the OEC will be obliged to consult the President of the Office for Personal Data Protection.

Opinion of SAUFEX

During public consultations, SAUFEX prepared an opinion on the complexity of the matters regulated by the act and challenges related to its implementation. Overcoming these challenges will require broad inclusion of third sector organisations and experts in view of: the necessary independence and expertise; competence to tackle illegal content; objectivity and diligence; transparency of procedures; and severity of penalties. As part of the consultations, the SAUFEX project coordinator submitted a paper entitled: "The Disinformation Resilience Council as the Social Consultative and Advisory Body of the Coordinator of Digital Services." The paper discussed, inter alia:

General assumptions

To better protect democratic processes in the EU from FIMI threats, while preserving the fundamental rights and freedoms underpinning them, as well as broadening the legitimacy and social underpinnings of prevention, regulation, and education, we propose the establishment of the FIMI Resilience Council (RC) as the social consultative and advisory body of the Digital Services Coordinator. Relevant provisions in this regard could be included in the proposed legislative amendments.

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) is a specific legal constitution to fight illegal content online, including disinformation. To achieve the objectives of the act, legislators envisaged the use of independent civil society organisations involving researchers, auditors, and experts. They could serve to ensure a safe and trustworthy online environment; assess risks and proactively anticipate and prevent them; and reactively counter the dissemination of illegal content online. These organisations could also contribute to voluntary codes of conduct. The FIMI RC could serve as a platform for their cooperation in these areas.

At the same time, synergies between public and non-governmental competences could be strengthened by establishing and accrediting the FIMI RC as a social body to assist legislative and executive authorities, first and foremost being the Digital Services Coordinator. The RC would gather experts and knowledge in various areas of the fight against disinformation, such as the state and its institutions, legal regulations, national security, media and the information space, education, psychology, and sociology. Participation in the work of the RC would therefore require expertise that would be integrated into the activities of state institutions.

The RC would advise the national Digital Services Coordinator in all related fields, using specialised tools, protocols, and knowledge to coordinate strategic and policy responses to disinformation threats, as well as to promote uniform solutions across the EU and improve internal coordination within the EU.

Objectives

The main objective of the establishment of the RC would thus be to decentralise and democratise processes related to proactively and reactively countering FIMI incidents and campaigns. It would also facilitate the implementation of the DSA in close coordination with relevant state actors. The council, representing a wide range of relevant civil-society-based organisations and experts who are experienced in collaborating with the legislative and executive authorities in Poland and internationally, could play an important role.

Functions

As part of a broad consultative and advisory mission, the following RC functions would also be possible:

- **An educational function** that would develop training materials for institutions and individuals involved in the implementation and operation of the act at the administrative and civil society level. This knowledge should be based on a specialised model of education and training, as reflected in the textbooks and educational materials prepared for this purpose. Academic research in this framework would also serve general social education on the use of digital media. In addition, the council would support efforts to identify obstacles faced by EU members in coordinating and strengthening national approaches and responses to relevant threats. Knowledge and expertise within the council could also lay the foundation for specialised curricula and courses (e.g., the European Masters of Disinformation - EMoD) for practitioners and officials at various levels, including the central, regional, and local level. Successful completion of the master's course could be mandated for council members.

- **A testing role** to verify the effectiveness of algorithmic protocols that describe and share knowledge about FIMI attacks and operations in real-time, allowing for swifter response and mitigation. This could have a significant impact on the resilience of democratic societies as well as the development of new products and services that aim to detect and counter disinformation and hybrid attacks. Council instruments supported by activist, expert, and media communities in all related domains could include existing specialised databases such as DISARM, STIX 2.1, EUvsDisinfo, and various Open CTI formats. At the same time, these databases could be extended to include data on national disinformation. They could also categorise offences and offenders according to the level of harm and consequences.

- **A depositary role.** It would be the responsibility of the council to gather feedback from civil society and private stakeholders to gain insight into society's perception of hybrid threats, including the potential role of artificial intelligence in combating them, and provide strategic communication advice. The involvement of civil society in this process will contribute to an improved space for solutions, ensuring that the proposed solutions are relevant, effective, and transparent while increasing civic resilience.

- **An intermediary function.** The RC's position between national actors could facilitate the standardisation of efforts to counter online threats, including through the establishment of partnerships and cooperation, for example, with EU-HYBNET to counter hybrid threats.

Effects

The direct effects of the work of the RC, together with general political, social, and educational effects (resulting in e.g., diminished affective polarization), would be:

- **Early detection and a coordinated response.** By contributing to early identification and coordinated dissemination and response to network threats, the RC would support efforts to minimise the impact of these threats and reduce the cost of corrective actions. This would include identifying and neutralising disinformation campaigns before they become popular and detecting and mitigating cyberattacks before they cause significant harm.

- **Undermining perpetrators' business models.** The RC would contribute to increasing the costs of operations for entities disseminating disinformation or illegal content.

- **Anticipating and preventing impactful FIMI incidents and campaigns.** The RC would formulate hypotheses on what FIMI to expect next as a form of prebunking.

- **Reduced reputational damage**. The risks of disinformation and illegal content can damage the reputations of public institutions, government agencies, and other institutions, which can be costly to repair. The RC can help minimise reputational damage and reduce the costs associated with rebuilding trust and credibility.

- **Better use of resources.** The RC can help ensure that resources are used efficiently and effectively to address relevant threats. By strengthening social and governmental responses, the council can help avoid duplication of efforts and ensure that resources are allocated to specific risks. To ensure maximum independence from national authorities, the work of the RC could be financed by EU funds and self-financing.

Methodology for the establishment of the FIMI Resilience Council

Based on simulations and academic tests, the establishment of a resilience council, at least half of which would be women, would result from:

- establishing criteria for participation based on knowledge and experience, including international experience;
- launching inclusive invitations to civil society organisations as well as academic, research, and media centres to select candidates based on specific criteria;
- training of nominated candidates and members related to the Digital Services Act; and
- a recruitment exam.

Summary

Decentralisation and democratisation processes for analysing and responding to online threats, including FIMI and illegal content, can offer significant societal benefits. By allowing for greater transparency and participation of civil society, these processes could lead to more informed decision-making and ultimately improve the resilience of democratic processes and institutions to hostile actions by foreign, state, and non-state actors. The establishment of the FIMI Resilience Council, anchored in the civic community, will strengthen the overall awareness and resistance of the state and society. **Through the possibility of direct EU support and self-financing through public-private partnerships, the council could become maximally immune to changing political will or the budgetary discretion of governments.** This model has the potential to transform the fight against FIMI from top-down to a peer-to-peer (if not bottom-up) approach, which could lead to a unique ecosystem for countering disinformation and other hybrid threats in the digital environment.

Interagency consultation

Following public consultation, the draft amendments to the Act on the Provision of Electronic Services and other relevant acts were submitted for interagency (interministerial) consultation. The Ministry of Foreign Affairs communicated its position referring to SAUFEX's contribution. The ministry noted that during the public consultation conducted from January 5, 2024 to January 19, 2024, several entities requested the establishment of a social advisory body that will act under the Digital Services Coordinator.

The Ministry of Foreign Affairs, sharing the views of social actors, proposed the creation

of a consultative and advisory body for the Digital Services Coordinator. This body would, at its own initiative or at the request of the coordinator, prepare and present positions on combating illegal content and countering FIMI in the digital information environment. Proposed areas of involvement include:

1. the certification of entities for out-of-court dispute resolution,
2. the status of a trusted flagger,
3. the status of a verified researcher,
4. liability of providers of intermediary services,
5. civil liability and proceedings before the courts,
6. complaints against providers of intermediary services, and
7. other matters referred by the Digital Services Coordinator.

According to the MFA, the council could include representatives of organisations registered in the National Court Register as well as universities, research centres, the media, and other entities (appointed by the Digital Services Coordinator) that work to counter the spread of illegal content, disinformation, and FIMI in the digital information environment.

The position of the Ministry of Foreign Affairs has been considered by the Ministry of Digital Affairs, which is the coordinator of the statutory work. It proposed the following wording be included in the draft act:

1. The President of the Office of Electronic Communications is advised by the Council for Digital Services, hereinafter referred to as "the Council".

2. The Council is a permanent advisory body to the President of the OEC on matters related to ensuring the safe, predictable, and trustworthy functioning of the digital services market.

3. The tasks of the Council shall include, in particular:
   a. making proposals to improve the functioning of out-of-court dispute settlement bodies and trusted flaggers and access to data for vetted researchers;
   b. expressing an opinion on the enforcement of the obligations of providers of intermediary services under Regulation 2022/2065 by competent authorities;
   c. expressing opinions on other matters related to the functioning of the market for intermediary services.

4. The Council is composed of representatives of non-judicial dispute resolution bodies, trusted entities, and media involved in exposing foreign disinformation campaigns through journalistic investigations. The procedure for appointing members of the Council and the rules for its organisation could be laid down in a separate regulation.

Because of these draft provisions and the political will to enact them, as well as the resulting increased potential for even more inclusive participation of the third sector, SAUFEX proposed the appointment of a second council under the Minister of Foreign Affairs. While the first would advise the Digital Services Coordinator on the implementation of the Digital Services Act, the second council under the foreign minister would work on cross-cutting issues such as strategies, policies, stratcom, info ops, legal solutions, institutions, and general media education to counter FIMI and disinformation.

At the same time, the Ministry of Foreign Affairs has been strengthening strategic communication and countering disinformation team. The Minister has appointed his Plenipotentiary on Countering Foreign Disinformation. The Ministry has also reinvigorated cross-institutional coordination to counter foreign FIMI and disinformation campaigns. A dedicated MFA's Department for Strategic Communications and Countering Foreign Disinformation was established in August 2024.

FIMI Resilience Council of the Minister of Foreign Affairs

The creation of a FIMI Resilience Council under the Minister of Foreign Affairs is possible in Poland due to the ability of a member of the Council of Ministers, when implementing policy established by the Council of Ministers and after notifying the Prime Minister (information should be forwarded to the Chancellery of the Prime Minister before the entry into force of an executive order), to appoint (on the basis of Article 7(4) point. 5 of the Act on the Council of Ministers) councils and panels as subsidiary bodies in matters falling within its scope of activity. The composition of the body should be consistent with its departmental nature. This means that the members of the boards should not be representatives of other ministries or units supervised by another minister.

If it is preferable for such a board to be composed of representatives of external entities (e.g., NGOs), in which case the board may be formulated by invitation rather than appointment, but the details may be refined accordingly.

The scope of the appointing order should specify all the tasks of the council, which should be defined as precisely as possible and indicate the result to be achieved (e.g., preparation of a recommendation or report). It should also specify the tasks to be carried out by the entity concerned and its intended composition.

Based on a law that stipulates that the Council of Ministers may set up an advisory committee attached to a minister and define the scope of his tasks, it is also possible to set up an auxiliary body attached to the minister. However, this formula has not been used in the Ministry of Foreign Affairs thus far, and the procedure would be much longer than in the case of an internal order.

To summarize, the appointment of a council attached to the minister requires the issuance of an order and formal notification of this fact to the Prime Minister's office. The regulation should specify how the members are appointed or invited and, above all, the specific tasks or purpose of the board. As a result of SAUFEX's activities, a draft order has been created, which is attached to this report.

Simulations of the work of the FIMI Resilience Council

The assumptions for the establishment of the board and the draft regulation were also the subject of seminars on countering disinformation with NGOs, think tanks, and the media at the Ministry of Foreign Affairs on June 5, 2024, and July 19, 2024 (a list of institutional participants is attached).

The Plenipotentiary of the Minister of Foreign Affairs for Countering International Disinformation presented the activities and initiatives taken by the Ministry of Foreign Affairs in the country and within the international arena, as well as potential common areas of cooperation to combat disinformation. These include:

- strengthening the team for strategic communication and counteracting FIMI and disinformation in the MFA, including the appointment of the plenipotentiary and establishment of a dedicated department.
- inter-ministerial coordination, including through the Information Exchange Group and the team for cybersecurity.
- The decisions of the Council of the EU on the creation of a Rapid Response Team to Hybrid Threats.
- the plans of the Polish Presidency in the Council of the EU, including the creation of a Resilience Council at the EU level, support for the AU, tightening the sanctions system, strengthening cooperation with civil society, and effective implementation of the Digital Services Act.
- cooperation within the EU, NATO, and formats of the Weimar Triangle (i.e., France, Germany, and Poland) the Lublin Triangle (i.e., Lithuania, Poland, and

Ukraine), and Polish-American cooperation under the Ukraine Communication Group.
- the creation of an advisory body to the Digital Services Coordinator.

During the meeting, participants also raised the following issues:

- Polish society is not currently immune to disinformation, and state institutions do not yet have the skills to fight disinformation.
- countering disinformation should take place in parallel on many levels, with the involvement of different ministries, including the Ministry of Education.
- the need to support NGOs and create an appropriate communication channel.
- the necessity of avoiding blanket censorship, which carries the risk of censoring legitimate content.
- the need to create an inter-ministerial strategy (education is not a task for the MFA, but rather the MEN, MPS) and an inter-ministerial body.

In addition to those issues, participants asked the following questions:

- Is the Ministry of Foreign Affairs evaluating this problem strategically in relation to the long-, medium-, and short-term?
- Is the Ministry of Foreign Affairs examining what specifically affects Poles?
- Will the Ministry of Foreign Affairs be the centre of counteracting FIMI in Poland?
- Does the Ministry of Foreign Affairs plan to create contact points for the media?
- What form will the Ministry of Foreign Affairs' participation in the work on the Digital Services Act take and when will a coordinator be appointed?

The seminars created an opportunity to exchange views and promote further cooperation between governmental actors, the media, think tanks, universities, NGOs, and civil society in countering FIMI. The invited participants expressed their willingness to continue collaboration and were encouraged to take part in the MFA Public Diplomacy Grant bids.

Conclusion

During the first six months of the project, SAUFEX:

- participated in public consultation on the implementation of the Digital Services Act; SAUFEX's contribution was noted and published in the post-consultation compendium.

- was instrumental in inter-ministerial consultations on this matter, prompting the Ministry of Foreign Affairs to propose the appointment of an expert council to advise the national coordinator for digital services; the MFA's application was included in the draft statutory provisions.

- initiated the establishment of a consultative and advisory board to the Minister of Foreign Affairs; a draft executive order has been drawn up in the Ministry of Foreign Affairs, and the ministry has conducted a series of meetings simulating the work of the new body.

Epilogue

As a defining element of resilience councils, the term "resilience" can be generally defined as "the ability to cope with shocks and keep functioning in much the same kind of way. It is a measure of how much an ecosystem, a business, a society can change before it crosses a tipping point into some other kind of state that it then tends to stay in" (Walker, 2020).

In the SAUFEX project, resilience is taken as a systemic quality. It is both seen as the amount of elasticity a system possesses and as a mechanism to keep the system from overstretching and reaching its tipping point. Resilience is about both trying to prevent the system from reaching a critical point while at the same time making the system more shockproof.

In this document, resilience refers mostly to defending the system: anticipating, preventing, detecting, and evaluating FIMI incidents and campaigns; combating and removing its effects; and restoring the system. In this epilogue, the authors also formulate a first draft of how to conceptualise the second aspect of resilience, which will be further elaborated throughout the project. But first, it needs to be clear what "the system" is that is defending itself against FIMI by utilising the model of a resilience council.

It might seem obvious to designate the information ecosystem ("infosphere") as the system that counteracts FIMI. This would nicely align with SAUFEX's focus on the DSA, although the DSA mainly focuses on the sphere of very large online platforms and search systems. Beyond the main objectives of the DSA, the information system consists of other online information systems such as hosting services, traditional media (offline and online), private information exchanges, and governmental information services.

Although taking the infosphere as the system seems a logical starting point, it is doubtful whether trying to keep the infosphere functioning should be a goal in itself. Perhaps a well-functioning infosphere is a precondition for another larger system to not be shoved over a cliff?

The European Commission states: "Disinformation erodes trust in institutions and in digital and traditional media and harms our democracies by hampering the ability of citizens to take informed decisions" (European Commission, 2018b). This implies that, in addition to the sphere of digital and traditional media, "institutions" and "our democracy" could also be harmed. Elsewhere, it specifies the potential victims of that harm as: "democratic processes as well as /.../ public goods such as Union citizens' health, environment, or security" (European Commission, 2018a). The system now seems to encompass media, institutions, democratic processes, and public goods. The frame to protect all these elements from the perspective of the European Commission seems to be the democratic European state.

If the state is indeed to be the systemic frame for resiliency, a temptation might occur for the state to rate its own survival above all other goals. It could start prioritising the defence of its institutions and processes as the highest goal and forget what its ultimate task is: serving its citizens through democratic governance.

This is the trap of "undemocratic liberalism" as described by Yasha Mounk (2018). The democratic state rather seems an element in the "keep functioning" aspect of resilience's definition. Instead, society is the system. This is why resilience councils are first and foremost representatives of civil society.

When taking inspiration from the field of prophylactics, and especially from the work of Bruce Alexander, it can be asserted that

people need a few preconditions to minimally function, a state that Alexander (2008) refers to as "getting by". The tipping point for not being able to get by anymore is, according to him, a state of dislocation: "[a]n enduring lack of psychosocial integration". Psychosocial integration, in turn, "reconciles people's vital needs for social belonging with their equally vital needs for individual autonomy and achievement. Psychosocial integration is as much an inward experience of identity and meaning as a set of outward relationships" (Alexander, 2008). Alexander asserts that an experience of dislocation is "excruciatingly painful" to such an extent that it becomes logical for those experiencing it to choose an alternative lifestyle.

Many social psychologists, such as Van der Kolk (2014), add a fourth basic human need to the three mentioned by Alexander: safety. The tipping point for people to cease functioning in society therefore is when their four basic needs - belonging, autonomy, achievement, and safety – are unattainable. When the four basic needs are out of reach for a prolonged time, individuals will turn away from democratic society and choose an alternative path. In that situation, they will "become susceptible to the lure of pills, gang leaders, extremist religions, or violent political movements – anybody and anything that promises relief" (Van der Kolk, 2014).

Taking all the elements mentioned above together, resilience in the SAUFEX project implies a focus on both (a) defending society against FIMI incidents and campaigns that try to undermine people's experiences of belonging, autonomy, achievement, and safety and (b) actively supporting people's positive experiences of belonging, autonomy, achievement, and safety.

The experience of belonging can be undermined by increasing polarisation and alienation. The experience of autonomy can be undermined by empowering an experience of learned helplessness, a state in which we unjustly feel we have no agency. The experience of achievement can be undermined by promoting relativism and nihilism. The experience of safety can be undermined by highlighting real or imagined threats to our physical and psychological health without providing solutions.

Resilience councils in the SAUFEX project are therefore to be vigilant against foreign activities that aim to promote polarisation, alienation, learned helplessness, relativism, and nihilism. They will work to address threats to our physical and psychological health while at the same time supporting citizens' psychosocial integration to avoid the tipping point of large segments of citizens turning their backs on democracy and choosing non-democratic alternatives.

References

Adler, E., & Drieschova, A. (2021) "The epistemological challenge of truth subversion to the liberal international order," *International Organization,* 75(2), pp. 359-386.

Alexander, B. (2008). *The Globalisation of Addiction: A Study in Poverty of the Spirit.* Oxford University Press.

Brand, F. S., & Jax, K. (2007). "Focusing on the Meanings of Resilience: Resilience as a Descriptive Concept and a Boundary Object," *Ecology and Society*, 12(1).

Brandt, J. (2022). "Autocratic Approaches to Information Manipulation: A Comparative Case Study," The Brookings Institution. https://docs.aiddata.org/ad4/pdfs/gf1_06_Autocratic_Approaches_to_Information_Manipulation.pdf (Accessed July 4, 2024).

European Commission (2018a). "Action Plan Against Disinformation." https://www.eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf (Accessed August 14, 2012).

European Commission (2022) "Strengthened Code of Practice on Disinformation." https://op.europa.eu/en/publication-detail/-/publication/c1c55f26-063e-11ed-acce-01aa75ed71a1/language-en (Accessed July 8, 2024).

European Commission (2018b). "Tackling Online Disinformation: A European Approach." https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236 (Accessed August 14, 2024).

European External Action Service (2017). Joint Communication to the European Parliament and the Council: A Strategic Approach to Resilience in the EU's External Action. https://www.eeas.europa.eu/sites/default/files/join_2017_21_f1_communication_from_commission_to_inst_en_v7_p1_916039.pdf (Accessed June 6, 2024).

European External Action Service (2022). 2022 "Report on EEAS Activities to Counter FIMI." https://www.eeas.europa.eu/eeas/2022-report-eeas-activities-counter-fimi_en (Accessed June 9, 2024).

European External Action Service (2024). "2nd EEAS Report on Foreign Information Manipulation and Interference Threats." https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en (Accessed June 10, 2024).

European Parliament and Council of the European Union (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), *Official Journal of the European Union*, 27.10.2022. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065 (Accessed June 3, 2024).

Huber, G. P. (1991). "Organizational Learning: The Contributing Processes and the Literatures," *Organization Science*, 2(1), pp. 88-115.

"G7 Foreign Ministers' Statement in Italy on Addressing Global Challenges, Fostering Partnership" (2024). https://www.state.gov/g7-italy-2024-foreign-ministers-statement-on-addressing-global-challenges-fostering-partnerships/ (Accessed July 7, 2024).

Kupiecki, R., Bryjka, F., & Chłoń, T. (2022). Dezinformacja międzynarodowa. *Koncepcja, rozpoznanie, przeciwdziałanie.* Warsaw: Wydawnictwo Naukowe Scholar.

Kupiecki, R., Bryjka, F., & Chłoń, T. (2025). *International Disinformation. A Handbook for Analysis and Response.* Leiden / Boston: Brill.

Levitt, B., & March, J. G. (1988). "Organizational Learning." Annual Review of Sociology, 1, pp. 319-338.

Longstaff, P., et al. (2010). "Building Resilient Communities: A Preliminary Framework for Assessment." *Homeland Security Affairs*, 6(3). https://www.hsaj.org/resources/uploads/2022/05/6.3.6.pdf (accessed May 28, 2024).

Mounk, Y. (2018). *The People vs. Democracy. Why Our Freedom Is in Danger and How to Save It.* Harvard University Press.

National Academies of Sciences, Engineering, and Medicine (2010). "America's climate choices: Adapting to the impact of climate change." The National Academies Press. https://doi.org/10.17226/12783

Norris, F. H., Stevens, S. P., Pfefferbaum, B., Wyche, K. F., & Pfefferbaum, R. L. (2008). "Community Resilience as a Metaphor, Theory, Set of Capacities, and Strategy for Disaster Readiness." *American Journal of Community Psychology*, 41(1-2), pp. 127-150. https://doi.org/10.1007/s10464-007-9156-6.

Padan, C., & Gal, R. (2020). "A Multidimensional Matrix for Better Defining and Conceptualizing Resilience." *Connections: The Quarterly Journal*, 19(3), pp. 33-46. https://doi.org/10.11610/Connections.19.3.02

Powley, E. H., Barker Caza, B., & Caza, A. (Eds.) (2020). *Research Handbook on Organizational Resilience*. Edward Elgar Publishing.

Rosenberger, L., & Gorman, L. (2020). "How Democracies can Win the Information Contest." *The Washington Quarterly*, 43(2), pp. 1-22. https://doi.org/10.1080/0163660X.2020.1771045

"Strategic Compass for Security and Defence: For a European Union that protects their citizens, values and interests and contributes to international peace and security" (n.d). https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf (Accessed June 15, 2024).

Svintsytskyj, A. V., Semeniuk, O. H., Ufimtseva, O. S., Irkha, Y. B., & Suslin, S. V. (2023). "Countering fake information as guarantee of state information security." *Security Journal*, 36, pp. 427-442. https://doi.org/10.1057/s41284-022-00347-0.

The 2022 Code of Practice on Disinformation. https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation (Accessed July 5, 2024).

Tocci, N. (2019). “Resilience and the role of the European Union in the world.” *Contemporary Security Policy.* https://doi.org/10.1080/13523260.2019.1640342.

Topor, L. (2024). “Mis/disinformation and national resilience: Are countries immune to fake news?” *Cyber Sovereignty. Global Power Shift.* Springer, Cham. https://doi.org/10.1007/978-3-031-58199-1_5

U.S. Federal Emergency Management Agency (2019). “Guidance for stakeholder engagement.” https://www.fema.gov/sites/default/files/202002/Stakeholder_Engagement_Preliminary_Production_Process_Guidance_Nov_2019.pdf

Van der Kolk, B. (2014). *The Body Keeps the Score. Mind, Brain and Body in the Transformation of Trauma.* Viking Press.

Walker, B. (2020). “Resilience: What it is and is not.” *Ecology and Society*, 25(2):11. https://doi.org/10.5751/ES-11647-250211 (Accessed August 14, 2024)

Wyniki konsultacji założeń wdrożenia Aktu o usługach cyfrowych w Polsce. https://www.gov.pl/web/cyfryzacja/wyniki-konsultacji-zalozen-wdrozenia-aktu-o-uslugach-cyfrowych-w-polsce (accessed July 30, 2024)

Appendices

Appendix 1

Participants of MFA-organised seminars

Name	Description
Alliance4Europe	A European network aimed at promoting democracy, civic engagement, and collaboration across Europe.
Defence24	A Polish defence news portal providing in-depth analysis and reporting on security and military issues.
Fundacja Citizen Project/ Citizen Project Foundation	A Polish foundation promoting ethical citizenship, human rights, and democracy through education, culture, and social engagement.
Free Press for Eastern Europe	An organisation dedicated to supporting independent journalism and media freedom in Eastern Europe.
Institute for Digital Citizenship	An organisation promoting responsible digital citizenship with a focus on the ethical, cultural, and social aspects of online interactions.
Konkret24 / TVN24	A fact-checking platform and news outlet in Poland focused on verifying information and combating misinformation.
OSW	A government-funded think tank focusing on political, economic, and social developments in Eastern Europe, the Balkans, the Caucasus, and Central Asia.
PAP	The Polish Press Agency, a major source of news and information in Poland.
PISM	A leading Polish think tank specialising in international relations, security, and foreign policy.
SWPS University	A private university in Poland with a strong emphasis on psychology, law, and social sciences.

Association of Citizens Network Watchdog Poland	A Polish NGO focused on promoting transparency, government accountability, and civic engagement.
The Eye Press	A Polish investigative journalism platform focusing on transparency, human rights, and corruption.
The Orange Foundation	The charitable arm of Orange, which supports digital education and social inclusion initiatives.
Panoptykon Foundation	A Polish foundation advocating for digital rights, privacy, and the protection of personal freedoms in the digital age.
Pulaski Foundation	A Polish foundation focused on security and defence issues, providing analysis and policy recommendations.
UMCS	A major Polish university known for a wide range of academic disciplines, particularly in the humanities and social sciences.
UKSW	A public university in Poland known for its strong programmes in theology, social sciences, and humanities.
Visegrad Insight	A Central European think tank providing analysis and insight on regional politics, security, and democracy.
Demagog Association	A Polish fact-checking organisation dedicated to verifying claims and combating misinformation.
Ice Cyber Hub Research Center	A research centre focused on cybersecurity, particularly in the context of academic and practical applications.
Pravda Association	A Polish association focused on transparency, public accountability, and combating corruption.

Appendix 2

ORDER N°... MINISTER FOR FOREIGN AFFAIRS of..... 2024 on the Advisory Council to the Minister of Foreign Affairs on Countering International Disinformation

On the basis of Art. 4 point 5 of the Act of 8 August 1996 on the Council of Ministers (Journal of Laws No. Journal of Laws 2022, item 1188, 2023, item 1195, 1234 and 1641 and of 2024, item 834), the following provisions are hereby laid down:

§ 1.

1. A Consultative Council on Countering International Disinformation, attached to the Minister for Foreign Affairs, hereinafter referred to as 'the Council', is hereby established.
2. The Council's task is to formulate opinions and recommendations on issues related to countering international disinformation.

§ 2.

1. The Council shall be composed of:

    1. Chairperson – Plenipotentiary of the Minister of Foreign Affairs for Countering International Disinformation;
    2. Deputy Chairperson – Director or Deputy Director overseeing the unit responsible for strategic communication and countering international disinformation;
    3. Members – representatives of civil society organisations invited by the Minister of Foreign Affairs to participate in the work of the Council.

2. The meetings of the Council may be attended, in an advisory capacity, by persons whose qualifications, knowledge, or experience may be of assistance to the work of the Council.

§ 3.

1. The Chairperson shall direct the work of the Council, in particular:

    1. Chair its meetings;
    2. Convene meetings as necessary, but at least once every two months;
    3. Invite the persons referred to in § 2 sec. 2.

2. In the absence of the Chairperson, the tasks referred to in para. 1 shall be carried out by the Deputy Chairperson.

§ 4.

1. The Council shall act at meetings held at the premises of the Ministry of Foreign Affairs, hereinafter referred to as 'the Ministry'.
2. Meetings of the Council may be held by means of direct distance communication and electronic communication.
3. The Chairperson may decide to deal with matters by correspondence (circulation mode).

4. In the event of a failure to agree on a case in a circular manner, it is considered at a meeting of the Council.

§ 5.

1. The Council acts collegially.
2. The Council shall adopt its decisions by consensus. In the absence of consensus, the Chairperson shall order a vote. Resolutions shall be passed by a simple majority of the members of the Council present and voting. In the event of a tie, the Chairperson shall have the casting vote.

§ 6.

1. Participation in the work of the Council shall not be remunerated.
2. Members of the Council and persons referred to in § 2 sec. 2 are entitled to reimbursement of travel expenses in accordance with the rules set out in the provisions on the entitlements of employees employed in the state or local government budgetary unit for a business trip within the territory of the country.

§ 7.

1. The Secretary, appointed from among the members of the foreign service by the Head of the organisational unit of the Ministry responsible for strategic communication and countering international disinformation, shall be responsible for the technical and organisational support of the Council, in particular the preparation of Council documents and the minutes of its meetings. The Secretary shall not take part in the adoption of resolutions.
2. The minutes of the Council meeting shall be signed by the Chairperson and the Secretary.
3. Substantive support for the work of the Council is provided by the organisational unit of the Ministry responsible for strategic communication and countering international disinformation.

§ 8.

The Order shall enter into force on the day following that of its publication.

Appendix 3

List of resilience councils surveyed

The table below contains a list of 43 case studies that meet the resilience council criteria adopted for research purposes. It includes the name of the organisation or programme, the path to publicly available activity data, and a brief description of the resilience activities carried out. Most of these are still functioning organisations. A small number of organisations have ended their activities but offer achievements relevant to this report. The surveyed organisations have been grouped (regardless of whether they are still operating or have already finished their activities) according to the sector in which they operate.

The list of areas in which resilience councils and related organisations operate is very rich, as shown in the table below. However, it is worth noting that not every case can be unambiguously categorised because many of these organitions operate in several thematic areas. In this case, the classification is based on an arbitrary decision resulting from analysis of the dominant area of activity.

Name of Organisation	Category	Characteristics of Activities
100 Resilient Cities (100 RC)	Resilience of Cities	Strengthening resilience to physical, social, and economic challenges; providing resources for developing a roadmap to resilience across finance, logistics, expertise, best practices, networking, and mutual learning.
Resilient Cities Network	Resilience of Cities	Development of resilience strategies with action-oriented initiatives co-designed with cities; emphasis on peer-to-peer learning and specialised resilience tools.
ICLEI – Local Governments for Sustainability	Resilience of Cities	Global network supporting over 2,500 local governments in sustainable urban development; focus on low emission, nature-based, equitable, resilient, and circular development.
Leadership in Local Government. Resilient Leaders – Resilient Cities	Resilience of Cities	Program based on an urban resilience concept to create cities resistant to various crises; focuses on experience exchange and proven system solutions.
C 40 Cities Climate Leadership Group	Climate and Environmental Resilience	Global network of cities addressing the climate crisis through collaborative, science-based approaches to reduce emissions and build resilient communities.

Name of Organisation	Category	Characteristics of Activities
The Nature Conservancy	Climate and Environmental Resilience	Global initiative focusing on nature conservation, climate, water security, and sustainable food systems; partnerships with financial institutions to leverage nature's value.
Alliance for Climate Resilience (ACR)	Climate and Environmental Resilience	Manages Uganda's commercial interests in the petroleum sector, ensuring sustainability and developing expertise in oil and gas.
Resilience Alliance (RA)	Climate and Environmental Resilience	Global research organisation advancing resilience, adaptive capacity, and societal transformation to cope with change; focuses on comparative research and local studies.
Australian Institute for Disaster Resilience (AIDR)	Climate and Environmental Resilience	National structure organising disaster risk reduction and resilience; supports networking, knowledge-sharing, and leadership in disaster management.
Global Water Partnership Southern Africa (GWPSA)	Climate and Environmental Resilience	Regional network promoting integrated water resource management for sustainable development without compromising ecosystems.
The International Federation of Red Cross and Red Crescent Societies (IFRC)	Resilience through Crisis Management	Global organisation operating before, during, and after disasters to improve lives and promote humanitarian standards, resilience, and peace worldwide.
National Resilience Council (Philippines)	Resilience through Crisis Management	Public-private partnership enhancing local governments' capacity through evidence-informed risk management and best practices sharing.
FEMA – Federal Emergency Management Agency	Resilience through Crisis Management	U.S. agency focused on disaster prevention and mitigation, covering all hazards from local to extreme threats.
National Advisory Council (NAC)	Resilience through Crisis Management	FEMA's advisory body, representing a cross-section of emergency management experts; focuses on readiness, workforce, and climate-related issues.
Alabama Resilience Council (ARC)	Resilience through Crisis Management	Coordinates state government and private sector activities to proactively address harmful impacts on Alabama communities and infrastructure.

Name of Organisation	Category	Characteristics of Activities
Vanuatu Business Resilience Council (VBRC)	Resilience through Crisis Management	Private sector vehicle for climate change and disaster risk management, enhancing disaster resilience in local communities.
Global Youth Resilience Network (GYRN)	Resilience through Crisis Management	Non-profit coalition dedicated to disaster risk reduction and climate change adaptation through education and community-building initiatives.
Consultative Group on International Agricultural Research (CGIAR)	Agricultural and Food Resilience	Global research organisation addressing hunger and inequality by transforming food, land, and water systems in a climate crisis.
Resilient Agriculture Network (RAN)	Agricultural and Food Resilience	USAID project supporting farmers in building adaptive and productive farming systems by improving soil health and water management.
International Food and Agriculture Resilience Mission (FARM)	Agricultural and Food Resilience	French initiative preventing the effects of Russia's war in Ukraine on global food security; focuses on solidarity, long-term production, and global cooperation.
Global Food Security Cluster (FSC)	Agricultural and Food Resilience	Joint initiative by the FAO and WFP coordinating food security responses during and after crises; addresses food availability, access, and stability.
Global Health Security (GHS)	Health Resilience	Supports strong and resilient public health systems to prevent and mitigate the increasing severity of emerging infectious diseases.
Global Health Security Agenda (GHSA)	Health Resilience	A coalition of countries and organisations working together to prevent, detect, and respond to global health threats posed by infectious diseases.
One Health	Health Resilience	Integrated approach to balance the health of people, animals, and ecosystems; focuses on infectious diseases, antimicrobial resistance, and food safety.
Coalition for Epidemic Preparedness Innovations (CEPI)	Health Resilience	International partnerships developing vaccines and countermeasures to prevent future epidemics and pandemics; accelerates vaccine development against viral threats.
Resilience First	Financial and Economic Resilience	The world's largest business network setting the standard for resilience leadership in the private sector for a sustainable future; fosters collaboration and knowledge-sharing.

Name of Organisation	Category	Characteristics of Activities
Global Resilience Institute (GRI)	Financial and Economic Resilience	The Northeastern University unit developing tools to strengthen resilience against climate change, urbanisation, and social tensions.
Global Travel and Tourism Resilience Council (GTRRC)	Financial and Economic Resilience	NGO addressing challenges in the travel industry; partners with governments and organisations to respond to crises and share best practices.
Business Resilience Council (BRC)	Financial and Economic Resilience	Non-profit fostering collaboration in cyber and physical security, geopolitical risk, and disaster recovery; supports regional, national, and international organisations.
US Resiliency Council (USRC)	Financial and Economic Resilience	Organisation improving community resilience in the built environment; includes experts in engineering, public policy, insurance, and disaster response.
Fiji Business Disaster Resilience Council (FBDRC)	Financial and Economic Resilience	Supports businesses in disaster risk management and resilience; integrates the private sector into national disaster management plans.
Business Continuity Institute (BCI)	Financial and Economic Resilience	Global association that provides education, training, and certification for resilience professionals; fosters collaboration and information exchange.
Urban Land Institute (ULI)	Financial and Economic Resilience	Oldest network of real estate and land use experts; sets standards of excellence in development practice through knowledge exchange and good practices.
Global Cyber Alliance (GCA)	Technological and Cyber Resilience	Reduces cyber risks by providing free tools and resources for organisations and individuals; focuses on scalable, measurable projects with a global impact.
Global Forum on Cyber Expertise (GFCE)	Technological and Cyber Resilience	Multi-stakeholder community fostering global cybersecurity; includes governments, businesses, and academics working together on cybersecurity issues.
Scientific and Academic Computer Network (NASK)	Technological and Cyber Resilience	Polish research institution focused on ICT security and resilience; educates users on safe internet practices and promotes information society concepts.

Name of Organisation	Category	Characteristics of Activities
Digital Europe Resilience Council (DERC)	Technological and Cyber Resilience	Association representing digitally transforming industries in Europe; shapes industry positions on legislative issues and contributes to EU policy development.
Building Resilient Infrastructure and Communities (BRIC)	Resilience of Infrastructure and Transport Systems	FEMA programme supporting infrastructure projects to reduce hazard risks; encourages innovation and flexibility in project management.
The Coalition for Disaster Resilient Infrastructure (CDRI)	Resilience of Infrastructure and Transport Systems	Partnership promoting infrastructure resilience to climate change and disaster risks; focuses on capacity-building, standards, and global research.
Business Executives for National Security Resilience Council (BENSRC)	Resilience of Infrastructure and Transport Systems	U.S. organisation of professionals strengthening strategic preparedness in critical infrastructure and public security.
The Global Resilience Council (GRC)	Global Systemic Resilience	Initiative preparing for and responding to multidimensional global crises; focuses on interconnected governance systems and efficient response protocols.
Resilience Research Centre (RRC)	Global Systemic Resilience	Conducts research on resilience across cultures, providing tools and training for resilience in various settings, including families and communities.
Stockholm Resilience Centre	Global Systemic Resilience	Research centre focusing on sustainability challenges like climate change and biodiversity loss; promotes cooperation among researchers and global leaders.
Global Resilience Partnership (GRP)	Global Systemic Resilience	Supports resilience by scaling innovations, generating knowledge, and shaping policy; partners with over 80 organisations for sustainable development.

Source: Own study.