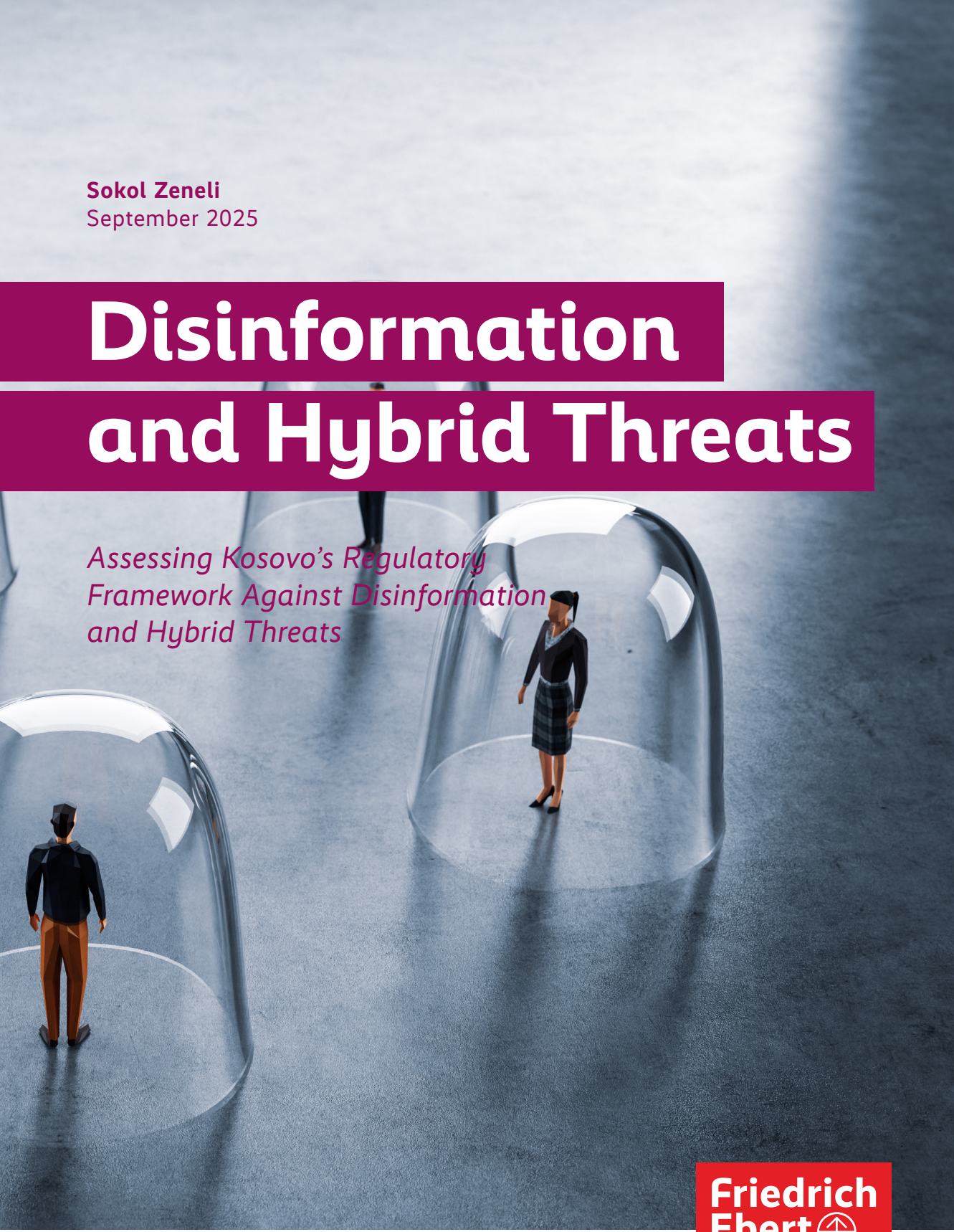
Sokol Zeneli
September 2025

Disinformation and Hybrid Threats

Assessing Kosovo's Regulatory Framework Against Disinformation and Hybrid Threats



RE-ACT LAB
on Policymaking and Good Governance

Friedrich Ebert Stiftung

Imprint

Publisher
Friedrich-Ebert-Stiftung e.V.
Godesberger Allee 149
53175 Bonn
info@fes.de

Responsibility for content and editing
Katharina Hofmann

Contact
Rudina Nallbani
rudina.nallbani@fes.de

Design/Layout
Trembelat

Front page design
Trembelat

Printing and production
Studio Forma

 This policy brief was developed as part of the project "Assessing the Resilience of Kosovar Society to Ecological and Institutional Shocks". A comprehensive scoring database, which underpins the analysis presented herein, is available upon request. Please send your requests to info@re-actlab.org.

September 2025

Further publications of the Friedrich-Ebert-Stiftung can be found here:
↗ www.fes.de/publikationen

Friedrich Ebert Stiftung

RE-ACT LAB
on Policymaking and Good Governance

Sokol Zeneli
September 2025

Disinformation and Hybrid Threats

Accessing Kosova's Regulatory Framework Against Disinformation and Hybrid Threats

Contents

Key Recommendations

The following key recommendations are proposed to build a more resilient regulatory and societal framework:

- **Modernise Media Regulation to Cover the Online Sphere** - The government should substantially reform the Law on the Independent Media Commission (IMC) to grant it a clear and expanded mandate to oversee online media, including news portals and digital platforms, ensuring it is equipped with adequate resources and independence.

- **Increase Transparency and Accountability for Online Platforms** - Adopt or amend legislation in accordance with the EU's Digital Services Act (DSA), especially its requirements on transparency for online political advertising, requiring clear labelling of state-sponsored content, politically sponsored and driven content, etc.

- **Integrate Counter-Disinformation into National Security** - Revise the Kosovo Security Strategy to explicitly define and integrate actions against disinformation and hybrid threats as a core priority, ensuring clear roles for cross-agency collaboration and strategic alignment with the National Cybersecurity Strategy.

- **Launch a National Media and Information Literacy Strategy** - Develop and implement a comprehensive, long-term national strategy to build societal resilience by integrating media and information literacy into the formal education system and strong public awareness programmes for all citizens.

Acknowledgement

This policy brief was developed as part of the project "*Assessing the Resilience of Kosovar Society to Ecological and Institutional Shocks*". A comprehensive scoring database, which underpins the analysis presented herein, is available upon request. Please send your requests to info@re-actlab.org.

Introduction

In an era defined by complex geopolitical competition, the stability and democratic development of small countries like Kosovo face unprecedented challenges. Kosovo's institutions operate within a complex geopolitical landscape which is marked by contested statehood, historic ethnic tensions in the region and strategic competition among regional and global powers such as Russia, China, Türkyie, Gulf States (United Arab Emirates, Saudi Arabia, Qatar and Kuwait), alongside the European Union (EU) and United States (US). This environment creates a fertile ground for external influence and instability, making Kosovo institutions and society susceptible to destabilising shocks, most notably disinformation and hybrid threats. These shocks are not abstract risks but persistent, tangible challenges impacting Kosovo's security, social cohesion and democratic development.

"These shocks are not abstract risks but persistent, tangible challenges impacting Kosovo's security, social cohesion and democratic development."

The core issue we aim to address is the acute vulnerability of Kosovo's institutional and societal structures to disinformation and hybrid threats. While the sources and manifestations of disinformation campaigns - from state-sponsored narratives aimed at delegitimising Kosovo's statehood to the internal dynamics of a media landscape grappled with clickbait and unverified information - are increasingly documented, a critical gap remains in systematically evaluating the resilience of the existing regulatory framework to withstand and counterattack these shocks. Hybrid threats, in their deliberate blend of clever and overt measures, including cyber operations, political coercion and the manipulation of cultural and religious narratives, demand a holistic and adaptive response mechanism that the current regulatory framework in Kosovo does not adequately provide. The persistence of ethnic divisions, coupled with socio-economic vulnerabilities and instances of foreign interference exploiting these seams, underscored the urgency of this assessment.

The policy brief aims to critically assess Kosovo's regulatory preparedness, specifically its capacity for resilience against the distinct yet intertwined challenges of disinformation and hybrid threats. The central aim is to move beyond cataloguing threats to rigorously analysing the existing legal, policy and institutional architecture's ability to anticipate, absorb, adapt to and recover from such shocks. The subsequent section will explain the methodology applied in this research. The next sections will delve into a detailed mapping of Kosovo's regulatory framework concerning these shocks, followed by an in-depth application of the 4Rs framework to selected policies. The findings of this assessment will be discussed, highlighting systemic vulnerabilities and areas of concern. Finally, the brief will conclude by offering a set of targeted recommendations designed to enhance Kosovo's institutional and societal resilience, aiming to foster a more robust, adaptive and rights-respecting approach to countering disinformation and hybrid threats in line with European best practices.

Methodology

The policy brief is part of a larger research conducted on institutional shocks that Kosovo faces. The research employs a systematic policy analysis framework designed to assess the resilience of Kosovo's existing regulatory framework (policies, laws, bylaws, strategies, governmental documents, etc) against several shocks. The research process followed a structured process consisting of three main phases: (i) identifying the nature of the shock, (ii) assessing the current policy responses through a scoring system, and (iii) developing recommendations based on the findings and best practices.

The classification of the nature of the shocks is based on the framework developed by the OECD in 2014, as explained in the table below:

Table 1. Classification of shocks[1]

Type of shock	Characteristics	Examples
Covariate Shocks (*Widespread, Systemic and Infrequent*)	Large-scale events that affect a large portion of the population at once. They are not frequent, but their impact is widespread and systematic.	Violent Conflict and political crises, pandemic and health crises, large-scale natural disasters, cybersecurity and hybrid threats.
Seasonal Shocks (*Recurring, Predictable and Localised*)	Periodic shocks that occur at regular intervals, often linked to seasonal changes or climate patterns. Usually predictable, but inadequate preparedness can exacerbate their impact.	Annual floods and droughts, heatwaves and cold snaps, seasonal food insecurities, recurring health risks.
Long-Term Stressors (*Gradual, Cumulative and Systemic Erosion of Resilience*)	Unlike shocks, long-term stressors develop slowly over time and weaken societal systems. These are often structural, environmental, economic or social shocks requiring policy responses.	Environmental degradation, demographic shifts, economic stagnation and inequality, weak institutions and governance.

To evaluate the effectiveness of the regulatory framework in countering various shocks, we build upon the 4Rs of Resilience framework. This framework assesses policies against four key dimensions of resilience:

Table 2. The 4Rs of Resilience Framework

Framework	Category	Definition
4Rs of Resilience	Robustness	The strength, or the ability of elements, systems and other units of analysis to withstand a given level of stress or demand without suffering degradation or loss of function.
	Redundancy	The availability of alternative resources in the recovery process of a system.
	Resourcefulness	The capacity to identify problems, establish priorities, and mobilise resources when conditions exist that threaten to disrupt some element, system, or other unit of analysis.
	Rapidity	The capacity to meet priorities and achieve goals in a timely manner in order to contain losses and avoid future disruption

Each source identified as part of the regulatory framework addressing the shocks is evaluated against the 4Rs framework using a structured scoring system, as explained below:

Table 3. Scoring system based on the 4Rs Framework

Scoring	
Robustness	0: No robustness—policy does not address stability in the face of shocks. 1: Weak or symbolic measures with little enforcement. 2: Moderate mechanisms exist, but they are inconsistently applied. 3: Strong, well-enforced mechanisms ensuring stability.
Redundancy	0: No redundancy—failure of the main system leads to collapse. 1: Minimal or informal alternatives that are unreliable. 2: Some redundancy, but gaps exist in coverage or efficiency. 3: Well-integrated redundancy ensures continuity under stress.
Resourcefulness	0: No resourcefulness—reactive rather than proactive approach. 1: Limited adaptability - response mechanisms are weak or ad hoc. 2: Moderate ability to mobilise resources, but gaps remain. 3: Highly flexible and well-coordinated response mechanisms.
Rapidity	0: No rapid response mechanisms—delayed or absent reactions. 1: Slow and bureaucratic response with major inefficiencies. 2: Moderate speed, but some bottlenecks exist. 3: Highly efficient, fast-track response ensuring swift action.

The total policy resilience score (0-12) is then normalised into a percentage, enabling comparative evaluation across different policies and sectors.

Resilience score = SUM (Total score/12) x 100

Table 4. Scoring interpretation

Scoring Interpretation		
0-25% (0-3 points)	Very Low Resilience	The policy makes the society highly vulnerable to shocks, offering little protection or response capability.
26-50% (4-6 points)	Low Resilience	Some resilience measures exist, but they are either weak, inconsistent, or incomplete.
51-75% (7-9 points)	Moderate Resilience	The policy provides a reasonable level of preparedness and response, but some critical gaps remain.
76-100% (10-12 points)	High Resilience	The policy is well-designed, with strong mechanisms ensuring stability, adaptability, and quick response.

For more detailed research methodology, please refer to the Policy Analysis Framework developed for this research. You can find it in this link.

Background info and context

Disinformation and hybrid threats are *covariate shocks* which vary in terms of frequency and have a systemic negative impact on society and political developments surrounding them. Disinformation refers to the systematic and intentional creation and propagation of false, biased, or manipulative information, created to deceive target audiences and achieve certain objectives.[2] This disinformation is disseminated through online portals, social media, and coordinated campaigns which aim to exploit existing societal fault lines.[3] Hybrid threats on the other hand refer to the broader utilisation of disinformation as a tool together with other hostile actions - political pressure, economic coercion, cyber operations, cultural and religious manipulations, etc - by state or non-state actors to destabilise Kosovo, exploit its vulnerabilities, and achieve strategic objectives without resorting to conflict.[4] The two are deeply intertwined; disinformation often prepares the ground for, or amplifies the effects of other hybrid tactics, leading to a general confusion, distrust and polarisation that makes institutions and society more vulnerable to manipulation and coercion.

"Kosovo's susceptibility to these shocks is not a recent development but rather a consequence of its post-conflict realities and its position as a geopolitical pressure point."

Kosovo's susceptibility to these shocks is not a recent development but rather a consequence of its post-conflict realities and its position as a geopolitical pressure point. The legacy of the conflicts, its contested statehood and ethnic divisions provide vulnerabilities that external and internal actors continue to exploit consistently. For instance, the conflict with Serbia has historically allowed ethnic nationalism to thrive on both sides, often dominating public discourse and political agendas.

Similarly, foreign interference has always been present, with various actors pursuing different - but often overlapping -agendas which impact the stability and democratic consolidation of the country.[5] Serbia, often supported by Russia, has engaged in long-running disinformation campaigns aimed at delegitimising Kosovo's independence, portraying it as unstable or dangerous (particularly for Serbs), and sabotaging its integration into international structures.[6] The majority of this disinformation

enters Kosovo through Serbian-language media outlets, some directly funded by Belgrade or linked to Russian state media like Sputnik's branch in Serbia.[7] These narratives are then further disseminated within Kosovo, mainly in areas with a Kosovo Serb majority, but often also get picked up by Albanian language online media chasing clicks.[8] For instance, in 2018 alone, no less than 700 false news stories were published by Serbian media reporting an 'imminent war' between Kosovo and Serbia.[9] A similar dynamic was also largely present during the 2022 Serbian elections.[10]

Other actors also influence events in Kosovo. Türkyie, for example, has created ties with Kosovo through its significant economic investments, cultural and religious diplomacy through its *Agency for Cooperation and Coordination (TIKA)* - including funding mosques, educational opportunities - media platforms like TRT Balkan[11], and defence cooperation.[12] However, Türkyie's influence has manifested in concerning ways, such as the 2018 covert rendition of alleged Gülen supporters, which exposed vulnerabilities and parallel structures within Kosovo's security apparatus susceptible to foreign pressures.[13] The influence of Türkyie continues to be strong even nowadays, such as in the case of the double cancellation of the performance "The Six Against Turkey" in Kosovo. The performance depicts the developments leading to the deportation of six Turkish teachers in 2018. The authors of the performance argued that the cancellation came due to the influence of the Turkish Embassy in Kosovo.[14] The cancellation was first justified due to technical issues, while later it was announced that the performance was cancelled as 'it is against the values of the Turkish community' and 'against Türkyie and its president'.[15]

Gulf States (especially Saudi Arabia) also have a significant influence over Kosovo. This influence has been largely linked to the spread of conservative Wahhabi interpretation of Islam, and in some cases, provided pathways for radicalisation and recruitment by extremist groups exploiting socio-economic marginalisation in areas neglected by the state.[16]

China, on the other hand, although with a lower presence in Kosovo, continues to influence the region through infrastructure investments under its Belt and Road Initiative[17] and provision of technology, like the surveillance systems that Kosovo uses, raising concerns about potential dependencies and the promotion of alternative governance models.[18] For instance, Kosovo has installed approximately 3,500 surveillance cameras with facial recognition capabilities produced by Chinese companies like Dahua and Hikvision.[19] The latter is a blacklisted company by the US.

These pressures and influences are further exacerbated by the internal factors in the country. Kosovo's media landscape, especially the online sector, suffers from systemic weakness. A lack of effective regulation, non-transparent ownership structures often linked to political or business interests, and intense competition contribute to the spread of disinformation.[20] Attempts to introduce regulation for online media have historically faced resistance or failed to materialise[21], and overall institutional capacity to counter disinformation campaigns and hybrid threats remains weak, lacking sufficient awareness, resources and coordinated strategies.

The consequences of these shocks are profound, impacting not only the institutional stability but also posing direct harm to citizens and society. One of the most harmful impacts remains the degradation of trust - be it between citizens and the state, among ethnic communities, or trust in the media - fueled by narratives of corruption, bias and the ongoing amplification of ethnic grievances. Additionally, by exploiting the socio-economic vulnerabilities of Kosovar society, disinformation and hybrid threats are used to create pathways to radicalisation. As it was shown, neglect, poverty, unemployment, and poor access to education in marginalised communities created an opening for extremist religious groups, funded by foreign actors, to spread radical ideologies, leading to tragic outcomes like citizens joining foreign conflicts.

The constant spread of narratives about potential conflict, ethnic threats, state failure, or external aggression leads to an increased sense of anxiety and instability among citizens and potentially contributes to 'brain drain'. Disinformation campaigns in Kosovo almost exclusively create panic or alarm, especially targeting minority communities, to achieve political goals or undermine confidence in Kosovo's future.[22] Similarly, these shocks directly impact the institutional integrity and functionality. Malign campaigns undermine governance effectiveness and the rule of law, often exploiting or exacerbating existing weaknesses like perceived corruption, political favouritism or inefficiency. This erodes institutional legitimacy both domestically and internationally.

The risks posed by disinformation and hybrid threats to Kosovo's institutions and society are not likely to diminish and could even intensify without proper mitigation efforts. The ongoing geopolitical tensions on Kosovo's status and regional power dynamics ensure it will remain a target for external actors seeking to exert influence, maintain instability, or disrupt Kosovo's Euro-Atlantic path. Furthermore, the methods employed in hybrid threats are constantly evolving, leveraging technological advancements to increase the speed, scale and sophistication of disinformation campaigns and cyber operations. The institutional capacity of Kosovo to counter these evolving threats remains a significant concern, with gaps in the legal frameworks, technical capabilities, human resources, and a lack of strategic coordination.

Regulatory Framework

The regulatory framework - comprising laws, regulations, strategies, and other policies - is crucial for Kosovo in addressing and resolving these shocks. Beyond that, the regulatory framework needs to ensure its resilience in order to help institutions and society to withstand the shocks. At the current state, although a relevant regulatory framework is in place, it is marked by significant gaps, outdated legislation and fragmented responsibilities.

The *Constitution of the Republic of Kosovo* is the bedrock for this regulatory framework. It guarantees fundamental rights relevant to the information space. More particularly, Articles 40 and 42 explicitly protect the freedom of expression and media freedom and pluralism, ensuring the right to disseminate and receive information while prohibiting censorship.[23] The constitution, through this, sets the stage for an open information environment, which, anyway, requires supporting legislation and regulation to function properly in the face of different shocks, including disinformation and hybrid threats.

In this regard, there are several laws that address aspects related to information integrity and accountability. More particularly, the *Law Against Defamation and Insults* sets standards for compensating individuals whose reputation is harmed, aiming to balance reputational protection with freedom of expression.[24] Other laws include those *Protecting Journalistic Sources*[25], *Whistleblowers*[26], ensuring *Access to Public Documents*[27], and safeguarding *Personal Data*.[28] While these laws are important, they primarily address specific harms or procedural rights rather than the systemic challenge of coordinated disinformation campaigns or hybrid threats. In general, Kosovo lacks specific laws regulating crucial aspects of the modern media environment, such as media financing and ownership, particularly those for online entities[29], therefore leaving significant space for hidden influence unexplored and unregulated.

The primary regulatory body for media is the *Independent Media Commission (IMC)*, which is established under Article 141 of the Constitution. Its mandate includes regulating broadcasting frequencies, licensing public and private audio and audiovisual broadcasters, and implementing broadcasting policies.[30] However, this law is widely considered outdated and not fit for the digital age.[31] Most worrying in this regard is the fact that IMC's authority does not extend to online media (news portals, social media platforms, etc), which play a crucial role in spreading disinformation. This regulatory framework is significant. For instance, the IMC has the authority to demand the removal of channels from broadcasting

operators, as it did following the Russian invasion of Ukraine when it ordered the removal of Russia Today, Russia 24 and Planeta RTR to prevent propaganda.[32] However, as such authority does not extend to online media, they are left with the risk of potentially amplifying such disinformation and propaganda without restriction. Additionally, considering that the board members of IMC are appointed by the National Assembly[33], concerns over its independence remain.

The work of online media falls under the purview of the *Press Council of Kosovo (PCK)*, which is a self-regulatory body founded by and for the media sector. The PCK is guided by its Press Code of Kosovo, and handles various complaints regarding ethical breaches by print and online media.[34] The biggest shortcoming of the PCK remains its inability to enforce decisions; the institution cannot issue fines or revoke licenses, limiting its effectiveness in efforts to counter disinformation and hybrid threats spread by online media.

The efforts of government and public institutions to strengthen the regulatory framework to fight discrimination were largely opposed by media bodies like the PCK and the *Association of Journalists of Kosovo (AGK)*, fearing the potential infringements on free speech.[35] Past attempts by the government in this direction include the Draft Media Law in 2018, and the proposal to regulate the issue of 'fake news' through Kosovo's Criminal Code by considering it as hate speech.[36]

With regards to cybersecurity - as a critical component of countering hybrid threats - Kosovo adopted the *Law on Cybersecurity* in 2023.[37] The legislation led to the establishment of the *Cybersecurity Agency (CSA)*, which is tasked with overseeing the cyber defence of Kosovo and providing relevant training through its Cybersecurity Training Centre.[38] Although the law is adopted, experts and international reports indicate that Kosovo continues to lack a comprehensive cybersecurity framework, sufficient operational mechanisms, technical capabilities and human resources to effectively address cyber threats, including those linked to disinformation campaigns.[39]

On a strategic level, Kosovo lacks a dedicated national plan to combat disinformation and promote media and digital literacy. Although the *Digital Agenda for Kosovo 2030* outlines goals for digital development, it does not propose or plan any measures or objectives related to countering disinformation, enhancing citizens' critical information consumption skills or their abilities to identify disinformation. The absence of a strategic vision and dedicated educational initiative leaves a significant gap in building societal resilience against manipulation.

While the regulatory framework is sufficient to provide fundamental rights, it largely suffers from outdated laws for traditional media, low regulation for online media, limited enforcement capacity among self-regulating bodies, weak cybersecurity structures and a lack of strategic focus on countering these shocks. The fragmentation and incomplete framework open the space for external and internal actors to exploit these vulnerabilities.

Applying the policy analytical framework

Building upon the mapping of Kosovo's relevant regulatory framework, this section will provide a more in-depth analysis by applying the 4Rs of resilience framework[40] (robustness, redundancy, resourcefulness and rapidity), to evaluate relevant laws, regulations, policies and strategies relevant to countering and addressing disinformation and hybrid threats. We do so in order to understand how each component of the regulatory framework contributes or fails to contribute to Kosovo's capacity to withstand and respond effectively to these shocks.

A total of 11 sources were assessed as part of this policy brief. The sources were selected based on their application in the event of disinformation and hybrid threats, and they included policies, laws, bylaws, administrative instructions, and national strategies. These were analysed as presented below:

Law No. 02/L-65 - Civil Law Against Defamation and Insult

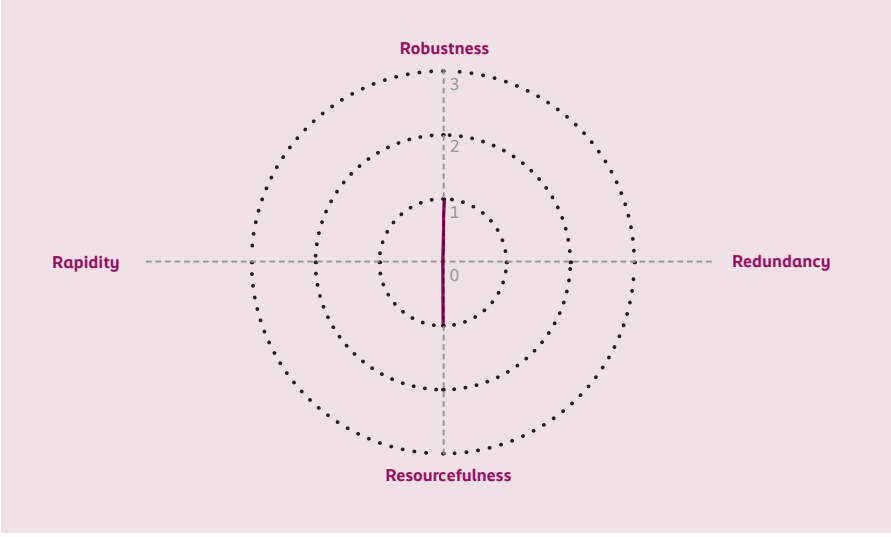


Figure 1: 4Rs Framework Assessment of Law No. 02/L-65 Civil Law Against Defamation and Insult. (Source: Own creation)

This is an important law that provides relevant avenues to address reputational harm, which can serve to address issues related to disinformation, however, the law itself demonstrates very low resilience against systemic disinformation and hybrid threats, assessed at only 17%.

The robustness of this law is weak (score 1). Although the law does not cover issues related to hybrid threats, it does offer a legal basis for dealing with reputational damage (which could come as a result of disinformation). However, it lacks specific measures for disinformation or

state-sponsored influence. Its redundancy is non-existent (score 0), as the law relies entirely on civil courts, therefore, it offers no alternative mechanisms or fallback systems to flag or mitigate information threats beyond litigation. Resourcefulness is also limited (score 1); the law permits individual resources but lacks collaborative or adaptive components like public awareness, digital platform engagement or media literacy promotion. Lastly, its rapidity is also non-existent (score 0) as standard court procedures are inherently long and take time.

It is worth noting that the law has a very narrow scope and focuses mainly on individual reputational harm. Allowing only for civil litigation means it is not suited to address the speed, scale and systemic nature of coordinated disinformation campaigns. Policymakers should acknowledge that the law, while important for individual rights, offers negligible protection or response against shocks like disinformation and hybrid threats.

Law No. 06/L-082 on Protection of Personal Data

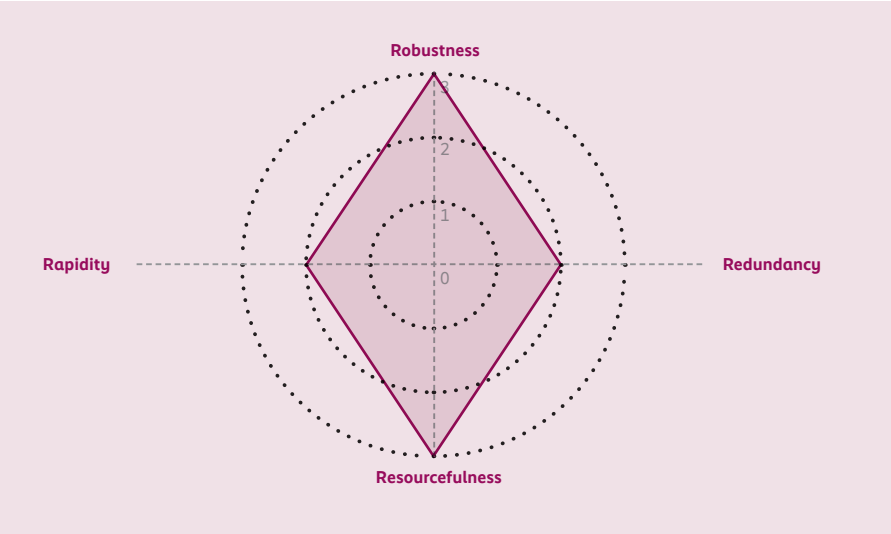


Figure 2: 4Rs Framework Assessment of Law No.06/L-082 on Protection of Personal Data.
(Source: Own creation)

The law is especially important in addressing these shocks as it provides strong data protection, indirectly supporting resilience against them by protecting a key attack vector. The law received a high resilience score of 83%.

Due to its alignment with GDPR, a dedicated supervisory authority (Information and Privacy Agency), and a clear enforcement mechanism through inspections and fines, it excels in robustness (score 3). Resourcefulness is also high (score 3) because the law empowers data subjects with rights (access, correction, deletion), mandates transparency and enables adaptive responses. Its redundancy is moderate (score 2); layered data protection principles and data minimisation principles offer some backup, but specific

institutional backup plans are lacking if the main agency is compromised. Rapidity is also moderate (score 2) with defined timelines for handling requests from data subjects, but provisions related to emergency operational systems for rapid actions (e.g. hybrid threats or disinformation campaigns exploiting personal data) are absent.

The strong robustness makes it harder for malicious actors to exploit personal data for disinformation, therefore complementing cybersecurity efforts in the country (will be explained below). While it shows high resourcefulness, its moderate redundancy implies potential risks if the primary authority fails during a crisis. In terms of rapidity, the law functions well for standard protection, but it is not designed for the immediate intervention speed needed during an acute data-driven information crisis. Therefore, its contribution remains primarily preventative.

Law No. 08/L-173 on Cyber Security

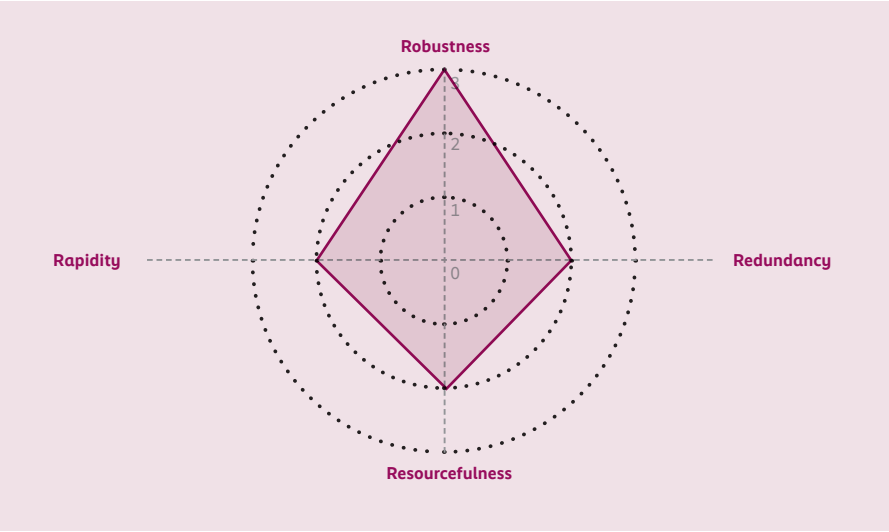


Figure 3: 4Rs Framework Assessment of Law No.08/L-173 on Cyber Security
(Source: Own creation)

This is a foundational law in the protection against cyber threats that tackle Kosovo's cyberspace. The law was assessed with an overall score of 75%, making it moderately resilient.

As it is visualised in the figure 3, the law demonstrates significant robustness (score 3), establishing a strong institutional basis with the Cybersecurity Agency (CSA) with clear responsibilities, and enforceable penalties for non-compliance.[41] Redundancy is moderately present (score 2) through the mandated cyber security incident response teams (CSIRTs), but it overall lacks depth regarding alternative communications infrastructure or comprehensive contingency plans, should the primary system fail. Similarly, resourcefulness is moderate (score 2) as it authorises CSA to coordinate nationally and internationally as well as plan training[42]. However, limitations exist in

broader stakeholder engagement (civil society, local actors) and a lack of provisions for flexible funding or fostering innovation in response strategies. Rapidity is also moderate (score 2); mandated reporting timelines exist (24-hour incident notification)[43], but the framework lacks defined fast-track decision-making or crisis coordination protocols crucial for effective and timely responses to dynamic cyber or disinformation events.

The strong robustness of the law provides a solid base for managing cyber threats and can serve as a legal foundation for related strategies. Its effectiveness against disinformation depends largely on the coordination with other - currently weak - bodies. However, it is worth noting that the moderate redundancy means that Kosovo remains vulnerable if primary cyber defences are overwhelmed in complex attacks. In terms of rapidity, while the alerts are timely, coordinated responses could face procedural delays without specific crisis protocols defined elsewhere.

Policymakers should recognise the limitations of this law in addressing the shocks as disinformation and hybrid threats. The law overall provides a necessary but insufficient condition for resilience; its potential can only be fully materialised through strong strategic direction (like the National Cybersecurity Strategy), other operational procedures and crucially, complementary measures addressing the information environment.

Administrative Instruction No.04/2024 on Registry of Cyber Incidents

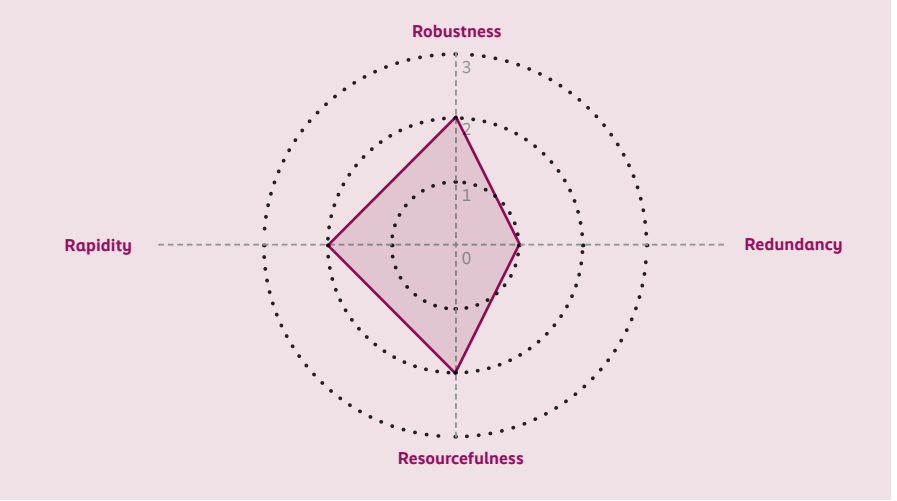


Figure 4: 4Rs Framework Assessment of Administrative Instruction No. 04/2024 on Registry of Cyber Incidents. (Source: Own creation)

The instruction is a crucial policy as it helps in logging incidents, but it overall reveals significant resilience gaps. The instruction received a score of 58% indicating a moderate level of resilience.

The robustness of the instruction is moderate (score 2); it requires the CSA to keep a secure incident registry and outlines relevant procedures for notification, tracking and analysis.[44] However, no measures specifically target disinformation or classify hybrid threats, restricting institutional strength. Redundancy is weak (score 1); while the registry is utilised for future risk assessments[45], no back-up registries of duplicate systems are mentioned, offering little proof of fallback infrastructure. Resourcefulness is moderate (score 2) with opportunity for anonymous reporting of incidents through the CSA website[46] potentially broading input, but it lacks inclusion of wider diverse stakeholders. Similarly, rapidity is moderate (score 2); the CSA has a duty to respond quickly to reported events[47], but the instructions lack multi-agency cooperation protocols or specific fast-track processes for urgent actions.

As it is, the instruction provides a solid administrative and operational procedure for registering incidents, but its lack of specific classifications for hybrid or disinformation-related cyber incidents limits its utility for targeted analysis. The weak redundancy makes the system largely vulnerable, while the CSA's duty to respond quickly is positive, but without multi-agency protocols, it risks slower coordinated action. Policymakers should consider introducing enhancements, especially with respect to robustness, redundancy and rapidity.

Administrative Instruction No.05/2024 on Registry of Cyber Security Risks and Threats

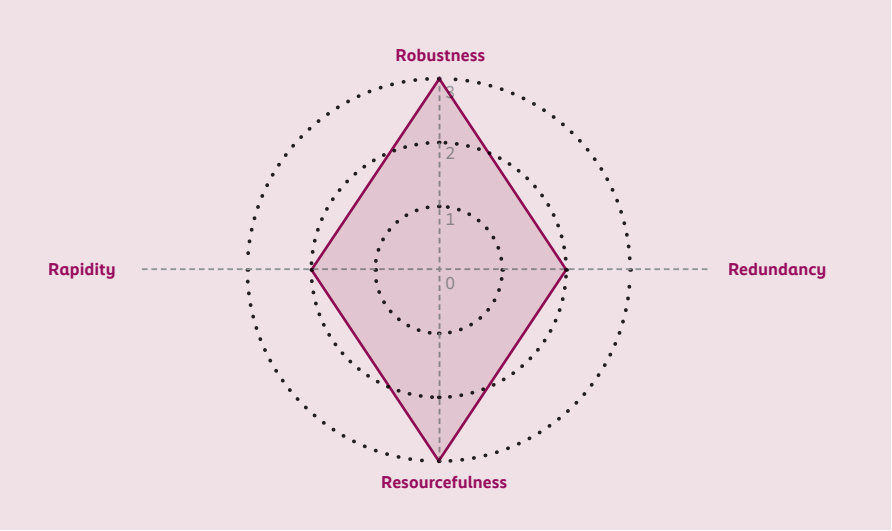


Figure 5: 4Rs Framework Assessment of Administrative Instruction No. 05/2024 on Registry of Cyber Security Risks and Threats. (Source: Own creation)

Assessed as highly resilient, with a score of 83%, the instruction provides a strong framework for the systematic identification and management of cyber risks.

The instruction has high robustness (score 3) as it establishes a mandatory, organised registry for cyber risks managed by the CSA in collaboration with other institutions, supported by classification criteria and analytical tools.[48] It also has a high resourcefulness (score 3) as it facilitates the development of specialised tools and guidelines, integrates several organisations (military, telecoms, regulators), and offers flexible risk evaluations[49], encouraging cooperative and adaptable institutional behaviour. Its redundancy is moderate (score 2); although the system prioritises and records risks, it does not create backup operational levels or alternative registries to prevent failure if the primary registry is compromised. The rapidity is also moderate (score 2) since the instruction does not foresee any urgent action or real time threat escalation based on registry data alone. It does, however, include annual reporting and continues data entry.

The instruction's robust system for risk identification and highly resourceful interagency cooperation are key strengths, directly supporting the National Cybersecurity Strategy by providing systemic data. Its effectiveness in a crisis depends largely on its integration with other policies capable of translating the identified risk into action.

National Cyber Security Strategy 2023 - 2027[50]

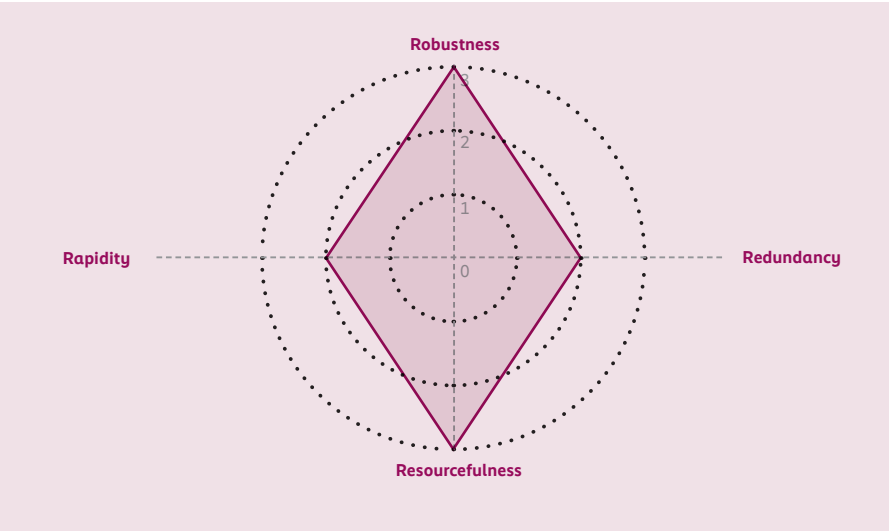


Figure 6: 4Rs Framework Assessment of National Cyber Security Strategy 2023 - 2027
(Source: Own creation)

The strategy is another important regulatory policy and it operationalises the Law on Cyber Security (discussed above), aiming for coordinated cyber resilience. The strategy is assessed as highly resilient with a score of 83%.

As presented in Fig.6, the strategy exhibits high robustness (score 3); it clearly assigns institutional responsibilities to entities like the Ministry of Internal Affairs and the CSA, mandates sectoral CSIRTs, and requires periodic security audits for critical infrastructure operators (pp. 20-22, 34-38). Its resourcefulness is also high (score 3), promoting a multisectoral approach, including collaboration between government, private sector and academia, outlines a national cyber risk management system, and plans for CSO inclusion in awareness campaigns (pp. 25, 22, 28, 40-41), indicating a flexible and well-coordinated response system. However, redundancy is moderate (score 2); although the measure encourages vulnerability mapping and introduces CSIRTs (pp. 22 -24), it does not ensure complete redundancy across all sectors or detailed, comprehensive plans for backups. Rapidity is also moderate (score 2) as the measure does introduce emergency response procedures like Emergency Team (EKRSH) and early warning alerts (pp. 26, 40), but it does not yet specify legally obligatory emergency procedures or formal fast-track resource allocation.

Kosovo Security Strategy 2022 - 2027[51]

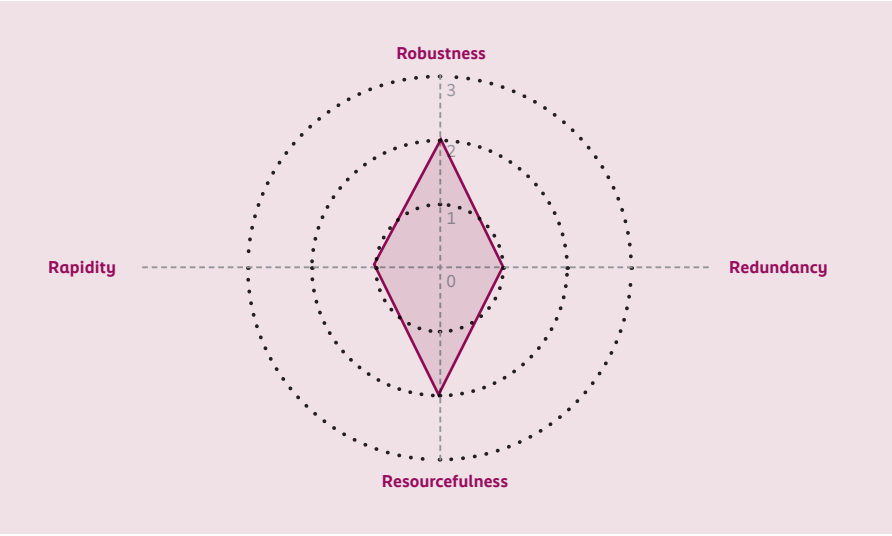


Figure 7: 4Rs Framework Assessment of Kosovo Security Strategy 2022 - 2027. (Source: Own creation)

This is an overarching strategy which acknowledges various threats. However, it demonstrates low resilience concerning specific challenges posed by disinformation and hybrid threats, assessed with a score of 50%.

Robustness is moderate (score 2) as the strategy acknowledges hybrid threats including disinformation campaigns and cyberattacks, and assigns responsibility of institutions like the Kosovo Intelligence Agency and Security Forces (pp. 7-8). However, specific tools and operational means for misinformation response remain broadly described and underdeveloped. Redundancy is weak (score 1); the strategy notes inadequate infrastructure and reliance on bilateral agreements for intelligence (p. 9), with no explicit parallel systems or backup communication frameworks mentioned to prevent cyber or information failures during hybrid attacks. Its resourcefulness is moderate (score 2) as it reflects institutional adaptability and aims to strengthen governance, however, it lacks multi-stakeholder collaboration (especially with media, CSOs for disinformation). Rapidity is weak (score 1) as the measure lacks concrete rapid-response mechanisms specifically tailored to the urgency of disinformation campaigns or hybrid threats.

Although the strategy is an important overarching instrument, its low resilience indicates that Kosovo's primary security strategy is not well equipped to effectively counter disinformation and hybrid threats. It is important that the strategy is revised to incorporate robust counter-disinformation tools, enhance its redundancy through contingency planning, and establish clear, rapid crisis response mechanisms that integrate effectively with other national strategies.

Law No. 04/L-044 on the Independent Media Commission (IMC)

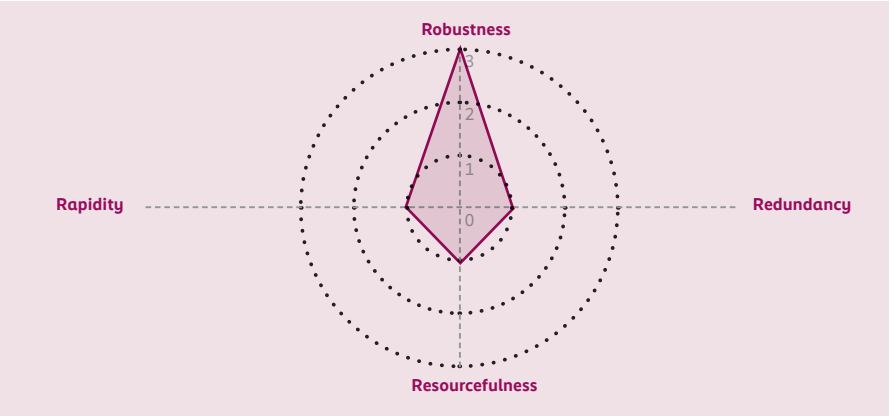


Figure 8: 4Rs Framework Assessment of the Law No. 04/L-044 on the Independent Media Commission. (Source: Own creation)

This law is important as it establishes the IMC as the regulator for audiovisual media in Kosovo. Although important in tackling disinformation and hybrid threats in media, it received a score of 50%, indicating low resilience.

Its robustness is high (score 3) for its mandated sphere. The law establishes the IMC as a constitutionally mandated, independent body tasked with licensing, monitoring, and sanctioning audiovisual broadcasters, with legally binding and enforceable rulings.[52] Through this, the law creates a strong institutional governance structure for traditional broadcast media. Its redundancy is weak (score 1) as the measure does not provide for alternative oversight organisations or parallel structures if the IMC is overburdened or compromised. While it provides collaboration with other institutions[53], specific fallback procedures or multiple enforcement routes are not specified. Resourcefulness is also weak (score 1); although the IMC can create internal rules and coordinate with the National Assembly, the law does not foster broader cooperation with other stakeholders (especially with CSOs or tech platforms to counter disinformation), or have an adaptive response tool like digital monitoring systems. Similarly, its rapidity is assessed as weak (score 1); while the IMC has the authority to suspend licenses and issue punishments, the law does not outline official emergency procedures or expedited methods for handling shocks such as disinformation or hybrid threats over media.

While the law is generally a positive step towards creating resilience against disinformation, in its current shape, it remains largely ineffective against the primary channels of modern disinformation and hybrid threats. Its limited scope (excluding online media), coupled with the other weaknesses mentioned above, means it cannot be relied upon as a central pillar of Kosovo's efforts to counter disinformation.

Code of Ethics of the IMC (IMC-2016/03)[54]

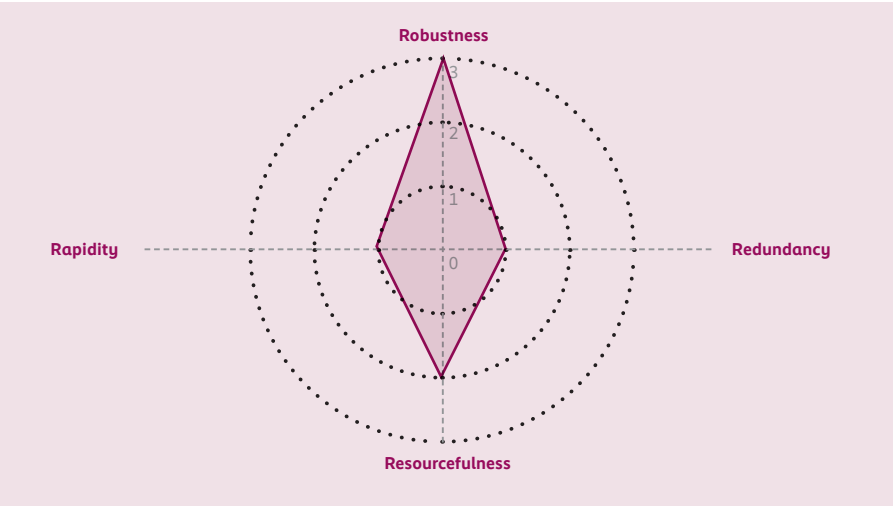


Figure 9: 4Rs Framework Assessment of Code of Ethics. (Source: Own creation)

The IMC Code of Ethics, although important in establishing professional standards, demonstrates moderate resilience against disinformation and hybrid threats, receiving a score of 58%.

As visualised in Fig. 9, its robustness is high (score 3) because it sets legally binding requirements such as accuracy, fairness and the correction of inaccurate content. The Code is supported by the Law on IMC and, through it, can enforce sanctions like fines or license suspensions for broadcasters, ensuring accountability and promoting systemic stability. The redundancy is weak (score 1); although sanctions are legally binding and do not require further legal actions, the system lacks fallback mechanisms if the IMC itself is unable to act or is compromised. Furthermore, the appointment of the IMC board by the National Assembly also introduces a potential vulnerability to political influence, limiting resilience due to reliance on a single actor without protective oversight. The resourcefulness is moderate (score 2) as the measure includes accountability mechanisms like the right of reply and correction. However, it lacks collaborative frameworks that would help media adapt to evolving hybrid threats or disinformation tactics beyond traditional broadcasting ethics. Its rapidity is also weak (score 1) with few procedural timelines (like the seven day limit for the right to reply), it does not offer emergency measures, expedited reviews or fast-track enforcement for urgent situations.

The effectiveness of the Code is closely tied to the Law on the IMC, which limits its applicability to licensed audiovisual media, excluding the online sphere where much of the disinformation occurs. The Code needs significant modernisation to expand its mandate to the online sphere, accompanied by new measures to enhance its independence, create redundancies and create collaborative response mechanisms.

Press Code for Kosovo of the Press Council of Kosovo

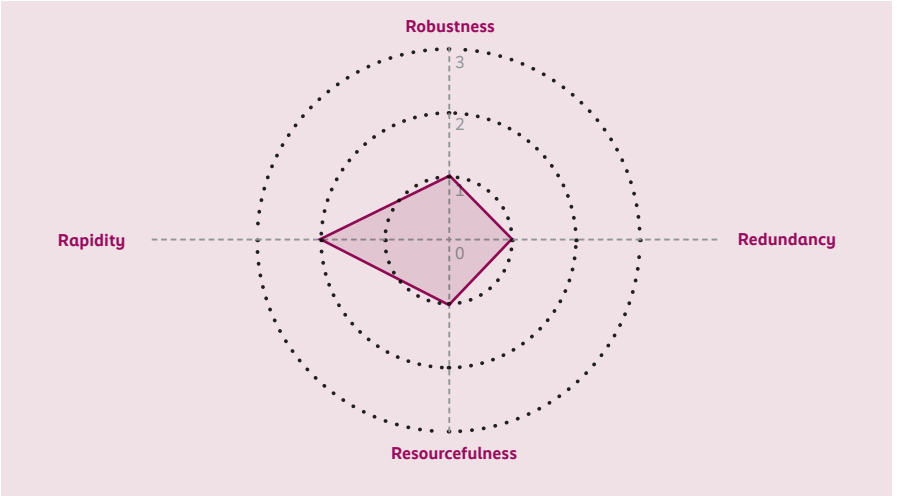


Figure 10: 4Rs Framework Assessment of Press Code for Kosovo. (Source: Own creation)

The Press Code is a self-regulatory ethical framework for journalists, editors and publishers, and it is important as it is the only regulatory policy that can apply to online platforms/media. The code received a score of 42% indicating a low resilience against disinformation and hybrid threats.

Fig. 10 demonstrates its limitations. Its robustness is weak (score 1); although the code promotes professional ethics such as truthful reporting and non-discrimination, the enforcement of these rules relies on voluntary compliance and peer control rather than legal authority. Its redundancy is also weak (score 1); while requirements for fairness, balanced reporting, and the right to reply promote a degree of ethical redundancy and information diversity, it does not outline systematic defences against disinformation, such as cooperative fact-checking networks or protocols for maintaining information integrity across multiple platforms during a crisis. Resourcefulness is also weak (score 1) as it lacks provisions for broader institutional adaptation or technological innovation essential for adaptive resilience. Its rapidity is moderate (score 2) as it emphasises prompt corrections of false information, but it does not establish emergency procedures or real-time systems to quickly counter coordinated attacks or visual disinformation campaigns.

The Press Code's main limitation lies in its self-regulatory nature, which is insufficient against external, often state-backed, hybrid threat actors who do not adhere to such ethical standards. Its primary contribution stands on fostering ethical conduct within the professional journalistic community, which is indeed a valuable component of a healthy information ecosystem. However, the code serves as a good foundational ethical layer upon which more robust regulatory or co-regulatory measures could be built, ensuring efforts to counter disinformation do not (negatively) impact journalistic freedoms.

Digital Agenda for Kosovo 2030[55]

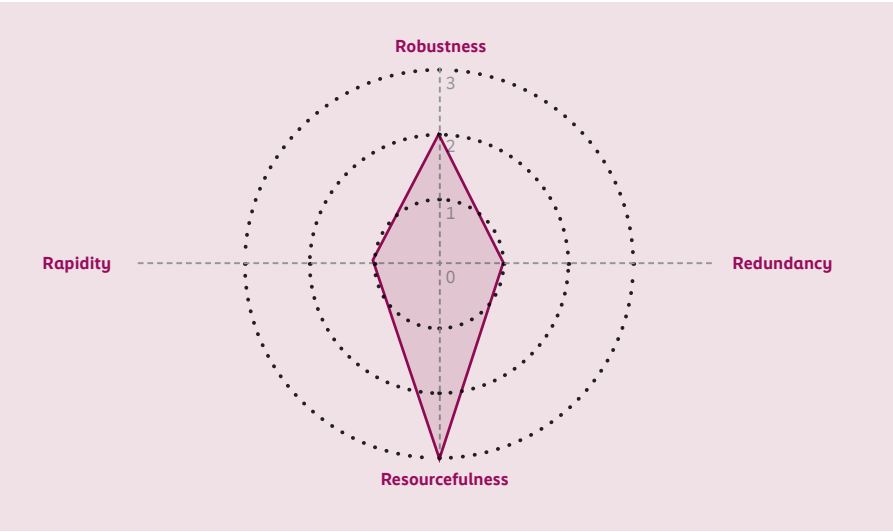


Figure 11: 4Rs Framework Assessment of Digital Agenda for Kosovo 2030. (Source: Own creation)

The Digital Agenda, although it is not a dedicated strategy to counter disinformation, includes elements relevant to building resilience against disinformation and hybrid threats, assessed with a score of 58%.

The strategy demonstrates a moderate robustness (score 2); it acknowledges disinformation and hybrid threats within the context of cyber resilience and assigns institutional responsibilities (CSA, Ministry of Internal Affairs), aiming to align with EU and NATO standards. However, it does not mention any enforceable legal framework directly addressing disinformation or hybrid threats. Redundancy is weak (score 1); although it encourages independent media and public awareness, specific institutional or systemic fallback measures are not present. Its resourcefulness is high (score 3) as it promotes collaboration between government, foreign partners, media and CSOs, and it also facilitates adaptive responses through education campaigns and capacity building initiatives. Rapidity is weak (score 1); although it mentions early warning systems and threat monitoring, formal rapid response methods or fast-track procedures are absent.

The Digital Agenda can contribute positively to long-term resilience by enhancing digital literacy. However, more concrete measures in these directions are required, especially in terms of formal education on disinformation and media literacy skills in high schools and higher education.

Discussing the Findings

The 4Rs assessment of Kosovo's regulatory framework reveals a fragmented and underdeveloped framework for countering the level of disinformation and hybrid threats the country has, and continues to face. With an **overall 59% resilience score (moderate resilience)**, the regulatory framework shows strengths (especially in the cybersecurity domain); however, systemic resilience is significantly undermined due to critical gaps in all four dimensions of the 4Rs framework.

Table 5: Total Score of Assessed Policies

#	Policy	Score	Max points
1	Law No. 02/L-65 - Civil Law Against Defamation and Insult	2	
2	Law No. 06/L-082 on Protection of Personal Data	10	
3	Law No. 08/L-173 on Cyber Security	9	
4	Administrative Instruction No.04/2024 on Registry of Cyber Incidents	7	
5	Administrative Instruction No.05/2024 on Registry of Cyber Security Risks and Threats	10	
6	National Cyber Security Strategy 2023 - 2027	10	132
7	Kosovo Security Strategy 2022 - 2027	6	
8	Law No. 04/L-044 on the Independent Media Commission (IMC)	6	
9	Code of Ethics of the IMC (IMC-2016/03)	7	
10	Press Code for Kosovo of the Press Council of Kosovo	5	
11	Digital Agenda for Kosovo 2030	7	
Total		79	59%

Robustness issues raise major concerns when trying to address or counter disinformation and hybrid threats. The outdated Law on IMC, critically failing to include online media, leaves a significant regulatory gap. Furthermore, policies designed for traditional media or ethical guidance, such as the IMC Code of Ethics and the Press Code of Kosovo, demonstrate very low to low resilience scores against coordinated disinformation campaigns, lacking the necessary legal authority, scope and enforcement mechanisms. Even policies with inherent robustness, like the Data Protection Law, have limited application in countering disinformation.

Furthermore, the assessment consistently exposed a minimal systemic redundancy in the regulatory framework. Generally, there is prevalent over-reliance on single institutions within their respective domains (e.g. IMC for audiovisuals, CSA for cybersecurity, PCK for online media ethics) without clearly defined or adequate resource backup systems, alternative operational protocols or contingency plans to address institutional failure or overload during crisis. Other overarching or strategic documents, such as the Kosovo Security Strategy, acknowledge coordination gaps but generally fail to outline concrete fallback mechanisms. This lack of redundancy in the regulatory framework increases its vulnerability to disruptions due to disinformation and hybrid threats.

Adaptability and multi-stakeholder collaborative approaches are also underdeveloped, which leads to an overall limited systemic resourcefulness. Although instruments like the National Cybersecurity Strategy and Digital Agenda promote multi-stakeholder approaches, this is not reflected across the rest of the regulatory framework. Most of the laws tend to prioritise administrative structures over fostering innovation or mandating broad collaboration. Most importantly, Kosovo lacks an overarching national strategy or an institutionalised platform dedicated to fostering collaboration specifically to counter disinformation and hybrid threats among diverse actors, including governments, security agencies, policymakers, CSOs, academia and tech platforms. Additionally, the lack of a national strategy to increase media literacy (especially within formal education) represents a major deficit in building the societal resilience to resist manipulation and disinformation campaigns.

The assessment also emphasises the insufficient rapidity present across the board. The speed of disinformation (especially through online platforms) significantly outpaces the response capacity provided within the policies of the current regulatory framework. Most policies assessed lack specific provisions for rapid detection, real-time analysis capabilities, fast-track decision-making processes, or protocols for emergency coordination. Even the policies which demonstrate a moderate rapidity in certain aspects (e.g. the Law on Cyber Security) lack defined crisis action plans for a fast and coordinated reaction. Policies which are reliant on self-regulation (e.g. PCK) or those that are reliant on judicial processes (e.g. Defamation law) are too slow to be effective against disinformation. This systematic lack of rapidity leads to interventions being too little, too late to effectively mitigate or address the impact of disinformation and hybrid threats.

"The speed of disinformation (especially through online platforms) significantly outpaces the response capacity provided within the policies of the current regulatory framework."

Another important finding worth noting is the significant degree of fragmentation and lack of strategic cohesion among the various policies assessed. For instance, although the efforts made in the cybersecurity domain are relatively advanced, they are poorly connected to the regulatory framework for the information space. Or in the case of the Kosovo Security Strategy, which fails to effectively integrate or guide specific measures countering disinformation as a security risk, creating a strategic disconnect. Similarly, the Digital Agenda, although it mentions digital literacy goals, lacks strong operational links to security frameworks or regulatory enforcement concerning disinformation.

Conclusions and Recommendations

Addressing disinformation and hybrid threats presents a complex challenge, requiring careful navigation to avoid infringing upon fundamental rights like freedom of expression and media freedom. However, the preceding analysis and other studies conducted clearly demonstrate significant vulnerabilities within the current regulatory framework, necessitating strategic and holistic interventions that move beyond the existing fragmented efforts. The following recommendations aim to advance the regulatory framework, learning from best practices, particularly the ones in the EU, concerning digital services and disinformation, while adapting them to the specific context of Kosovo.

The assessment consistently revealed critical weaknesses across the 4Rs of resilience. To build a more resilient framework, a primary focus must be on modernising the regulatory framework for the information space in Kosovo, particularly concerning online media. This necessitates a comprehensive reform, by substantially amending the Law on the IMC to grant it a clear, expanded mandate covering online media (news portals and other online platforms) with adequate resources and independence. This reform body is crucial for providing institutional strength where it is currently lacking.

"Building societal resilience is probably the most problematic part as it requires dedicated long-term investment."

Building on the reform of the Law on IMC, it is crucial to adopt specific legislative measures focused on enhancing transparency and accountability in the online space, drawing particular lessons from the EU's Digital Services Act (DSA) and the Strengthened Code of Practice on Disinformation. Instead of creating laws and regulations that could attempt content censorship, raising significant freedom of expression concerns, legislation should focus on the dynamics of disinformation spread. This could include (i) mandating transparency for online political advertising, for example, by requiring platforms operating in Kosovo to maintain publicly accessible ad repositories similar to those required under the DSA, (ii) clear labeling requirements for state-sponsored content and (iii) establishing mechanisms to address coordinated inauthentic behaviour (like bot networks).

Additionally, adopting a proportionate risk-based approach for online platforms could be useful. By doing this, online platforms will be required to

assess and mitigate systemic disinformation risks (akin to DSA Article 34) under the oversight of IMC. Furthermore, exploring a co-regulatory model, blending formal regulation with structured self-regulation inspired by the EU's Strengthened Code of Practice, could also foster industry responsibility. Key adaptable commitments include the demonetisation of disinformation, enhancing service integrity against fake accounts/bots, empowering users, and facilitating secure data access for researchers studying disinformation, while respecting data protection laws, in line with the GDPR.

Beyond specific regulation related to media and online platforms, enhancing strategic cohesion and institutional capacity across public institutions is crucial. The Kosovo Security Strategy needs to be revised to integrate actions to counter disinformation and hybrid threats as core priorities. Furthermore, this instrument as an overarching strategy should clearly define cross-agency roles and ensure effective connection with other strategies (e.g. the National Cybersecurity Strategy). Similarly, the operational capacity of all relevant institutions must be enhanced through adequate funding, specialised training and technical resources, while protecting their independence.

Building societal resilience is probably the most problematic part as it requires dedicated long-term investment. On this goal, the development and sustained implementation of a comprehensive National Media and Information Literacy Strategy is paramount. Furthermore, the integration of this strategy and its actions across the education system and supporting public programmes (non-formal education) to empower citizens with media literacy skills and countering disinformation would be necessary. Fostering a pluralistic and sustainable independent media environment through transparent public funding mechanisms and support for quality journalism would provide citizens with diverse, reliable information sources, acting as a natural buffer against disinformation and hybrid threats.

Throughout this process, strengthening international cooperation and alignment remains crucial. Continuous engagement with the EU, NATO, and bilateral partners for intelligence sharing, adopting best practices, and harmonising Kosovo's framework with evolving international standards, particularly learning from the implementation of the DSA and related initiatives, will be key to building effective, modern, and rights-respecting resilience against disinformation and hybrid threats.

As mentioned throughout the paper, addressing these challenges requires strategic and holistic interventions that go beyond the current fragmented efforts. Moving forward, a dedicated and sustained commitment to implement reforms will be essential to properly enhance the capacities of institutions to navigate and counter disinformation and hybrid threats.

References

1 Classified based on the OECD (2014) "Guidelines for Resilience Systems Analysis: How to Analyse Risks and Build a Roadmap to Resilience". OECD Publishing.

2 Vishnska, I. (2023) "Geopolitical Perspective of Disinformation Flows in the Western Balkans". Metamorphosis Foundation for Internet and Society.

3 NDI (2022) "Information Integrity in Kosovo: Assessment of the Political Economy of Disinformation". National Democratic Institute.

4 Zamfir, R. (2020) "Risks and Vulnerabilities in the Western Balkans". NATO Strategic Communications Center of Excellence.

5 Burmester, I, et al., (2025) "Political Threat Assesment in Eastern Neighbourhood & Western Balkan Countries". ReUnir Working Paper.

6 Ibid, 2.

7 Ibid, 3

8 Ibid 2.

9 EUvsDinfo (2019) "700 False New Stories in Serbian Tabloids in 2018". EUvsDisinfo.

10 Disinfo (2022) "Misnformation of Public Opinion in Serbia as an Electoral Strategy". Sbunker

11 Zamfir, R. (2019) "Propaganda Made-to-Measure: Dimensions of Risk and Resilience in the Western Balkans". Global Focus/The Balkan Trust for Democracy.

12 Prime Minister Office (2024). "Agreement signed with Turkish state-owned defense industry producer "Makine ve Kimya Endüstrisi". Last accessed: May 5, 2025.

13 Die Morina (2018) "Kosovo Minister and Spy Chief Sacked Over Turkish Arrests". BIRN/ Balkan Insights (Last accessed: May 5, 2025).

14 Shaban Mexharraj (2025) "'The Six Against Turkey' Does Not Give Up on Prizren, Officials Remain Silent". Koha.

15 Ibid.

16 Ibid, 11.

17 Belt and Road Initiative (known also as the One Belt One Road) is an international infrastructure development strategy implemented and funded by the Chinese Government. See more at: Belt and Road Portal.

18 Gashi, K. (2024) „Institutional Unpreparedness: Kosovo's Challenge Against Disinformation". In Balažič, P. & Brglez, L (2024) "The Mirage of Truth: Complexities and Challanges of Disinformation in the Western Balkans". Center for European Perspective.

19 Disnfo (2022) "Under the Surveillance of Suspicious Chinese Cameras". Sbunker

20 Mehmeti, J (2021) "National Regulatory and Self-Regulatory Framework Against Hate Speech and Disinformation". SEENPM, Peace Institute and Kosovo 2.0.

21 Ibid, 3.

22 ISD (2024) "Monitoring Influence & Disinformation Campaigns in the Western Balkans".

23 Constitution of the Republic of Kosovo.

24 Law No. 02/L-65 Civil Law Against Defamation and Insult. Article 14 and 15.

25 Law No. 04/L-137 on the Protection of Journalism Sources.

26 Law No. 06/L-085 on Protection of Whistleblowers.

27 Law No. 06/L-081 on Access to Public Documents.

28 Law No. 06/L082 on Protection of Personal Data.

29 Ibid, 3.

30 Law No. 04/L-044 on the Independent Media Commission. Article 3(2).

31 Ibid, 3.

32 Ibid, 2.

33 Ibid, 30. Article 11.

34 Press Code of Kosovo, March 2005.

35 Ibid, 3.

36 Ibid.

37 Law No. 08/L-173 on Cyber Security.
38 Ibid, Article 12, and 21.

39 Ibid, 14.

40 For more information regarding the methodology, please refer to the methodology section.

41 Ibid, 37. Article 12-16 and 24.

42 Ibid. Article 9.

43 Ibid. Article 6.

44 Admnistrative Instruction No.04/2024 on Registry of Cyber Incidents. Article 4(5).

45 Ibid. Art. 4(2)

46 Ibid. Art 5(2)

47 Ibid. Art 5(1) and (3)

48 Administrative Instruction No. 05/2024 on Registry of Cyber Security Risks and Threats. Articles 1-7.

49 Ibid. Article 2 and 8.

50 Government of Republic of Kosovo (2023). National Cyber Security Strategy 2023 - 2027

51 Government of Republic of Kosovo (2022). Kosovo Security Strategy 2022 - 2027.

52 Ibid, 30. Article 1 -4.

53 Ibid. Art. 8

54 Independent Media Commission. Code of Ethics for the IMC.

55 Government of Republic of Kosovo (2023). Digital Agenda for Kosovo 2030.

Friedrich Ebert Stiftung