International Journal of Innovative Technology and Interdisciplinary Sciences
https://journals.tultech.eu/index.php/ijitis
ISSN: 2613-7305
Volume 9, Issue 4
DOI: https://doi.org/10.15157/IJITIS.2026.9.4.2308-2351
Received: 18.07.2026; Revised: 26.09.2026; Accepted: 24.10.2026

Research Article

Technology-Enabled Hybrid Threats and Institutional Resilience in Kosovo: A Qualitative Study of Security Professionals

Refik Ramadani , Buen Bajrami*
Faculty of Computer Science, Public University "Kadri Zeka", Gjilan, Kosovo
***buen.bajrami@uni-gjilan.net**

Abstract

Hybrid threats exploit technological, informational, political, and organizational instruments to capitalize on existing vulnerabilities while complicating detection, attribution, and response. The current study investigates how professionals working in security-related fields in Kosovo perceive the role of digital technologies in facilitating hybrid threats, the institutional vulnerabilities that increase exposure to such threats, their implications for political stability and public trust, and the measures required to strengthen institutional resilience. An exploratory qualitative research approach was adopted with the involvement of nine purposively chosen professionals working in the fields of cybercrime investigation, prosecution, journalism, security, and other institutional sectors. Data were collected in March 2026 using an asynchronous online qualitative questionnaire with five open-ended questions. The analysis identified five thematic strands, including hybrid warfare as an evolving security challenge, technology as an enabling mechanism, institutional and informational vulnerabilities, political stability and public trust, and multidimensional priorities for strengthening institutional resilience. The framework provides a formalization of a socio-technical analytical approach where technological enablers increase the operational potential of hybrid threats, institutional and communication vulnerabilities determine the risk of being exposed to such threats, and the effects of those go beyond the technical aspect and include the issue of credibility of information and political stability. The notion of resilience, thus, requires comprehensive technological, organizational, informational, legal, educational, and cooperative efforts.

Keywords: Hybrid Warfare; Cybersecurity; Disinformation; Institutional Resilience; Western Balkans.

INTRODUCTION

Contemporary hybrid threats operate across technological, informational, political, economic, and institutional domains and often seek to exploit vulnerabilities without crossing a clear threshold into conventional armed conflict. The literature therefore treats

©2026 Authors. This is an Open Access article distributed under the terms and conditions of the Creative Commons Attribution 4.0 International License CC BY 4.0 (http://creativecommons.org/licenses/by/4.0).

hybridity less as the simultaneous presence of many instruments than as the coordinated use of different instruments against weaknesses in a target environment [1-5]. At the same time, recent scholarship warns against using the label so broadly that every cyber incident, disinformation campaign, or political dispute is treated as hybrid warfare [6-8]. This paper takes this warning to heart and employs the hybrid threat conceptual framework only when technology-mediated actions are associated with larger strategic, organizational, informational, or societal consequences.

Digital technologies enable a wider range of opportunities for hybrid actors through greater speed, scale, reach, anonymity, automation, and cross-border accessibility. Cyber operations can target institutions and their infrastructures, and platforms can increase the speed and amplification of the manipulation of information. These mechanisms are analytically distinct but can become mutually reinforcing when cyber, information, and political pressure are combined [4, 9-12]. The central issue is therefore not technology alone, but the interaction between digital capability and the vulnerabilities of the institutions and societies against which it is used.

The Western Balkans provide a relevant context for studying this interaction. Research on the region emphasizes structural vulnerabilities, contested political identities, institutional fragmentation, information manipulation, and exposure to external influence [12-16]. Kosovo is particularly relevant because security institutions, digital infrastructures, public communication, and contested political narratives coexist within a small and highly interconnected institutional environment. Existing regional research identifies cyber-enabled interference, disinformation, and influence operations, but less frequently examines how professionals from different security-related fields connect technological enablement, institutional vulnerability, public trust, and resilience in one analytical chain [12-16].

This leads to four connected gaps. First, the conceptual gap concerns the tendency to discuss cyber threats, information manipulation, institutional weakness, and resilience in parallel rather than as interacting elements of one socio-technical process. Second, the empirical gap concerns limited qualitative evidence from professionals working across cybercrime investigation, prosecution, security, media, and related fields in Kosovo. Third, the methodological gap concerns the limited use of transparent cross-domain qualitative coding to connect practitioner evidence with resilience frameworks. Fourth, the validation gap concerns the absence of a context-specific framework that is explicitly positioned against established approaches such as North Atlantic Treaty Organization (NATO) resilience guidance, the European Union (EU) Hybrid Toolbox, National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0, and the Hybrid CoE/JRC resilience ecosystem [10, 11, 17-19].

The present study does not claim to replace these established frameworks. NATO emphasizes continuity of government, essential services, civil preparedness, and national resilience; the EU Hybrid Toolbox emphasizes coordinated prevention, cooperation, stability, restriction, support, and recovery measures; NIST CSF 2.0 structures

cybersecurity risk outcomes; and Hybrid CoE/JRC work emphasizes systemic vulnerabilities, societal interdependencies, and whole of society resilience [10, 11, 17-20]. The contribution of this study is narrower: it uses professional perceptions from Kosovo to connect technological enablers, threat mechanisms, institutional vulnerabilities, societal effects, and resilience capacities in a single context-sensitive analytical model.

The aim of this study is to examine how technology enables hybrid threats in Kosovo, identify the institutional vulnerabilities that increase exposure, and determine which measures security professionals consider necessary for strengthening institutional resilience.

- RQ1. How do security-related professionals in Kosovo perceive the role of digital technologies in enabling contemporary hybrid threats?
- RQ2. Which technological, informational, and organizational vulnerabilities are perceived as increasing institutional exposure to hybrid threats in Kosovo?
- RQ3. How do professionals understand the relationship between institutional vulnerabilities, public trust, and the security effects of technology-enabled hybrid threats?
- RQ4. Which technological, organizational, legal, informational, and societal measures are considered most important for strengthening institutional resilience?

Research Hypotheses

Based on the theoretical framework and the research questions, the following hypotheses are proposed:

- H1: Digital technologies are perceived as increasing the operational capacity of hybrid threats particularly when they enable multiple cyber, informational, and influence mechanisms to operate rapidly, remotely, and across institutional or geographical boundaries.
- H2: Institutional exposure to technology-enabled hybrid threats is perceived to increase when technological vulnerabilities coexist with weak inter-institutional coordination and limited strategic communication capacity.
- H3: The perceived effects of technology-enabled hybrid threats extend beyond technical disruption when cyber and information activities undermine information credibility, public trust, and institutional legitimacy, thereby increasing perceived risks to political stability.
- H4: Institutional resilience is perceived as stronger when cybersecurity capacity is combined with inter-institutional coordination, strategic communication, legal and investigative capability, media and digital literacy, and international cooperation than when resilience is approached primarily through technical cybersecurity measures.

These hypotheses cover different yet connected aspects of the proposed socio-technical approach to hybrid activities. H1 centers on the role of technology as a means of enabling

the execution of hybrid activities, especially due to the rapidity, connectivity, scalability, and anonymity afforded by digitalized operations. Such an expectation aligns with scholarly descriptions of modern hybrid threats in terms of their greater dependence on cyber technology and information systems that enable them to conduct operations outside of traditional geographical and institutional borders.

H2 departs from the exclusive consideration of technological capability and brings in the interplay of technological factors with institutional contexts. Its main premise is that technological exposure does not automatically lead to institutional vulnerability. In other words, its implications may become more pronounced when technical vulnerabilities are coupled with weak coordination, poor information exchange, lack of preparation, or ineffective strategic communication. Hence, the hypothesis assumes that vulnerability is a socio-technical construct created by the interaction of technological and organizational aspects.

H3 deals with the wider implications of technology-enabled hybrid threats. In addition to interfering with the work of information systems or technical infrastructure, hybrid threats could also affect public trust in institutions, credibility of information, political stability, and society itself. The hypothesis therefore assumes that the implications of hybrid threats can transfer from the spheres of technology and information to the spheres of institutions and society, thereby making public trust an element of resilience.

H4 considers the multi-faceted nature of resilience. In case hybrid threats take advantage of vulnerabilities in technology, institutions, information, and society, resilience will not be possible without more than cybersecurity measures. The hypothesis therefore expects the participants to stress the importance of an array of factors including cybersecurity capability, coordination of institutions, preparedness in law, strategic communications, education/media literacy, and international cooperation. In this framework, resilience is understood as an institutional capability to prepare for, withstand, respond to, and recover from technology-enabled hybrid threats.

These hypotheses are treated as qualitative analytical expectations rather than statistically testable causal claims. Their purpose is to examine whether participants' accounts support specific relationships among technological enablement, institutional vulnerability, societal effects, and multidimensional resilience.

Contributions of the Study

This study makes three bounded contributions. First, it provides context-specific qualitative evidence from professionals working across cybercrime investigation, prosecution, security, media, and related institutional fields in Kosovo. This cross-professional perspective allows the study to examine how technological, organizational, informational, and societal dimensions of hybrid threats are interpreted across different areas of professional practice.

Second, the study contributes analytically by connecting technological enablers, hybrid-threat mechanisms, institutional vulnerabilities, effects on public trust and political

stability, and resilience measures within a single socio-technical analytical sequence. The contribution does not lie in proposing these individual elements as new constructs, but in examining how participants perceive them as interdependent rather than isolated dimensions of security.

Third, the findings identify a specific relational pattern within the Kosovo context: technological exposure is perceived as becoming more consequential when it coincides with weak institutional coordination and limited strategic communication, while resilience is understood as requiring the combined operation of technical, organizational, informational, legal, educational, and cooperative capacities. Public trust therefore emerges not only as a possible consequence of hybrid activity but also as a security-relevant dimension of institutional resilience.

The study does not claim to introduce a new universal theory of hybrid warfare, establish causal relationships, or provide statistical generalizability. Its novelty is therefore contextual and analytical: it provides practitioner-based evidence on how these dimensions are perceived to interact within Kosovo and organizes those relationships into a socio-technical framework that can be examined and validated in future research.

Literature Review

Hybrid warfare is the combination of regular and irregular techniques, as well as political, economic, information, criminal, and technological tools for the accomplishment of strategic aims, without having to resort solely to military confrontation. According to [5], the concept of hybrid warfare involves a combination of the employment of regular capabilities, irregular methods, terrorism, and criminal means in the same battle space. Likewise, [21] stress that the idea behind hybrid strategies is the utilization of vulnerabilities along with the blurring of the existing distinction between war and peace. From these definitions, it is evident that hybridity is more than simply the use of several tools at once. It is a strategy in which different tools interact and complement each other in the achievement of strategic aims.

Modern scientific sources confirm that hybrid warfare is a permanent component of today's international security environment. The application of hybrid strategies enables states and non-state entities to make political, economic, informational, and security-related expenses without escalating to conventional forms of warfare [1-4, 22, 23]. In turn, hybrid approaches are closely associated with grey-zone competition, strategic ambiguity, deniability, and the use of asymmetric vulnerabilities of political and institutional systems. The absence of escalation to conventional types of warfare makes it challenging to attribute and react to hostile actions because they may be individually small but create a cumulative impact. Thus, the efficiency of hybrid strategies often lies in the possibility of actors to use various means that make it difficult for institutions to detect, decide, and respond to actions.

The emergence of technology has significantly changed the extent, pace, access, and geographic range of hybrid activities. Technologies enable hostile entities to launch attacks

on government networks, databases, communications, and infrastructures without physically being present in the country where the attacks are launched. Digital monitoring and cyber espionage can help gather intelligence, while technologies such as artificial intelligence can automate the creation of information, its translation and dissemination. Such technologies can thus increase the quantity and speed of influence operations and expand their geographic range [4, 9, 24]. Thus, technology does not simply add new tools to the arsenal of hybrid actors but also alters the conditions in which hybrid threats are conducted and delivered.

However, the reliance on digital technologies leads to new vulnerabilities of institutions. Public sector organizations become more dependent on information systems and cloud services, digital identities, communication via the Internet and online public services. On the one hand, such reliance can bring many benefits, but, on the other hand, when appropriate protection measures are not taken, these dependencies can create weak points. Insufficient access control, outdated information systems, lack of monitoring and coordination of incident response can offer new opportunities for hybrid actors to exploit technology systems. Thus, technological resilience cannot be considered only from the point of view of technical cybersecurity issues.

From a socio-technical viewpoint, such vulnerabilities have a useful theoretical background because this perspective considers technological systems and organizations not as separate but as interdependent factors. Socio-technical studies stress that the performance, vulnerability, and resilience of a system are determined by interactions between technological infrastructure, organizational structure, people, and institutions. A socio-technical perspective is particularly applicable to technology-enhanced hybrid threats, since the role of technological exposure may become more significant when combined with poor coordination, communication, dependence, or a lack of institutional readiness [25-27].

In addition to the aspects described above, information warfare is another key component of hybrid conflicts. Disinformation can be employed to create uncertainty, increase polarization within politics and society, create a lack of trust in institutions, and delegitimize political decisions. Online environments have amplified the possibilities for such attacks, since the algorithms behind the recommendations in the digital space tend to prioritize content that is able to draw attention, arouse emotions, or stimulate high engagement among users [13, 15, 16, 24]. Media manipulation can be used in a hybrid environment not only by itself but also alongside cyber-attacks, leaks, espionage, and fake narratives to create an overall impression of institutional vulnerability or insecurity.

The consequences of disinformation go far beyond simply the spread of false or inaccurate information. Constant exposure to contradictory narratives could result in public cynicism, decreased trust in official sources, and ineffective communication by institutions. Citizens who are unsure about who is and who isn't a trustworthy source make it harder for institutions to communicate during security events, political crises, or moments of increased tensions. In this context, there exists a clear link between information

security and institutional resilience. Strategic communication and media literacy must be regarded not only as a means of communication or education, but rather as a tool within the field of security. Their relevance becomes especially apparent when hybrid actors try to capitalize on public mistrust, divisions, or political narratives [13, 15, 16, 24].

Research on information disorder provides a broader conceptual basis for understanding these effects by distinguishing among different forms of problematic and manipulative information and by emphasizing the wider consequences of polluted information environments. Such environments may affect not only the accuracy of individual messages but also institutional credibility, public trust, and the capacity of citizens to assess competing claims. From a resilience perspective, disinformation therefore represents not only a communication problem but also a potential institutional and societal vulnerability [28, 29].

Cognitive-warfare research further extends this perspective by emphasizing that contemporary influence activities may target perceptions, decision-making, behaviour, and societal trust rather than only information systems or digital infrastructure. Digital platforms, algorithmic amplification, and technologically mediated information environments can increase the reach and persistence of such influence activities. This perspective reinforces the relevance of information credibility, public trust, and cognitive resilience as security-related dimensions within the wider analysis of technology-enabled hybrid threats [30].

Hybrid tactics are most effective where the inherent vulnerability of institutions and societies is capitalized upon. Studies analyzing the Western Balkans region consider political divisions, poor coordination between institutions, contestation of history, lack of cybersecurity capacities, and dependence on foreign information environments to be among such vulnerabilities [13, 14]. Vulnerabilities such as these can help strengthen the effects of hybrid tactics since opposing forces do not need to initiate tensions but rather utilize the inherent tension in political, institutional, or social realms. Thus, resilience is understood as the ability of institutions to prepare for, endure, react to, and recover from hybrid pressures without affecting their functionality and legitimacy.

Consequently, institutional resilience cannot be confined only to cybersecurity infrastructure, which implies that institutional resilience consists of secure IT systems, trained staff, availability of threat intelligence, good incident response capabilities, communication capabilities, legal authority, cooperation with the media, and raising public awareness. In this regard, these factors are interrelated since weakness in one dimension may neutralize the strength of another dimension. Thus, while a well-protected IT system may not be sufficient for the situation where there is no coordination among institutions, communication capabilities may not be sufficient when institutions do not have enough information and response capability. Moreover, it is necessary to emphasize international cooperation, which is fact that cyberspace operations, information warfare, and influence campaigns usually cross-national borders. Cooperation and coordination

among NATO, the EU, and regional institutions could help improve early warning and information sharing [20, 31].

Research on organizational resilience provides additional support for the process-based definition of resilience. Instead of considering resilience solely as the act of recovering from disruption, capability-based studies define resilience in terms of anticipation, coping, and adaptation. Such a definition is pertinent to the current study because resilience to technology-enabled hybrid threats entails more than technical protection; it involves organizational preparedness, coordination, learning, and adaptation processes [32].

The literature on cyber-resilience also considers more than prevention when defining the concept, focusing on the ability of organizations and systems to anticipate, tolerate, recover from, and adapt to cyber threats. Such a definition is pertinent to technology-enabled hybrid threats in that resilience is considered not in isolation but as a system capability. Thus, the current research is complemented by studies on cyber-resilience, which link protection, continuity, recovery, adaptation, and institutional learning to cyber threats [33, 34].

The Western Balkans constitute a crucial context in which one can study these issues since the region is still susceptible to geopolitical rivalries, external interference, disputed political identities, and unresolved historical and political disputes. The available literature describes the region as being fragile, which is associated with institutional fragmentation, disputed identity, unresolved political questions, and lack of integration with Euro-Atlantic institutions [13,14]. In this way, the above-mentioned structural factors can serve as an opportunity for hybrid actors to exploit political disagreements, informational vulnerabilities, and institutional fragility. Consequently, the technological threats to security in the region cannot be studied only from the technical perspective.

Kosovo is a prime example in the larger regional security framework of the Western Balkans. Based on previous research, the disinformation and influence campaigns in Kosovo have focused on politically charged narratives related to legitimacy, the Kosovo conflict, the Reçak massacre, the Kosovo Liberation Army, and NATO intervention [15, 16]. Such narratives show how historical, political, and informational factors can be combined within a larger framework of influence operations. It is also evident from the narratives mentioned above that hybrid threats are not limited to cyber infrastructure but can target collective memories, legitimacy, and perceptions.

Although the existing literature provides an important geopolitical and conceptual foundation, comparatively limited evidence is available regarding how professionals working within Kosovo assess technology-enabled hybrid threats, identify institutional weaknesses, and prioritize measures for strengthening resilience. Much of the existing literature focuses either on broader geopolitical dynamics, specific cyber risks, or information manipulation, while less attention is given to how these dimensions are perceived as interconnected by professionals operating within relevant institutional and security environments [13-16]. This represents an important empirical limitation because professionals working in cybercrime investigation, prosecution, security, media, and

related institutional areas may provide valuable insight into the practical interaction among technological threats, organizational weaknesses, public trust, and resilience measures.

According to the analysis of the literature discussed above, the current research uses an integrated socio-technical approach to assessing the nature of technology-driven hybrid threats and institutional resilience. Specifically, it is assumed that technological means enhance the level of operational capacities of hybrid actors, whereas these capacities become realized in terms of cyber, information, political, and influence mechanisms. Institutional vulnerability impacts the extent to which such mechanisms could produce tangible results, whereas the results themselves can be observed in the realm of security and in the sphere of society. Resilience measures are implemented in all these dimensions, enhancing prevention, preparedness, response, and adaptation.

The convergence of socio-technical systems, organizational resilience, cyber resilience, information disorder studies, and cognitive warfare concepts provides an additional theoretical background for this approach. Collectively, they indicate that technology-based hybrid threats should not be considered solely in terms of technological capacity or cyber risks. Their consequences depend on the interaction between technological systems, organizational readiness, the information context, coordination among institutions, public confidence, and resilience. In this regard, the current theoretical approach is based on these related theoretical concepts while being applied to the interaction between hybrid threat mechanisms and institutional resilience [25-30, 32-34].

The proposed framework is structured as an analytical sequence rather than as a statistically validated causal model. It contains five interconnected constructs: technological enablers, hybrid-threat mechanisms, institutional vulnerabilities, security and societal effects, and resilience capacities. Technological enablers refer to the digital capabilities that expand the speed, reach, accessibility, anonymity, and scalability of hybrid activities. Hybrid-threat mechanisms refer to the concrete forms through which such capabilities may be used, including cyberattacks, cyber espionage, information manipulation, disinformation, and related influence activities.

Institutional vulnerabilities represent the conditions that may increase the effect of these mechanisms, including weak technical protection, insufficient inter-institutional coordination, limited information exchange, and ineffective strategic communication. Security and societal effects refer to the perceived consequences that may extend from technical disruption to reduced information credibility, weakened public trust, political polarization, and institutional instability. Resilience capacities include cybersecurity preparedness, incident-response capability, institutional coordination, strategic communication, legal and investigative capacity, media and digital literacy, and international cooperation.

The model proposes four analytical relationships. First, technological enablers increase the operational capacity of hybrid-threat mechanisms. Second, institutional vulnerabilities condition the extent to which these mechanisms may translate into wider institutional

effects. Third, technical and informational effects may extend into societal outcomes such as reduced public trust and political instability. Fourth, resilience capacities operate both as protective mechanisms and as a feedback process through which institutions can reduce exposure, improve preparedness, and adapt to subsequent threats. These relationships are examined qualitatively in the present study and are intended for future empirical validation rather than presented as established causal effects

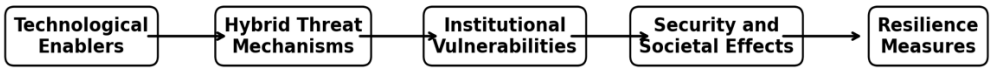


Figure 1. Socio-Technical Analytical Model of Technology-Enabled Hybrid Threats, Institutional Vulnerability, Societal Effects, And Resilience Capacities

Figure 1 should be regarded more as an analytical framework rather than a deterministic cause-and-effect illustration. Arrows show the manner in which technological capabilities contribute to the use of hybrid-threat mechanism, the influence of institutional vulnerabilities on outcomes, as well as the extent of their effects from interference with technical activities to the reliability of information, trust, and stability. Resilience capability is a component of the framework in terms of reducing exposure, effect propagation, coordination, and learning. The feedback process occurs due to the ability of experience to affect future readiness, coordination, communication, and technical protection.

Stages of the framework need not necessarily flow into one another but are analytically created paths that should be empirically verified.

The suggested model is an analytic, but not a mathematical, one. In view of the exploratory nature of this study, the associations between variables such as technology enablers, mechanisms of hybrid threats, institutional vulnerabilities, social impacts, and resilience capabilities cannot be shown through formulas, coefficients, and path estimates. The relationships between them are specified directionally and can be further examined quantitatively in future research.

METHODOLOGY

Research Design

The study adopted an exploratory qualitative research design that seeks to investigate the perceptions held by security-related professionals about the technology-enabled hybrid threats, institutional vulnerabilities and measures required to increase the resilience of institutions. The reason why the researchers opted for a qualitative approach is that the study involves the interpretation of security issues that occur within certain institutional contexts. This means that the study does not involve statistical analysis of predetermined variables. Considering this, the research questions developed sought to identify the

perceptions that the respondents hold about the use of technology in current hybrid threats, their institutional and information vulnerabilities and resilience measures.

In the study, the combination of a comprehensive review of literature on an academic and policy level as well as primary data gathered from experts in security-related fields was used. While the literature review formed a theoretical basis for comprehension of hybrid warfare, technology-based threats, vulnerabilities of institutions, disinformation, and resilience, the empirical part included relevant insights into those concepts in the context of Kosovo. The analysis was framed within the socio-technological approach that was formulated in the theoretical part and considered all these factors interrelated.

The study should be understood as exploratory rather than statistically generalizable. Its purpose was not to estimate the prevalence of views within Kosovo's security sector or to establish causal relationships among variables. Instead, it sought to identify recurring patterns, areas of agreement and divergence, and relationships among the themes emerging from participants' written responses. The research hypotheses were consequently evaluated through qualitative thematic evidence rather than inferential statistical testing.

The study was designed as an exploratory qualitative investigation rather than as a quantitative or mixed-methods study. Accordingly, the numerical information reported for participant characteristics is descriptive only and is not used for inferential statistical testing. Given the purposive sample of nine professionals and the qualitative nature of the data, inferential statistics, effect-size estimation, reliability coefficients for survey scales, and predictive modelling were outside the scope of the research design.

Participants and Sampling

The sample comprised nine individuals, professionals in their respective areas with exposure to various aspects related to cybersecurity in Kosovo. Participants in this study came from backgrounds including cybercrime investigation, prosecution, journalism, and security, and others working within security-related institutional departments. Purposive expert sampling was used because the study required participants who would be able to assess certain issues concerning cybersecurity, investigations, information environment, public communication, security, or any resilience matters in institutions in relation to their professional exposure to these matters.

Eligibility in the sampling process was based on participants' exposure to these issues, whether directly or indirectly as part of their profession. Individuals with no professional exposure to these issues were not within the scope of this study. The resulting sample thus comprised several professional viewpoints rather than institutional membership. This was important in the study since technology-enabled hybrid threats can encompass technical, legal, informational, investigative, and institutional issues at once.

To ensure the anonymity of the information gathered, participants were given anonymized labels from P1 to P9. Professional background in terms of affiliation to a certain institution and role within this institution along with years of work experience were

only provided at the aggregate level when necessary to prevent identification of the participants due to the small sample size. In addition, it should be noted that this study does not try to obtain a statistically representative sample of professionals employed by the security institutions of Kosovo.

Research Instrument

Data were gathered through an online qualitative questionnaire based on five primary open-ended questions. The survey was created based on the study's research questions and conceptual framework to elicit participants' professional interpretations of technology-driven hybrid threats and institutional resilience. The five main issues covered were: definition and perception of hybrid warfare in Kosovo; role of technology in enabling cyber and information warfare; organizations and institutions that are perceived as being particularly vulnerable; impact of cyberattacks and disinformation on political stability and trust in institutions; and actions needed to increase institutional resilience.

Open-ended questions were used as they provided participants with the opportunity to freely voice their opinions without being limited by the set response options. Such an approach is relevant for an exploratory study involving participants' perceptions. At the same time, all participants were given the same set of core questions.

The instrument was developed based on analytical dimensions that were specified in advance on the basis of the objectives of the research. These dimensions include an understanding of hybrid warfare, the technological component, institutional vulnerability, consequences for political stability and confidence in authorities, and resilience. Thus, the instrument helped build a link between the research questions, the theoretical framework, and the coding procedure.

It is important to mention that due to the asynchronous, written submission of responses via Google Forms, the instrument cannot be considered a traditional face-to-face or synchronous semi-structured interview as there was no real-time interaction between the interviewer and respondent while collecting data. This methodology can instead be regarded as an asynchronous qualitative online questionnaire.

Data Collection Procedure

The data collection process was carried out in March 2026 via Google Forms. The link to the questionnaire was sent to the targeted participants using digital platforms. The participants answered the five questions independently in written form. No audio or video recordings were made since all the data were collected in written format.

Prior to answering the questions in the questionnaire, the participants were briefed on the purpose of the research, the voluntary nature of participation in the study, the confidentiality of the responses, and their right to withdraw from the study. The participants gave their answers using the digital platform without providing any information that would identify them during the data-analysis process.

Each participant was assigned an anonymous code ranging from P1 to P9. These identifiers were subsequently used when presenting representative excerpts in the Results section. The responses were organized in a structured format that enabled comparison across participants and across the five analytical dimensions of the questionnaire. Personally, or institutionally identifying information was not used in the presentation of qualitative quotations.

The asynchronous written format offered participants the opportunity to formulate their responses without the time pressure associated with synchronous interviews. However, it also limited the researchers' ability to conduct immediate probing, request clarification in real time, or explore unexpected responses through additional follow-up questions. This methodological characteristic is acknowledged when interpreting the depth and scope of the findings.

Data Analysis

The written responses were analyzed manually using thematic analysis. The analysis began with repeated reading of all responses to familiarize the researchers with the data and identify recurring concepts relevant to the research questions. During the initial coding stage, segments of participants' responses were assigned descriptive codes reflecting the issues expressed in the data. These included hybrid pressure, cyberattacks, cyber espionage, disinformation, technological enablement, institutional weaknesses, inter-institutional coordination, strategic communication, political stability, public trust, and resilience measures.

The first author conducted the initial coding. After the initial codes had been identified, conceptually related codes were compared and grouped into broader analytical categories. For example, references to cyberattacks, cyber espionage, remote access, information gathering, and rapid dissemination were grouped within categories related to technological and informational mechanisms. References to insufficient technical protection, weak institutional coordination, limited information exchange, and inadequate strategic communication were grouped within categories related to institutional and information-space vulnerabilities. In the same way, references to declining trust, reduced information credibility, polarization, and instability were grouped as societal and institutional effects, while cybersecurity preparedness, coordination, strategic communication, legal and investigative capacity, media literacy, and international cooperation were grouped as resilience-related capacities.

These categories were subsequently compared across the participants' responses and organized into five overarching themes: (1) hybrid warfare as a current and evolving security concern; (2) technology as an operational enabler; (3) institutional and information-space vulnerabilities; (4) effects on political stability and public trust; and (5) multidimensional priorities for institutional resilience. The analytical process therefore progressed from participant statements to initial codes, from related codes to broader categories, and from categories to overarching themes.

In a further analytical stage, the five themes were examined in relation to one another rather than treated only as separate descriptive findings. Technology was interpreted primarily as an operational enabler of cyber and information mechanisms, while institutional and communication weaknesses were interpreted as conditions that could increase exposure to such threats. The perceived consequences extended beyond technical disruption to information credibility, public trust, and political stability. Resilience was consequently interpreted as a multidimensional response involving technological, organizational, informational, legal, educational, and cooperative capacities. These relationships provided the analytical basis for the socio-technical framework developed in the study.

The second author reviewed the initial codes, analytical categories, and final themes against the original written responses. Where differences in interpretation occurred, the relevant responses were re-examined, and the classifications were discussed until agreement was reached. This procedure represented a consensus-based review rather than independent double coding. Therefore, Cohen's kappa or another intercoder-reliability coefficient was not calculated.

No qualitative data-analysis software was used. Coding, categorization, and thematic comparison were conducted manually using structured tables and systematic comparison of the written responses. The final themes were subsequently examined in relation to RQ1-RQ4 and H1-H4. The purpose of this stage was not to conduct statistical hypothesis testing, but to assess whether the qualitative evidence was consistent with, partially consistent with, or insufficient to support the theoretically derived expectations. Differences in emphasis across professional perspectives were also considered where they were evident in the participants' responses.

Attention was also given to observations that differed from the dominant thematic patterns. However, because no formal negative-case analysis was conducted, the absence of explicit disagreement was not interpreted as evidence of complete consensus among the participants.

No inferential statistical tests were applied to the qualitative responses. Numerical information was limited to descriptive participant characteristics and, where appropriate, transparent cross-case summaries of qualitative patterns. Such descriptive summaries were used only to support qualitative interpretation and were not treated as statistical evidence of population-level relationships, effect sizes, or causal associations

To improve analytical transparency and reproducibility, the coding hierarchy used in the thematic analysis is presented in Appendix A. The codebook documents the progression from first-order codes to broader analytical categories and overarching themes, together with illustrative examples from the participants' written responses.

Trustworthiness

The credibility of the analysis was supported through comparison between participants' written responses and the reviewed literature, use of participants from

several professional domains, maintenance of a clear thematic structure, and inclusion of representative quotations. Dependability was strengthened by documenting the questionnaire dimensions and analytical steps. Confirmability was supported by distinguishing participant perceptions from the authors' interpretation. Transferability is limited to comparable institutional and geopolitical contexts and should not be understood as statistical generalization.

RESULTS

Participant Characteristics

The participants consisted of nine individuals who worked in various professional settings associated with security in Kosovo. Four individuals belonged to the Kosovo Police Cyber Crime Directorate, three others were associated with various security-related institutions, one individual was from the State Prosecutor's Office, and the remaining individual was from a media institution. Thus, the sample consisted of investigators, journalists, security officers, and other professionals as can be seen in Tables 1 until 3.

Moreover, the participants had varying levels of professional experience. Four participants had more than 15 years of professional experience, three participants had 6 to 10 years of experience, one had 11 to 15 years, and one had 1 to 5 years of experience. This gave a balanced view of the experiences of both highly experienced and less experienced professionals.

Table 1. Distribution of Participants by Institution

Institution	**n**	**%**
Kosovo Police - Cyber Crime Directorate	4	44.4
Other security-related institutions	3	33.3
State Prosecutor's Office	1	11.1
Media institution	1	11.1
Total	9	100.0

Table 2. Distribution of Participants by Professional Position

Professional position	**n**	**%**
Investigator	3	33.3
Journalist	3	33.3
Other	2	22.2
Security officer	1	11.1
Total	9	100.0

Table 3. Distribution of Participants by Professional Experience

Professional experience	n	%
1-5 years	1	11.1
6-10 years	3	33.3
11-15 years	1	11.1
More than 15 years	4	44.4
Total	9	100.0

Theme 1: Hybrid Warfare as a Present and Growing Threat

In general, participants considered hybrid warfare a multifaceted concept involving actions such as cyber-attacks, disinformation, political pressures, espionage, media manipulation, and many other actions of this sort. It appears that these activities are seen by participants not only as possible future threats but also threats already relevant to the security of Kosovo today.

It is worth mentioning that several participants noted that hybrid operations could be difficult to identify and fall below the threshold needed to trigger conventional responses. This uncertainty was seen by participants as an important aspect of modern hybrid threats, as it enables hostile activities to affect political, institutional, and societal conditions without direct engagement in military activity.

It should be stated that one of the participants described hybrid warfare as using "disinformation, sanctions, media and social networks for destabilization and creating tension" (P1). Another participant stressed the growing relevance of hybrid pressures due to the manipulations performed with the help of media and external politics (P2).

Theme 2: Technology as an Operational Enabler

Technology has proven to be another important concept mentioned by many participants while discussing hybrid threats. Technology was related to cyberattacks, cyber espionage, gathering sensitive information, attacks on public institutions, and rapid spread of disinformation. Social media sites are particularly noteworthy because of their ability to rapidly spread information around the globe.

Furthermore, the participants pointed out that technology has increased the operational reach of actors engaging in hybrid actions. Digital tools enable actors to remotely penetrate institutional structures, gather information, operate anonymously, and distribute information in large amounts within short periods of time.

For instance, one of the participants stated that "technology is one of the fundamental pillars of hybrid warfare in this age" (P3). Another participant mentioned that technological means provide an actor with opportunities to attack systems, gather information, and spread false information (P4). Participants also discussed the importance of algorithms in spreading politically divisive narratives. All of the above implies that technology was seen by participants not as a stand-alone threat but rather as infrastructure that enables hybrid activity.

Theme 3: Institutional and Information-Space Vulnerabilities

Several institutions and systems potentially exposed to technology-enabled hybrid threats were listed by the participants. These included government institutions, ministries, law-enforcement agencies, Kosovo Security Forces, media institutions, public communication systems, and digital communication systems. National-security-related institutions and public-communication-related institutions were frequently mentioned because an incident or disruption in these domains would influence not only institutional functioning but also its reputation and legitimacy.

It was also evident that vulnerability should not be seen as a technical problem alone. The responses referred to insufficient technical protection, poor coordination among institutions, lack of strategic communication, political polarization, and the weakness of public information systems as interrelated exposures.

As one participant said, "All institutions are vulnerable if technical protection, communication and coordination are not considered as a single security issue" (P5). There is a trend throughout the data in which both the technical and organizational weaknesses were perceived as interrelated problems.

Effects on Political Stability and Public Trust

The participants understood that cyberattacks, media manipulation, and disinformation could have an impact on political stability, institutional credibility, and public trust. In their responses, participants made it clear that the effects of hybrid threats could go beyond the actual disruption and affect people's perceptions of institutions, media organizations, and information provided by the authorities.

Disinformation was linked to confusion, polarization, decreased institutional credibility and diminished confidence in public communications. The participants noted that exposure to manipulated or conflicting information could make the work of institutions difficult since they would not be able to communicate effectively with citizens during times of uncertainty.

One participant mentioned that cyberattacks and disinformation campaigns could lead to the erosion of citizens' trust in institutions and the media (P6). Another participant pointed out that destabilization and political influence were among the goals of such actions (P7). This shows that public trust and political stability were considered crucial outcomes of technology-based hybrid activities by the participants.

Priorities for Institutional Resilience

Participants identified several priorities for enhancing the resilience of institutions against hybrid threats. These priorities mostly concerned the improvement of cybersecurity infrastructure, incident response capacity, preventive measures, strategic communication, media and digital literacy, law enforcement and investigative capacity, and international cooperation.

From the respondents' answers, it becomes clear that neither the institutions themselves nor technical aspects of cybersecurity are primarily seen by participants as the sources of resilience from hybrid threats. Rather, resilience is viewed as a phenomenon that requires a coordinated effort among institutions responsible for security, law enforcement, communication, education, media, and international cooperation.

Also, from the answers it became clear that technical security must be supplemented with effective communication with the public, legal and investigative capacity, education, and information exchange. International cooperation is especially relevant due to the cross-border nature of cyber and information-related threats. Overall, it can be concluded that the participants see resilience as a multidimensional effort requiring technology, organizations, information, law, education, and international cooperation.

Thematic Synthesis

Table 4 depicts the synthesis of themes identified in the participants' written questionnaire responses.

Table 4. Synthesis of Themes Identified in the Participants' Written Questionnaire Responses

Theme	Key subthemes	Analytical role in the framework	Illustrative participant evidence
Hybrid warfare as a current and evolving concern	Multidimensional pressure; below-threshold activity	Defines the broader threat environment	Hybrid tactics were perceived as already present in Kosovo
Technology as an operational enabler	Cyberattacks; espionage; platform amplification	Expands speed, reach, scale, and anonymity	Technology was described as a fundamental pillar of hybrid warfare
Institutional and information-space vulnerabilities	Weak protection; poor coordination; exposed systems	Conditions the extent to which hybrid mechanisms may generate wider effects	Institutions and public information systems were viewed as vulnerable
Effects on political stability and public trust	Disinformation; polarization; manipulated narratives	Represents institutional and societal consequences	Participants linked manipulation with confusion and declining trust
Multidimensional resilience	Cybersecurity; coordination; strategic communication; literacy; cooperation	Reduces exposure, limits propagation, and supports response and adaptation	Participants emphasized coordinated national and international action

Evidence Chain and Cross-Participant Illustration

To increase transparency between the participants' written responses and the analytical interpretation, Table 5 presents an evidence chain linking selected participant material to the corresponding first-order code, analytical category, overarching theme, and theoretical implication. Direct quotations are reproduced only where the original wording was retained in the dataset; other participant contributions are presented as attributed summaries rather than reconstructed quotations. The final column indicates how each evidence chain contributes to the socio-technical interpretation developed in the study.

Table 5. Analytical Evidence Chain from Participant Material to Code, Category, Theme, and Theoretical Implication

Participant	Participant evidence	First-order code	Analytical category	Theme	Theoretical implication
P1	"Disinformation, sanctions, media and social networks for destabilization and creating tension."	Multidimensional hybrid pressure	Threat characterization	Hybrid warfare as a current and evolving security concern	Hybrid threats are interpreted as multidimensional processes in which informational, political, and societal instruments may operate in combination rather than as isolated mechanisms.
P2	Emphasized media manipulation and external political pressure as elements of contemporary hybrid pressure.	Information and political pressure	Threat characterization	Hybrid warfare as a current and evolving security concern	Hybrid-threat analysis requires attention to the interaction between information manipulation and broader political pressure.
P3	"Technology is one of the fundamental pillars of hybrid warfare in this age."	Technology as enabling infrastructure	Technological enablement	Technology as an operational enabler	Technology functions primarily as an enabling capability that expands the operational reach and effectiveness of hybrid-threat mechanisms.

P4	Emphasized the use of technological means to attack systems, gather information, and spread false information.	Cyber and information enablement	Technological mechanism	Technology as an operational enabler	Digital capabilities can support multiple cyber and informational mechanisms simultaneously, reinforcing the socio-technical character of hybrid threats.
P5	"All institutions are vulnerable if technical protection, communication and coordination are not considered as a single security issue."	Technical-organizational interdependence	Socio-technical vulnerability	Institutional and information-space vulnerabilities	Institutional vulnerability emerges through the interaction of technical, organizational, and communication weaknesses rather than through technical exposure alone.
P6	Linked cyberattacks and disinformation campaigns with erosion of citizens' trust in institutions and media.	Trust erosion	Societal effect	Effects on political stability and public trust	The consequences of technology-enabled hybrid activity may extend beyond technical disruption to information credibility and public trust.
P7	Emphasized destabilization and political influence as possible objectives of hybrid activity.	Political and societal destabilization	Societal effect	Effects on political stability and public trust	Hybrid-threat effects may propagate from technological and informational mechanisms into wider political and institutional consequences.

The results indicate that the thematic analysis was based on the participants' written responses. There were several dimensions that were consistent with the data, such as technological enablement, socio-technical vulnerability, impact on trust and political stability, and the significance of multidimensional resilience. However, there was variation

in the extent to which respondents emphasized the above-listed dimensions. While some people paid greater attention to technologies and institutions, other participants emphasized manipulation of information, political influence, trust, and wider societal effects.

The evidence chains also demonstrate how the analysis progressed beyond descriptive coding. Participant statements were first translated into descriptive codes and broader analytical categories, then consolidated into themes, and finally interpreted in relation to the socio-technical framework. The theoretical implications therefore represent analytical interpretations grounded in the participant evidence rather than independent causal claims.

The cross-case comparison indicates variation in the dimensions of technology-enabled hybrid threats emphasized across participant accounts, reflecting differences in analytical focus rather than identical interpretations across cases. Themes 1, 3, and 4 were substantively represented across all nine participant accounts, whereas Themes 2 and 5 were represented across eight of the nine accounts, see Table 6. This pattern indicates that the major analytical dimensions were widely represented in the dataset, although not every participant contributed substantive evidence to every theme. The matrix therefore demonstrates variation in both the number and combination of themes represented across participant accounts.

Table 6. Participant-Theme Cross-Case Matrix Showing Descriptive Prevalence of the Five Major Themes Across all Participants

Participant	Theme 1	Theme 2	Theme 3	Theme 4	Theme 5	Number of themes represented
P1	✓	✓	✓	✓	✓	5
P2	✓	✓	✓	✓	✓	5
P3	✓	✓	✓	✓	✓	5
P4	✓	✓	✓	✓	✓	5
P5	✓	✓	✓	✓	✓	5
P6	✓	✓	✓	✓	✓	5
P7	✓	✓	✓	✓	✓	5
P8	✓	—	✓	✓	—	3
P9	✓	✓	✓	✓	✓	5
Participants with explicit evidence (n/9)	9/9	8/9	9/9	9/9	8/9	—

Notably, the above differences should not be considered contradictions among the participants. Instead, the differences lie in analytical focus and thematic representation. The available information does not provide sufficient evidence to suggest either disagreement or complete agreement among the nine participants.

For this reason, the cross-case analysis will be used as descriptive qualitative data on thematic representation.

Descriptive Theme Frequency Analysis

In addition to the cross-case matrix at the individual level, a frequency analysis was performed to provide an overview of the extent to which the major themes, first-order codes, and analytical categories were covered across the nine participant accounts. The frequencies reflect the number of participants whose interview responses provided substantial evidence pertaining to a particular theme, code, or category.

Since this is a qualitative study with a purposive sample of nine participants, frequencies are used only for descriptive purposes and should not be construed as inferential statistics or causal measures, see Table 7.

Table 7. Descriptive Frequency of Major Themes Across Participant Accounts

Theme	**Participants with substantive evidence (n/9)**	**Percentage**
Theme 1: Hybrid warfare as a current and evolving security concern	9/9	100.0%
Theme 2: Technology as an operational enabler	8/9	88.9%
Theme 3: Institutional and information-space vulnerabilities	9/9	100.0%
Theme 4: Effects on political stability and public trust	9/9	100.0%
Theme 5: Multidimensional priorities for institutional resilience	8/9	88.9%

Note: Frequencies indicate the number of participants whose written responses contained substantive evidence related to each theme. Percentages are descriptive only and are based on nine participant accounts.

The frequency measures at the thematic level imply that there is good representation of all five dimensions within the dataset. Themes 1, 3, and 4 have substantial representation in all nine participant stories, while Themes 2 and 5 are represented in eight participant stories. These are not measures of statistical prevalence.

The distribution of first-order codes shows that disinformation was the most widely represented code across participant accounts, while cyberattacks, destabilization, and cybersecurity preparedness also appeared across several cases. Other codes were more selectively represented.

These differences should not be interpreted as a ranking of analytical importance, since the questionnaire structure and the varying level of detail in participants' written responses influenced the extent to which codes were articulated. Table 8 depicts the descriptive participant-level frequency of first-order codes.

Table 8. Descriptive Participant-Level Frequency of First-Order Codes

First-order code	Participants with explicit evidence (n/9)	Percentage
Disinformation	9/9	100.0%
Hybrid pressure	6/9	66.7%
Cyberattack	5/9	55.6%
Destabilization	5/9	55.6%
Cybersecurity preparedness	5/9	55.6%
Public mistrust	4/9	44.4%
Media and digital literacy	4/9	44.4%
Cyber espionage / digital information gathering	3/9	33.3%
Information credibility erosion	3/9	33.3%
Polarization	3/9	33.3%
Legal and investigative capacity	3/9	33.3%
Rapid dissemination	2/9	22.2%
Below-threshold activity	1/9	11.1%
Weak technical protection	1/9	11.1%
Information-system weakness	1/9	11.1%
Institutional coordination	1/9	11.1%
Strategic communication	1/9	11.1%
International cooperation	1/9	11.1%

Note: *A code was counted only when the participant's written response contained substantive evidence corresponding to that code. Multiple mentions of the same code by the same participant were counted once at participant level. Frequencies therefore represent cross-case occurrence rather than the total number of textual references.*

Divergent Emphases, Negative Cases, and Alternative Interpretations

Even though the responses converged on the themes of technology enablement, institutional vulnerability, public trust, and resilience in general, the respondents did not give equal importance to these themes. While some of the responses considered mainly cyberattacks, technology access, and institutional vulnerabilities, others considered disinformation, politics, strategic communication, public trust, and destabilization as important factors. This is evidence of differences in emphasis across participant accounts and interpretations of the topics rather than absolute consistency among all respondents.

No specific rejection by the participants of any of the major themes presented in this study could be found in the data collected in this study. Nevertheless, the lack of such rejection does not mean that all of the participants agreed with the findings. Since the data was collected using an asynchronous written survey, respondents could not argue about or respond to the views of other respondents.

The analysis therefore identified variation in emphasis rather than clear contradictory cases. Some participants foregrounded technological and cyber-related mechanisms,

whereas others placed greater emphasis on information manipulation, political influence, public trust, strategic communication, and institutional coordination. Importantly, not every participant explicitly connected technological threats with wider political or societal consequences. This suggests that the socio-technical relationships proposed in the framework should be interpreted as recurring analytical patterns across the dataset rather than as relationships uniformly expressed by every participant.

A possible interpretation is that the institutional vulnerabilities mentioned by the respondents might simply be regular organizational flaws, cybersecurity limitations, communication issues, or other constraints within the institution rather than signs of a hybrid threat. This is why the study refrains from interpreting technical vulnerabilities, communication issues, disinformation, or political tension as proof of a hybrid operation. Rather, they are viewed as conditions that can be exploited if they are linked to technological, informational, organizational, and strategic means.

Consequently, the negative-case analysis does not reveal direct rejection of the five major themes, but it does identify limits to thematic uniformity. The data support a multidimensional interpretation of technology-enabled hybrid threats, while also showing that the salience and perceived relationship of these dimensions varied across participant accounts. These variations are treated as analytically relevant rather than as inconsistencies to be removed from the interpretation.

Evaluation of Research Hypotheses

The qualitative findings were examined in relation to the four research hypotheses formulated in the theoretical section. This evaluation was qualitative rather than statistical. The terms used in this section indicate the degree of consistency between the participants' accounts and the theoretically derived expectations and should not be interpreted as statistical hypothesis testing, effect estimation, or causal confirmation.

The qualitative evidence was consistent with H1, whereby participants reported that digital technology had enabled the acceleration, intensification, global spread, anonymity, and transnational nature of hybrid warfare tactics. This trend was clearly captured in Theme 2, where technology is viewed as a tool that enabled cyber-attacks, information collection, cyber espionage, and disinformation.

The qualitative evidence was also consistent with H2, whereby participants viewed institutional vulnerability as the consequence of the intersection between technological vulnerabilities, inadequate inter-institutional cooperation, lack of information sharing, poor strategic communication, and organizational readiness. This trend is especially clear in Theme 3, where vulnerability is seen as a socio-technical phenomenon, and not just a technical one related to cybersecurity.

Theme 4 provided qualitative evidence consistent with H3, whereby cyberattacks, disinformation, media manipulation, and informational pressures are associated with a decrease in public trust, credibility of information, institutional legitimacy, and political instability.

The qualitative evidence was also consistent with H4, as they highlighted the importance of institutional resilience as a multidimensional construct consisting of cybersecurity readiness, inter-institutional coordination, strategic communication, investigative capability, media literacy, international cooperation, and law. Therefore, the responses indicated that resilience is viewed by the participants as broader than technical cybersecurity alone.

In general, the thematic data are in line with all four hypotheses that were theoretically generated. Nevertheless, the results should be seen as qualitative and exploratory, not statistical or causal. The study reveals certain patterns in the stories told by nine participants, and not relationships at the population level or causal effects.

DISCUSSION

The results provide an understanding of how security experts in Kosovo see the connection between technology, hybrid threats, vulnerabilities, and resilience. In all five themes, the security-related experts did not view cyber-attacks, disinformation, political interference, organizational vulnerabilities, and public trust as separate security problems but, rather, as interacting aspects of a wider security environment in which technologies could be used to expand the scope of hybrid operations, while vulnerabilities could intensify their impact. Such an interpretation aligns with the conceptualization of hybrid warfare in terms of the coordinated use of various means and exploitation of pre-existing vulnerabilities instead of resorting exclusively to military power [5, 21].

One of the key findings relates to the enabling nature of technology. The respondents saw digital technologies as being associated with cyberattacks, cyber espionage, information collection, attacks on institutional systems, and rapid spread of misinformation. The significance of social media and digital communication platforms in their narratives was that they make the spread of information fast and borderless. This finding is consistent with H1, which proposes that digital technologies are perceived by participants as increasing the operational capacity of hybrid threats through greater speed, scale, reach, anonymity, and cross-border accessibility. The finding also corroborates other research on the increasing significance of technological capabilities in hybrid operations today [4,9,24]. Technology must be understood not merely as another form of a threat but rather as an enabling environment for conducting several types of hybrid activity at once.

Also, it should be noted that exposure to technology does not lead to institutional vulnerability on its own. There were many instances when participants mentioned the correlation between technological vulnerabilities and organizational and communicative challenges such as limited cybersecurity, poor interinstitutional coordination, deficient strategic communication, political polarization, and weaknesses in public information systems. This finding is consistent with H2, which proposes that exposure to technology-enabled hybrid threats increases when technological vulnerabilities coexist with weak coordination and limited strategic communication. This finding becomes especially relevant as it implies that institutional vulnerability has a socio-technical nature:

technological vulnerabilities become more dangerous when they are combined with organizational weaknesses. Such a perspective on institutional vulnerability aligns with existing research on the Western Balkans that sees institutional fragmentation and security-related capacity issues as sources of vulnerability [13,14].

In terms of the relationship between technology and institutional vulnerability, there are also implications for the conceptualization of cybersecurity policy. Improving technological capabilities is crucial, but the responses of the participants show that it might not be enough to guarantee resilience when responsibilities are dispersed or when communication between institutions is inefficient. On the other hand, institution-level coordination is also not enough to ensure resilience when digital infrastructure is insecure. This suggests that there is an interdependence between technological capability and institutional readiness. This interconnection is a crucial component of the socio-technical framework of the study because it goes beyond the narrow view of hybrid threats.

The third finding relates to the impact of hybrid activity on public trust and political stability. The respondents related cyber-attacks, propaganda, and media manipulation to chaos, polarisation, erosion of institutional credibility and declining trust in official information. These findings are consistent with H3, which proposes that technology-enabled hybrid threats may negatively affect institutional resilience by undermining public trust, information credibility, and political stability. This result is consistent with the findings of prior research, which stresses the informational nature of hybrid warfare and the use of disinformation in affecting political and societal environments [15,16,24]. Most importantly, such attitudes on the part of the respondents indicate that hybrid activities should not always be judged solely on the basis of technical losses inflicted by an attack.

This is especially true in the case of Kosovo. According to the existing literature, the Western Balkans represent an area that is defined by geopolitical competition, institutional fragmentation, contested identities, and political conflicts [13,14]. Also, research papers that examine the specific case of Kosovo have examined disinformation and influence operations linked with politically sensitive issues such as state legitimacy, the Kosovo conflict, the Reçak massacre, Kosovo Liberation Army, and NATO intervention [15,16]. In addition, the findings from the current study complement the existing literature with a practitioner perspective, as the results show that information manipulation is perceived as something that does not just relate to media, but is also linked to institutional and political stability and security.

On the other hand, one must note that the results cannot be viewed as proving the fact that each cyber-attack, disinformation campaign, or political dispute may be considered an example of hybrid warfare. Such an interpretation would be too broad for the purposes of analysis. Instead, one can argue that the answers obtained from the participants imply that technological and informational operations become hybridized when they are linked to the attempt to take advantage of weak spots, affect decision making, undermine the legitimacy of institutions, or create a destabilizing effect. This is significant because the hybrid nature

of operations lies not in their technological nature but in their connection to other means and goals.

Analytical Comparison with Previous Research

The findings broadly correspond with previous research that characterizes contemporary hybrid threats as combinations of technological, informational, political, and institutional mechanisms. However, the present findings also indicate that the relationship among these dimensions may be more important than the presence of any single threat mechanism. Participants did not describe technological exposure as sufficient in itself to produce institutional vulnerability. Instead, technological weaknesses were perceived as becoming more consequential when they interacted with limited institutional coordination, weak information exchange, and inadequate strategic communication. This interpretation extends approaches that treat cyber vulnerability primarily as a technical problem by emphasizing the institutional conditions through which technological exposure may acquire broader security significance.

A similar distinction emerges in relation to information manipulation. Previous research has emphasized disinformation, propaganda, and influence activities as important elements of contemporary hybrid strategies. The participants in this study generally shared this view, but their responses also connected information manipulation with institutional legitimacy, public trust, and the capacity of institutions to communicate during periods of uncertainty. The findings therefore suggest that information credibility should not be interpreted only as an outcome of hybrid activity. Within the present analytical framework, it also functions as a component of institutional resilience because reduced trust may weaken the effectiveness of institutional communication and response.

The findings further elaborate on interpretations of resilience that see technical cybersecurity capacity as its cornerstone. While participants repeatedly mentioned protection, they did not see technical capacity alone as a sufficient condition for resilience. Instead, institutional coordination, strategic communication, capacity to conduct investigations and legal processes, digital literacy, and international cooperation were seen as necessary aspects of preparedness and response. The findings thus point towards a more nuanced and socio-technical interpretation of resilience where technical and non-technical capacities are interdependent and complement each other rather than being exchangeable.

On the other hand, the findings should not be seen as evidence that any cyber-attacks, disinformation campaigns, institutional deficiencies, or political instability are manifestations of hybrid warfare. One of the alternative explanations could be that some of the vulnerabilities identified by participants are actually caused by regular organizational deficiencies, lack of cybersecurity capacity, communication problems, or the general social and political environment, and not a coordinated hybrid attack. The analytic significance of these vulnerabilities comes from their possibility of exploitation within hybrid operations, not the necessity of them coming from such an operation.

It is also important to consider another interpretative nuance introduced by the specific context of Kosovo. Current academic research into the region of the Western Balkans tends to be based on such issues as geopolitical rivalry, political polarization, narrative disputes, institutional fragmentation, and the role of foreign influences. The current results fit within the framework of existing research, but at the same time, introduce a new perspective, which is practitioner-oriented and demonstrates how technological, organizational, informational, and social vulnerabilities are perceived as interconnected by practitioners daily in the environment of security practice.

About technological enablement, the findings are broadly consistent with literature that describes digital technologies as increasing the speed, reach, scalability, anonymity, and cross-border accessibility of cyber and information operations. However, the findings do not indicate that technology alone determines the effectiveness of hybrid activity. An alternative explanation is that the significance attributed to technology may partly reflect the increasing digitalization of institutional activity and the growing dependence of public organizations on digital infrastructure, rather than hybrid-threat dynamics alone. The theoretical implication is therefore that technological capability should be treated as an enabling condition whose security significance depends on its interaction with organizational, informational, and institutional vulnerabilities.

A similar qualification applies to institutional vulnerability. The findings are consistent with research emphasizing institutional fragmentation, weak coordination, communication problems, and limited security capacity as factors that may increase exposure to hybrid pressure. At the same time, these weaknesses should not automatically be attributed to hostile hybrid activity. They may also result from routine administrative fragmentation, resource limitations, unclear institutional responsibilities, or uneven organizational preparedness. The theoretical implication is that institutional vulnerability should be understood as a conditioning factor rather than as evidence of hybrid activity. Its relevance increases when such weaknesses are exploited through technological, informational, or strategic mechanisms.

Conversely, the results relating to public trust and political stability also require an alternative interpretation. As noted in previous academic studies, disinformation and manipulation can play a role in generating confusion, division, and a lack of confidence in institutions. Yet, shifts in the level of public trust can also be affected by political strife within a country, institutional effectiveness, media fragmentation, past levels of public trust, or other social factors. This means that the current results cannot be seen as proving that the lack of trust has anything to do with hybrid pressure. Rather, they suggest that information credibility and public trust can acquire a security dimension because of the interplay between technological and informational challenges and pre-existing institutional and societal weaknesses.

Finally, the results regarding resilience generally confirm the importance of preparedness, institutional coordination, communication capabilities, legal capacity, education, and cooperation as ways to enhance it. Nevertheless, it also appears from the

stories told by participants that none of the measures mentioned could be used as a replacement for the others if they are weak. Good cybersecurity may become insufficient in cases of poor institutional coordination or a lack of strategic communication, while communication itself would be ineffective in cases of weak digital security or poor investigative abilities.

How the Proposed Framework Differs from Existing Frameworks

This framework is not meant to substitute for the existing cybersecurity, resilience, or hybrid threat frameworks. Instead, it provides an analytical framework for understanding how technology-enabled hybrid threats are perceived in a Kosovo security-related context. Different approaches to resilience consider varying aspects of resilience. The NIST Cybersecurity Framework 2.0 concentrates mainly on risk governance and management associated with cybersecurity. The NATO approach to resilience highlights civil preparedness, continuity of essential functions, and resilience of the state. The European Union coordinated response framework covers prevention, coordination, response, and recovery in relation to hybrid campaigns.

Current conceptualizations provide valuable but divergent boundaries for understanding resilience and hybrid threats. The NATO perspective is relatively comprehensive, considering resilience at the national and civil levels, while the EU framework focuses on policy coordination in response to hybrid attacks. In addition, the NIST CSF 2.0 framework provides a structured perspective on cyber risk governance and management. Nevertheless, these approaches do not sufficiently describe the interaction among technological capabilities, organizational fragmentation, information credibility, public trust, and social consequences within a single analytical pathway. Moreover, sociotechnical and organizational resilience approaches provide strong explanations of technical-organizational interdependence and institutional adaptation; however, they were not developed to address hybrid threat mechanisms, information manipulation, and geopolitics in connection with public trust, see Table 9.

Table 9. Comparative Positioning of the Proposed Framework Against Selected Hybrid-Threat, Cybersecurity, Socio-Technical, and Organizational Resilience Approaches

Framework	Strengths	Limitations	Unresolved issue	Contribution of the present framework
NATO resilience framework [18]	Strong national and civil-resilience orientation; emphasis on continuity, essential services, and preparedness	Operates mainly at national and civil-preparedness level	Does not explicitly trace how digital enablers interact with institutional, informational, and societal vulnerabilities at practitioner level	Connects technological enablement with institutional vulnerabilities, societal effects, and resilience capacities
EU hybrid-threat	Strong coordination of prevention,	Primarily policy- and	Limited explanation of	Adds a practitioner-

Framework	Strengths	Limitations	Unresolved issue	Contribution of the present framework
framework [19]	response, restriction, support, and recovery	response-centered	practitioner-level interaction among technological, institutional, and societal factors	grounded relational analysis of interacting hybrid-threat dimensions
NIST CSF 2.0 [17]	Strong structured cybersecurity risk governance and management approach	Primarily cybersecurity-centered	Gives limited analytical attention to disinformation, public trust, political stability, and broader societal effects	Extends the analysis beyond technical cybersecurity to informational and societal consequences
Hybrid CoE/JRC frameworks [10,11]	Strong systemic treatment of hybrid threats, vulnerabilities, interdependencies, and resilience	Broad cross-societal orientation	Not tailored to Kosovo-specific practitioner perceptions or institutional conditions	Provides contextual qualitative grounding from security-related professionals in Kosovo
Socio-technical systems models	Strong integration of technical and organizational systems	Generally broad and not hybrid-threat specific	Often do not explicitly include hybrid-threat mechanisms, information manipulation, public trust, or geopolitical context	Applies socio-technical logic specifically to technology-enabled hybrid threats
Organizational resilience models	Strong focus on adaptation, continuity, recovery, and institutional capacity	Often organization-centered	May underemphasize information warfare, cyber-enabled influence, and societal trust	Integrates organizational resilience with information credibility, public trust, and hybrid-threat mechanisms
Present study	Integrates technological, organizational, informational, and societal dimensions	Exploratory and context-specific	Requires external validation and comparative testing	Provides a practitioner-based socio-technical analytical pathway for Kosovo

The innovation of this framework lies not in the creation of entirely new dimensions but in connecting the existing dimensions within a single context-dependent sociotechnical pathway. In contrast to frameworks centred on national resilience, policy responses, cybersecurity risk management, or systemic resilience, the current framework considers technological factors, hybrid threat mechanisms, institutional vulnerability, information veracity, societal impacts, and resilience capacity within a single analytically oriented framework. The contribution of this framework is, therefore, relational and context-based, as it concerns the relationships among these dimensions within Kosovo's specific security environment.

The current framework is distinct from these approaches on three counts. First, it makes an explicit connection between the technological enablers and the hybrid-threat mechanism rather than considering cybersecurity capabilities separately. Second, it considers institutional vulnerabilities, strategic communication, credibility of information, public trust, and political stability in one analytical chain. Finally, this framework is based on qualitative practitioner experience in Kosovo and thus offers a contextual understanding of how technological, organizational, informational, societal, and resilience factors might relate in practice.

This framework should consequently be viewed as complementary rather than as an alternative approach to other frameworks. The analytical value of this framework stems from its ability to connect technological enablement, hybrid-threat mechanisms, institutional vulnerabilities, societal consequences, and resilience capabilities within one socio-technical system.

Illustrative Socio-Technical Threat Pathway

The socio-technical framework developed in this study can also be interpreted as an illustrative threat pathway rather than only as a set of separate dimensions. A technology-enabled hybrid activity may begin with the use of digital capabilities that increase speed, reach, anonymity, and cross-border accessibility. These capabilities may then support mechanisms such as cyberattacks, cyber espionage, information manipulation, or coordinated disinformation.

The impact that could be caused by the mechanisms will depend on the institutional context within which they take place. If there is poor technical protection, poor information exchange, poor inter-institutional coordination, or poor strategic communication, the technological or informational event in question might cause impacts far from the actual site of disruption. A case in point would be when a technical problem occurs within an institution's infrastructure, leading to uncertainties, and poor and delayed communication leads to confusion among the people. In this case, the technical weakness and communication problems may combine to cause further impact.

This analytical pathway can be expressed as follows: technological enablers increase the operational capacity of hybrid-threat mechanisms; institutional vulnerabilities condition the extent to which those mechanisms generate wider effects; and security and societal

effects may subsequently influence institutional legitimacy, public trust, and political stability. Resilience capacities operate across the pathway by reducing exposure, limiting propagation, supporting coordinated response, and enabling institutional adaptation.

The pathway should not be interpreted as a deterministic causal sequence or as evidence that every cyber or information incident will produce cascading societal effects. Rather, it provides an analytical representation of how the relationships identified in the qualitative findings may interact under conditions of institutional vulnerability. The sequence is therefore intended as a conceptual extension of the socio-technical framework and requires future empirical testing through comparative cases, incident analysis, or larger-scale mixed-methods research

Preliminary Framework Validation and Future Testability

The proposed socio-technical framework has not been formally validated through external expert assessment, Delphi procedures, independent datasets, or quantitative model testing. Accordingly, the present study should be understood as providing preliminary analytical support rather than formal empirical validation. The framework was developed by linking the study's theoretical foundations, questionnaire dimensions, first-order codes, analytical categories, overarching themes, and cross-case patterns into a coherent analytical structure.

Preliminary support for the framework derives from the internal consistency between the conceptual model and the qualitative evidence. The five major themes correspond to the principal analytical components of the framework: technological enablers, hybrid-threat mechanisms, institutional vulnerabilities, societal and institutional effects, and resilience capacities. The participant-level matrix and evidence chains further show that these dimensions were represented across multiple participant accounts rather than being derived from a single isolated response. This consistency provides an initial basis for assessing the framework's analytical plausibility, but it should not be interpreted as proof of causal validity.

A limited form of analytical triangulation was also used by comparing participant evidence with the academic and policy literature reviewed in the study and by examining whether similar relationships were reflected across participants from different professional backgrounds. This form of triangulation strengthens interpretive credibility by comparing the emerging analytical relationships with more than one source of evidence. However, it does not constitute full methodological triangulation because the study did not combine independent empirical datasets, observational data, quantitative measurements, or external expert validation.

Future validation should therefore proceed in several stages. First, the framework could be evaluated by independent security, cybersecurity, communication, and institutional-resilience experts to assess conceptual completeness and clarity. Second, a Delphi study could be used to examine whether experts converge on the proposed relationships among technological enablers, institutional vulnerabilities, societal effects, and resilience

capacities. Third, comparative case studies across Kosovo and other Western Balkan settings could assess whether the same relationships recur across different institutional contexts. Finally, larger-scale quantitative or mixed-methods research could operationalize the framework's constructs and test their associations using appropriate statistical models.

The framework is testable, then, because the main constructs and relationships proposed can be measured in future studies. Technological enablement, institutional coordination, strategic communication, information credibility, public trust, and resilience capacity can all be measured to some degree. Future researchers will, therefore, be able to determine whether the relationships proposed in this study hold up, change, or are refuted through future research. This makes the framework a testing framework for future research rather than a theory.

Theoretical Contribution

In terms of theoretical contribution, this work contributes to existing knowledge of the technological, institutional, informational, and social aspects of hybrid threats through their combination into a socio-technical perspective. Instead of suggesting a new definition of hybrid warfare, the paper draws on existing knowledge about hybrid conflict as the application of conventional and unconventional means of warfare along with the exploitation of existing weaknesses. The results extend the knowledge on hybrid conflict by demonstrating how security-related practitioners in Kosovo view technology as a facilitator that ties together cyberspace attacks, information manipulation, institutional weaknesses, and their wider impact on social trust and political stability.

An important implication for theory relates to the interdependence of technology and institutional vulnerability. According to the findings, technological exposure should not be studied separately from organizational conditions since cybersecurity weaknesses can acquire greater significance depending on inter-institutional coordination, strategic communication, and organizational readiness. On the other hand, organizational resilience can be hampered when institutions rely on technologically vulnerable resources. Therefore, the interaction between organizational and technological factors supports a socio-technical approach in which the phenomenon of institutional weakness is the result of the interaction between technological capabilities and organizational conditions.

This research also contributes to the development of the notion of the consequences of hybrid threats. In addition to being understood in terms of disruptions to digital systems, the threats were also perceived in connection with information credibility, institutional legitimacy, public trust, and political stability. In this way, the scope of analysis of possible consequences of cyber and information operations is expanded, since the effects are extended from the technical ones to those that might arise at societal and institutional levels. Accordingly, in the framework that is developed in this study, public trust becomes one of the factors of institutional resilience rather than something that is separate from security considerations.

In addition, the development of the multidimensional and interconnected nature of resilience is another contribution of the research. It was found that resilience could not be explained in terms of technical cybersecurity measures alone. At the same time, participants stressed such factors of resilience as cybersecurity capacity, institutional coordination, strategic communication, law enforcement capacity, media and digital literacy, and international cooperation. Consequently, resilience is seen as a combination of technical, organizational, informational, legal, educational, and international aspects.

Based on the relationships identified in the qualitative findings, the study advances the following analytical propositions for future empirical examination:

- Proposition 1 (P1): The perceived operational effectiveness of technology-enabled hybrid threats increases when technological capabilities interact with institutional and communication vulnerabilities.
- Proposition 2 (P2): Institutional fragmentation and weak strategic communication condition the extent to which technological and informational mechanisms generate broader institutional and societal consequences.
- Proposition 3 (P3): Public trust functions both as a potential outcome of technology-enabled hybrid activity and as a component of institutional resilience.
- Proposition 4 (P4): Institutional resilience is strengthened when technical cybersecurity capacity is combined with organizational coordination, strategic communication, legal capacity, literacy, and cross-border cooperation.

These propositions should be interpreted as analytically derived expectations rather than validated causal relationships and require testing in future comparative and quantitative research.

Practical and Institutional Implications

These findings have several practical implications regarding resilience of institutions in Kosovo. First, preparation for cybersecurity issues should be viewed as an integral component of broader institutional planning efforts rather than a purely technical task. In their responses, the participants point out the close relationship between technology-based protection, information sharing, institutional coordination, and strategic communication.

The second implication is associated with the role of strategic communication in the process of security preparedness. If disinformation and information manipulation affect institutional uncertainty and credibility, public institutions need the ability to communicate quickly and efficiently. Therefore, cybersecurity response and public communication can be viewed as complementary components of institutional resilience.

Third, the issue of media and digital literacy needs to be incorporated in broader resilience plans since hybrid influence involves not only technical systems, but also information environments where citizens need to be able to evaluate information.

Lastly, international cooperation is necessary since information and cyber threats tend to go beyond the borders of individual institutions and countries. Information sharing,

professional cooperation, and coordination in response processes can enhance the capability of Kosovo to prepare for technology-driven hybrid threats.

Limitations and Future Research

This study has several limitations. First, the research involved a purposive sample of nine professionals. Although the participants represented different security-related professional backgrounds, the sample is not statistically representative, and the findings should therefore be interpreted as exploratory and context-specific.

The second limitation is that the data were gathered through an asynchronous online qualitative questionnaire with five open-ended questions. In this way, it was possible for the respondents to submit their responses in writing, yet there were fewer chances for real-time questioning and probing.

The asynchronous nature of the questionnaire made it difficult to find explicit contradictions or negative perspectives since there was no way for the participants to refute or question the perspectives put forth by other participants. As a result, the study could look at differences in emphasis across participant accounts, but it could not systematically look at the issue of disagreement among the participants. In future research using semi-structured interviews or focus groups, this problem should be addressed.

Thematic analysis was done manually. The first author coded the data initially and then the second author evaluated the codes, categories, and themes that emerged. Any disagreements were sorted out through discussion and agreement. Independent double coding was not conducted. The second author reviewed the coding structure and resolved interpretive differences with the first author through discussion and consensus. Therefore, an intercoder-reliability coefficient such as Cohen's kappa was not calculated, and the coding procedure should be interpreted as consensus-based rather than as an independently replicated coding process.

Formal thematic saturation was not assessed using a prospectively defined saturation procedure. Because the study involved a small purposive sample of nine professionals and an asynchronous written questionnaire, the analysis cannot claim that all potentially relevant perspectives or themes within the wider Kosovo security context were exhaustively captured. The identified themes should therefore be interpreted as recurring patterns within this specific sample rather than as a complete representation of all possible professional perspectives. Future studies should incorporate larger and more diverse samples, iterative data collection, and explicit saturation monitoring to assess when additional data no longer generate substantively new codes or themes.

Further research may conduct studies using bigger samples, in-depth synchronous interviews, cross-sector comparison and comparative research across other Western Balkans. Also, some quantitative research could be done to operationalize the dimensions of socio-technical framework discussed above.

Because this was an exploratory qualitative study based on a small purposive sample, the analysis was not designed to estimate statistical associations, effect sizes, predictive

relationships, or population-level effects. Future research could operationalize the dimensions identified in the socio-technical framework and test their relationships quantitatively using larger samples and appropriate statistical models.

SUMMARY AND CONCLUSION

This study presents a qualitative exploration of the way in which security experts working in Kosovo interpret technology-enabled hybrid threats, vulnerabilities, societal consequences, and resilience capabilities. The key finding is that the analytical relevance of hybrid threats is determined not by technological capabilities per se but by their interaction with organizational vulnerabilities, the information environment, public trust, and institutional capabilities to respond to threats. In this way, the present research suggests that the effects of hybrid threats can be interpreted as interdependent socio-technical phenomena rather than as issues within specific security domains.

The key theoretical implication is that resilience is an interdependent capacity rather than a set of separate protection measures. In addition to previously developed concepts of cybersecurity, national resilience, and hybrid threats, the present study highlights how technological enablers, institutional coordination, strategic communications, information credibility, public trust, and resilience are interrelated within a particular security environment through a single practitioner-based analytical framework. It is not about developing new concepts but about demonstrating the potential ways in which existing analytical dimensions can be related within a specific security environment. Public trust can become both a consequence and an important element of institutional resilience.

From a methodological point of view, the study reveals the importance of using thematic coding with sufficient transparency, participant-level cross-case analysis, evidence chains, consideration of negative cases, and thematic frequency analysis as means of developing a theory within a small-scale exploratory qualitative study. Such a methodology allows for establishing a clearer connection between participant evidence, first-order codes, analytical categories, themes, and theoretical interpretation. However, the study remains exploratory in nature: the sample was purposive and small, the data were collected using an asynchronous written questionnaire, and the developed framework has not been externally validated.

In policy and institutional terms, the research results show that increasing resilience to technology-enabled hybrid threats requires more than investment in cybersecurity. In addition to cyber-preparedness, there is also a need for interinstitutional coordination, strategic communication, investigative and legal capacity-building, media and digital literacy, information exchange, and international collaboration. The research results also imply that institutional vulnerabilities cannot be considered signs of hybrid activity; instead, they can be viewed as potentially exploitable conditions, depending on their interaction with other factors.

Future research must, therefore, focus on testing and validating the socio-technical model in question. Comparing the framework within Kosovo and with other parts of the

Western Balkans may help ascertain whether the same relationships persist across different institutional and geopolitical environments. Expert panel reviews, Delphi analysis, mixed-methods research, and the quantification of technological enablement, institutional coordination, strategic communication, public trust, and resilience capacity will make it possible to test, critically assess, or further develop this framework. In this regard, this study should not be viewed as a globally validated model but rather as a context-specific theoretical foundation for future empirical validation.

AUTHOR CONTRIBUTIONS

Conceptualization, R.R. and B.B.; methodology, R.R. and B.B.; formal analysis, R.R. and B.B.; investigation, R.R.; writing-original draft preparation, R.R. and B.B.; writing-review and editing, R.R. and B.B. All authors have read and agreed to the published version of the manuscript.

DATA AVAILABILITY STATEMENT

All the data's underlying the results can be provided by the corresponding author upon reasonable request.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

ACKNOWLEDGMENTS

The authors would like to thank all professionals who participated in this study and shared their perspectives and professional experiences. Their contributions provided valuable insights into technology-enabled hybrid threats, institutional vulnerabilities, and resilience in the context of Kosovo.

REFERENCES

1. Karimi Parsheh, S., Chegnizadeh, G. International security evolutions and hybrid warfare in the 21st century. *Int. Relat. Res.* **2025**, *14*, 309-327.
2. Çetinkaya, Ş. Hybrid war: International security at the intersection of traditional and modern warfare. *Nevşehir Hacı Bektaş Veli Üniv. SBE Derg.* **2025**, *15 (3)*, 1920-1934.
3. Khan, A.R., Awais, F. Hybrid warfare and the transformation of modern conflict: Challenges for international security frameworks. *Contemp. J. Soc. Sci. Rev.* **2025**, *3*, 3005-3016.
4. Khan, M.S., Rana, F.A., Irfan, Z. Hybrid warfare in the digital age: Cyberpower, AI, and the future of global security. *Advance Social Science Archive Journal* **2025**, *4*(1), 3050-3065.
5. Hoffman, F.G. *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies: Arlington, VA, USA, 2007, p. 51.
6. Caliskan, M. Hybrid warfare through the lens of strategic theory. *Defense & Security Analysis* **2019**, *35*, 40-58.

7. Libiseller, C. "Hybrid warfare" as an academic fashion. *Journal of Strategic Studies* **2023**, *46*, 858-880.
8. Johnson, R. Hybrid war and its countermeasures: A critique of the literature. *Small Wars & Insurgencies* **2018**, *29*, 141-163.
9. Khan, Z.F. Cyber warfare and international security: A new geopolitical frontier. *Crit. Rev. Soc. Sci. Stud.* **2025**, *3*, 513-527:
10. Aho, A., Alonso Villota, M., Giannopoulos, G., Jungwirth, R., Lebrun, M., Savolainen, J., Smith, H., Willkomm, E. *Hybrid Threats: A Comprehensive Resilience Ecosystem*, Hybrid CoE/JRC Research Report, 2023. Available online: https://www.hybridcoe.fi/publications/hybrid-threats-a-comprehensive-resilience-ecosystem/ (Accessed on 27 June 2026)
11. Giannopoulos, G., Smith, H., Theocharidou, M., Eds. *The Landscape of Hybrid Threats: A Conceptual Model (Public Version)*, European Commission, Joint Research Centre: Luxembourg, 2021. Available online: https://publications.jrc.ec.europa.eu/repository/handle/JRC123305 (Accessed on 18 June 2026).
12. Kovačiková, N., Salvi, A., Zorić, B. *Countering Cyber-Enabled Hybrid Interference in the Western Balkans: A Scenario-Based Approach*, European Union Institute for Security Studies: Paris, France, 2024. Available online: https://www.iss.europa.eu/sites/default/files/2024-12/2024-2%20BZ%20FIMI%20in%20WB.pdf (Accessed on 10 June 2026)
13. Bojicic-Dzelilovic, V. Western Balkans as the frontline of Russian hybrid warfare. *Glob. Policy* **2026**, 1-12.
14. Dolan, C.J. Hybrid warfare in the Western Balkans: How structural vulnerability attracts maligned powers and hostile influence. *SEEU Rev.* **2022**, *17(1)*, 3-25.
15. Kuçi, G. Russia's hybrid warfare in the Western Balkans: Geopolitical strategies and proxy actors. *Octopus Journal: Hybrid Warfare & Strategic Conflict.* **2024**, 3, 1-27.
16. Kuçi, G. The struggle for truth: Unveiling efforts to discredit the history and stability of Kosovo. *Octopus Journal: Hybrid Warfare & Strategic Conflict*. **2024**, *2*, 16.
17. National Institute of Standards and Technology. *NIST Cybersecurity Framework 2.0: Resource and Overview Guide*, NIST SP 1299, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2024.
18. North Atlantic Treaty Organization. *Resilience, Civil Preparedness and Article 3.* Available online: https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3 (Accessed on 15 June 2026).
19. Council of the European Union. *Implementing Guidelines for the Framework for a Coordinated EU Response to Hybrid Campaigns*, ST 15880/2022, Council of the European Union: Brussels, Belgium, 2022. Available online: https://data.consilium.europa.eu/doc/document/ST-15880-2022-INIT/en/pdf (Accessed on 15 June 2026)
20. Anagnostakis, D. "Taming the storm" of hybridity: The EU-NATO relationship on countering hybrid threats—From functional overlap to functional cooperation. *Def. Stud.* **2025**, *25*, 587-611.
21. Reichborn-Kjennerud, E., Cullen, P. *What Is Hybrid Warfare?*, Norwegian Institute of International Affairs: Oslo, Norway, 2016. Available online: http://www.jstor.com/stable/resrep07978 (Accessed on 22 June 2026)

22. Abbas, S.R. The emergence of hybrid warfare and the future of global security: A comparative study of Russian and NATO's hybrid infrastructure in Ukraine. *The Rest: Journal of Politics and Development* **2025**, *15*(2), 198-212.
23. Otaiku, A.A. A framework for hybrid warfare: Threats, challenges and solutions. *J. Def. Manag.* **2018**, *8*, 178.
24. Brown, J. An alternative war: The development, impact, and legality of hybrid warfare conducted by the nation state. *J. Glob. Faultlines* **2018**, *5*, 58-82.
25. Baxter, G., Sommerville, I. Socio-technical systems: From design methods to systems engineering. *Interacting with Computers* **2011**, *23*(1), 4-17.
26. Amadi-Echendu, J., Thopil, G.A. Resilience Is Paramount for Managing Socio-Technological Systems During and Post-Covid-19. *IEEE Engineering Management Review* **2020**, 48(3), 118-128.
27. Vert, M., Sharpanskykh, A. The Resilience of Complex Sociotechnical Systems: A Meta-Review of Conceptualisations. *Systems* **2026**, 14(1), 71.
28. Wardle, C., Derakhshan, H. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Council of Europe, 2017. Available online https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html (Accessed on 15 June 2026)
29. Surjatmodjo, D., Unde, A.A., Cangara, H., Sonni, A.F. Information Pandemic: A Critical Review of Disinformation Spread on Social Media and Its Implications for State Resilience. *Social Sciences* **2024**, *13*(8), 418.
30. NATO. *NATO's Approach to Cognitive Warfare*. 2026. Available online https://www.nato.int/content/dam/nato/webready/documents/sto/chief-scientist-report-cognitive-warfare.pdf (Accessed on 25 June 2026)
31. Ivanov, I., Shalamanov, V. NATO and partner countries cooperation in countering asymmetric and hybrid threats in South Eastern Europe's cyberspace. In *Toward Effective Cyber Defense in Accordance with the Rules of Law*, Brill, A., Charvat, J., Mueller, C., Eds., IOS Press: Amsterdam, The Netherlands, **2020**, pp. 59-70
32. Duchek, S. Organizational resilience: a capability-based conceptualization. *Business Research* **2020**, *13*, 215-246.
33. Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., McQuaid, R. *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*, NIST SP 800-160 Vol. 2 Rev. 1, National Institute of Standards and Technology, 2021. Available online https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf (Accessed on 25 June 2026)
34. Steinmann, P., Tobi, H., van Voorn, G.A.K. Resilience Metrics for Socio-Ecological and Socio-Technical Systems: A Scoping Review. *Systems* **2024**, *12*, 357.

APPENDIX A. QUALITATIVE CODEBOOK AND CODING HIERARCHY

First-order code	Operational meaning	Second-order analytical category	Overarching theme	Illustrative participant evidence
Hybrid pressure	References to combined non-conventional, political, informational, or technological pressure	Threat characterization	Hybrid warfare as a current and evolving security concern	P1 referred to disinformation, sanctions, media, and social networks as instruments used for destabilization and tension.
Below-threshold activity	Activities perceived as difficult to attribute or remaining below conventional military-response thresholds	Threat characterization	Hybrid warfare as a current and evolving security concern	Participants described hybrid activities as difficult to identify and capable of influencing political and institutional conditions without direct military engagement.
Cyberattack	Attempts to disrupt, compromise, or gain unauthorized access to digital systems	Technological mechanism	Technology as an operational enabler	Participants associated technology with attacks on institutional systems and public infrastructure.
Cyber espionage	Digital collection or acquisition of sensitive information	Technological mechanism	Technology as an operational enabler	Participants referred to the use of technological means for gathering sensitive information.
Remote access and operational reach	Use of digital technologies to operate without physical presence and across geographical boundaries	Technological enablement	Technology as an operational enabler	Participants emphasized remote access, anonymity, and cross-border reach.
Rapid dissemination	Use of digital platforms to distribute	Information mechanism	Technology as an operational enabler	Participants described digital technologies and online platforms as

First-order code	Operational meaning	Second-order analytical category	Overarching theme	Illustrative participant evidence
	information rapidly and at scale			enabling rapid dissemination of information.
Disinformation	Deliberate dissemination of false or manipulative information	Information mechanism	Technology as an operational enabler	Participants associated digital technologies with the rapid spread of false or manipulative information.
Weak technical protection	Insufficient cybersecurity safeguards or exposure of institutional systems	Technical vulnerability	Institutional and information-space vulnerabilities	Participants identified inadequate technical protection as an institutional weakness.
Weak institutional coordination	Limited cooperation, communication, or information exchange among institutions	Organizational vulnerability	Institutional and information-space vulnerabilities	Participant evidence linked technical protection, communication, and institutional coordination as interconnected security concerns.
Strategic communication weakness	Limited capacity to communicate timely, consistently, and credibly during security-related events	Informational vulnerability	Institutional and information-space vulnerabilities	Participants linked weak strategic communication with greater institutional exposure.
Information-system weakness	Weaknesses in public information or communication systems	Informational vulnerability	Institutional and information-space vulnerabilities	Participants identified weaknesses in public information systems as part of institutional exposure.
Public mistrust	Reduced confidence in institutions, media, or official information	Societal effect	Effects on political stability and public trust	Participants associated cyberattacks and disinformation with erosion of citizens' trust in institutions and media.

First-order code	Operational meaning	Second-order analytical category	Overarching theme	Illustrative participant evidence
Information credibility erosion	Reduced perceived reliability of institutional or public information	Societal effect	Effects on political stability and public trust	Participants associated conflicting and manipulated information with reduced institutional credibility.
Polarization	Increased social or political division associated with manipulative information	Political and societal effect	Effects on political stability and public trust	Participants linked disinformation with confusion, polarization, and social division.
Destabilization	Perceived weakening of political or institutional stability	Political and societal effect	Effects on political stability and public trust	Participants emphasized destabilization and political influence as possible objectives of hybrid activity.
Cybersecurity preparedness	Technical protection, preparedness, and incident-response capacity	Technical resilience	Multidimensional priorities for institutional resilience	Participants emphasized stronger cybersecurity infrastructure and incident-response readiness.
Institutional coordination	Cooperation and information exchange among relevant institutions	Organizational resilience	Multidimensional priorities for institutional resilience	Participants emphasized coordinated institutional responses rather than isolated technical measures.
Strategic communication	Timely and credible communication with institutions and the public	Informational resilience	Multidimensional priorities for institutional resilience	Participants considered effective public communication necessary for resilience.
Legal and investigative capacity	Capacity to investigate, attribute, and respond institutionally to cyber and hybrid activity	Institutional/legal resilience	Multidimensional priorities for institutional resilience	Participants highlighted law-enforcement and investigative capabilities.

First-order code	Operational meaning	Second-order analytical category	Overarching theme	Illustrative participant evidence
Media and digital literacy	Capacity to recognize, assess, and respond to misleading or manipulative information	Societal resilience	Multidimensional priorities for institutional resilience	Participants identified media and digital literacy as part of broader preparedness.
International cooperation	Cross-border information sharing, professional cooperation, and coordinated response	Cooperative resilience	Multidimensional priorities for institutional resilience	Participants emphasized international cooperation because cyber and information threats can cross national borders.

The codebook documents the progression from first-order descriptive codes to broader analytical categories and overarching themes. Codes were derived from the participants' written responses and were subsequently grouped according to conceptual similarity. The coding structure was used to support the evidence chains, cross-case comparison, participant-theme matrix, and descriptive frequency analysis reported in the Results section. Participant-level frequencies are reported separately in the manuscript and are not intended to indicate statistical significance or population-level prevalence.

Coding hierarchy

Theme 1: Hybrid warfare as a current and evolving security concern

- Threat characterization
- Hybrid pressure
- Below-threshold activity

Theme 2: Technology as an operational enabler

- Technological mechanism
- Cyberattack
- Cyber espionage
- Technological enablement
- Remote access and operational reach
- Information mechanism
- Rapid dissemination

- Disinformation

Theme 3: Institutional and information-space vulnerabilities

- Technical vulnerability
- Weak technical protection
- Organizational vulnerability
- Weak institutional coordination
- Informational vulnerability
- Strategic communication weakness
- Information-system weakness

Theme 4: Effects on political stability and public trust

- Societal effect
- Public mistrust
- Information credibility erosion
- Political and societal effect
- Polarization
- Destabilization

Theme 5: Multidimensional priorities for institutional resilience

- Technical resilience
- Cybersecurity preparedness
- Organizational resilience
- Institutional coordination
- Informational resilience
- Strategic communication
- Societal resilience
- Media and digital literacy
- Institutional/legal resilience
- Legal and investigative capacity
- Cooperative resilience
- International cooperation