

INSTITUTIONAL VULNERABILITIES IN THE CONTEXT OF HYBRID THREATS IN THE REPUBLIC OF NORTH MACEDONIA AFTER THE PRESPA AGREEMENT

Ilche Dimovski¹, Filip Popovski² and Hristina Dimova Popovska³

¹Doctor of Political Science, University "St. Kliment Ohridski" - Bitola, North Macedonia

²Full Professor, Technical Faculty - Bitola, University "St. Kliment Ohridski" - Bitola, North Macedonia

³Assistant, Faculty of Information and Communication Technologies - Bitola, University "St. Kliment Ohridski" - Bitola, North Macedonia

ABSTRACT

Amid heightened geopolitical tensions and complex security challenges, hybrid threats pose significant challenges to the institutional stability and democratic development of modern states. Owing to its Euro-Atlantic orientation, geopolitical position, and existing institutional vulnerabilities, the Republic of North Macedonia may be exposed to political and information influence, criminal activities, and cyber threats. The paper analyses organised crime and corruption as factors that can create and deepen institutional vulnerabilities and facilitate hybrid action. It also examines the implications of contemporary digital threats for democratic institutions, the rule of law, and public trust. The research employs a qualitative approach based on relevant scholarly literature, international reports, and strategic documents, together with a comparative analysis of four case studies. The findings indicate that strengthening national resilience requires an integrated approach combining institutional integrity and the rule of law with digital resilience, cybersecurity capabilities, and interinstitutional cooperation.

KEYWORDS

Hybrid threats, institutional vulnerabilities, digital resilience, democratic resilience, Republic of North Macedonia.

1. INTRODUCTION

Contemporary hybrid threats rank among the most significant security and democratic challenges facing modern states. Unlike traditional forms of conflict, they combine political, information, economic, cyber, and other instruments of influence to weaken institutions, democratic processes, and social cohesion. States simultaneously undertaking political and institutional reforms may be particularly vulnerable to such forms of influence, including the Republic of North Macedonia following the conclusion of the Prespa Agreement.

Although the existing literature extensively addresses hybrid threats, corruption, organised crime, and digital security, their interrelationship through the concepts of institutional vulnerability and democratic resilience remains less developed, particularly in the context of the Republic of North Macedonia.

A key scientific contribution of the paper lies in developing and applying an analytical framework that conceptualises institutional vulnerability as an intermediary category between internal weaknesses and their potential exploitation within broader hybrid strategies.

The paper examines the relationship between organised crime, corruption, contemporary digital threats, and the functioning of democratic institutions in the Republic of North Macedonia after the Prespa Agreement. Its central thesis is that organised crime and corruption do not constitute hybrid threats in themselves but may create or deepen institutional vulnerabilities that state or non-state actors can exploit as part of broader hybrid strategies, with potential consequences for democratic, institutional, and national resilience.

2. METHODOLOGICAL AND CONCEPTUAL FRAMEWORK

2.1. Methodological Approach

A qualitative analytical approach is employed, integrating a review of scholarly literature, documentary analysis, and a comparative examination of four case studies. This approach is appropriate to the subject of the research because it enables institutional vulnerabilities to be examined within their broader political, legal, security, and informational contexts. It also allows an analysis of the mechanisms through which such vulnerabilities may reduce the resilience of democratic institutions and create conditions conducive to hybrid influence. The study does not seek to establish a direct causal relationship between the cases examined and specific hybrid operations. Instead, it aims to identify and compare institutional vulnerabilities that, under certain conditions, may be exploited within broader hybrid strategies.

Conceptually, the study draws on relevant scholarly literature concerning asymmetric and hybrid threats, institutional vulnerability, and democratic, institutional, digital, and national resilience. The political, institutional, and security context of the Republic of North Macedonia is examined through official documents, strategic documents, and reports issued by NATO, the European Union and its institutions, GRECO, ENISA, the OECD, and the OSCE, as well as documents and data provided by relevant national institutions. Official and institutional sources constitute the primary documentary basis, while academic analyses and relevant media sources provide additional contextualisation and corroboration of the findings. Sources were selected according to their thematic relevance, institutional credibility, temporal relevance to the events examined, and the possibility of comparing their findings with data from other independent sources.

The case studies were selected purposively, according to predefined criteria, rather than to constitute a statistically representative sample. The following criteria guided the selection: the significance of the case for the functioning of democratic institutions; the availability of relevant and publicly accessible sources; the possibility of identifying a specific type of institutional vulnerability; the diversity of the institutional areas affected; and the potential relevance of the identified vulnerability to mechanisms of hybrid influence. On this basis, the study selected the political and institutional crisis of 2015–2017, the “Reket” case, the “Dvojniki” case, and the series of false bomb threats. Together, these cases encompass the political, judicial, administrative, security, and digital dimensions of institutional vulnerability.

Although the paper’s principal temporal and analytical focus is the period following the Prespa Agreement, the political and institutional crisis of 2015–2017 is included as a pre-Prespa contextual baseline. Its inclusion enables the identification of institutional vulnerabilities that preceded the Agreement and remain relevant to understanding the post-Prespa political and security context. The case is not used to measure the continuity or transformation of these

vulnerabilities longitudinally but as an analytical basis for comparison with vulnerabilities identified in the subsequent cases.

Each case is examined through a common analytical framework comprising: the source and type of institutional vulnerability; the institutions affected; the documented mechanisms and consequences; the manner in which the vulnerability could be exploited; its potential impact on democratic, institutional, digital, and national resilience; and relevant measures for its mitigation. A specific hybrid actor is identified, or a particular activity attributed to such an actor, only when clear and verifiable evidence is available. Otherwise, the analysis is limited to identifying possible mechanisms and strategic effects of hybrid exploitation without associating them with a specific state or non-state actor.

A comparison of the case-study findings identifies both common and case-specific patterns. The analytical synthesis links documented facts and institutional assessments to the concepts developed in the theoretical framework. Throughout the paper, a distinction is therefore maintained between factually documented circumstances, analytical conclusions derived from multiple sources, and hypothetical mechanisms of potential hybrid exploitation. Accordingly, the inclusion of a particular case does not imply its classification as a hybrid operation. Instead, it enables the identification of an institutional vulnerability that could be exploited as part of a broader hybrid strategy.

Methodological limitations stem from the qualitative and documentary nature of the study, its reliance on publicly available sources, and the absence of primary data collected through interviews, surveys, or other field-research methods. A further limitation concerns the unequal availability and varying levels of detail of the data relating to the individual cases. Consequently, the conclusions have analytical and conceptual, rather than statistically representative, significance. They are not intended to attribute specific hybrid activities but to develop a framework for identifying and comparing institutional vulnerabilities.

2.2. Conceptual Framework

Contemporary security studies increasingly examine asymmetric threats as an important element in understanding the dynamics of modern conflicts. Unlike traditional armed conflicts, in which outcomes largely depended on military, economic, and technological superiority, asymmetric conflicts demonstrate that less powerful states, non-state actors, and transnational networks can achieve significant political and security effects through unconventional strategies. Mack argues that the success of the weaker actor depends not only on the resources available but also on selecting a strategy that neutralises the opponent's advantages. Arreguín-Toft similarly emphasises that asymmetry lies in the different ways in which conflict is conducted, rather than merely in the unequal distribution of power [1], [2].

Under contemporary conditions, asymmetric action extends beyond conventional military operations and may involve or exploit terrorist activities, criminal networks, cyberattacks, economic coercion, political infiltration, and coordinated disinformation campaigns. Williams notes that contemporary asymmetric threats are characterised by considerable flexibility, organisational adaptability, and the capacity to exploit institutional weaknesses. Shelley demonstrates that transnational criminal organisations increasingly operate as dynamic network structures capable of adapting rapidly to political, economic, and technological change [3], [4]. Digital transformation further increases the complexity and cross-border nature of organised crime, enabling criminal activities to adapt more rapidly and intersect with other security challenges [5].

Although asymmetric and hybrid threats are frequently considered within the same context, they are not identical concepts. Asymmetry concerns imbalances in the capabilities, resources, and strategies of opposing actors and the use of different modes of action to overcome or exploit those imbalances. Hybrid action, by contrast, constitutes a broader and coordinated strategy combining political, diplomatic, economic, informational, cyber, criminal, and, under certain circumstances, military instruments to achieve strategic objectives. Asymmetric methods may therefore form part of a hybrid strategy, but their individual use is insufficient to classify a particular activity as a hybrid threat [6], [7].

This distinction introduces institutional vulnerability as an intermediary category between internal weaknesses and potential exploitation within hybrid strategies. In institutional theory, North defines institutions as formal and informal rules that reduce uncertainty and shape political and economic behaviour[8]. March and Olsen emphasise that institutional stability depends not only on the normative framework but also on organisational practices, professional standards, and institutional culture [9]. Similarly, Fukuyama relates institutional strength to the state's capacity to implement public policies professionally, impartially, and consistently, while Acemoglu and Robinson identify inclusive institutions as a fundamental prerequisite for political stability, democratic accountability, and long-term social development [10], [11].

On this basis, institutional vulnerability refers to the extent to which weaknesses in the normative framework, organisational practices, professional capacities, oversight mechanisms, interinstitutional coordination, and institutional integrity increase the exposure of the political and institutional system to internal and external pressures. It therefore extends beyond administrative inefficiency and denotes a condition in which existing shortcomings may be exploited to exert political, economic, informational, criminal, or other strategic influence. Hybrid actors do not necessarily need to create new weaknesses; they may instead identify and exploit existing institutional vulnerabilities, particularly in environments marked by political polarisation, limited public trust, and insufficient interinstitutional coordination [12].

Institutional resilience represents the corresponding capacity of individual institutions to maintain lawful, independent, and effective functioning, ensure the continuity of their essential functions, and respond and adapt to different forms of pressure in a coordinated manner. It may be assessed through institutional integrity, professionalism, autonomy, oversight and accountability mechanisms, interinstitutional coordination, and the capacity to learn from previous crises. OECD and European Commission analyses confirm the importance of the rule of law, a professional public administration, and institutional accountability in strengthening this capacity [13], [14].

Although essential, institutional resilience constitutes only one component of democratic resilience. Whereas institutional resilience concerns the functionality, integrity, and capacity of individual institutions, democratic resilience encompasses the broader capacity of the democratic order to preserve the rule of law, the separation of powers, political pluralism, legitimacy, and public trust under sustained political, informational, and security pressures. Diamond associates democratic resilience with the rule of law, political accountability, and effective governance. Levitsky and Ziblatt caution that contemporary democracies most often deteriorate not through sudden institutional overthrows but through the gradual erosion of institutional autonomy and democratic norms [15], [16].

Democratic resilience also depends on the relationship between institutions and society. Norris highlights the importance of the relationship between citizens' democratic expectations and their support for and trust in political institutions, while Putnam identifies social capital as an important prerequisite for the effective functioning of democracy [17], [18]. In this sense,

resilience is not a static condition but a continuous process of adaptation, institutional learning, and capacity-building [19]. Institutions may therefore continue to function formally while democratic resilience remains weakened by declining pluralism, public trust, political accountability, or social cohesion.

For the purposes of this paper, digital resilience is defined as the capacity of institutions to preserve the integrity and availability of data, the security of digital communication channels, and the continuity or rapid restoration of public services that depend on digital systems. It is not limited to the technical protection of information systems but also encompasses access control, organisational procedures, and human capacities. Digital resilience has a cross-cutting function: weaknesses in digital systems may disrupt the operation of individual institutions while also producing broader consequences for public trust, democratic processes, and national security [20], [21].

These dimensions are integrated at the level of national resilience, which encompasses the broader capacity of the state and society to ensure the continuity of essential functions, protect the population and critical infrastructure, and provide a coordinated response during serious crises and hybrid threats. While the European Commission emphasises the relationship between the rule of law, judicial independence, a professional public administration, and democratic resilience, NATO associates national resilience with continuity of government, essential services, civil preparedness, and the protection of critical infrastructure [14], [22]. National resilience is therefore not synonymous with institutional or democratic resilience but represents a broader integrative category whose quality depends on their interrelationship, including the state's digital capacities.

Corruption and organised crime are particularly relevant to this conceptual framework because they may connect internal institutional weaknesses with broader political and security influences. Rose-Ackerman links corruption to declining institutional efficiency and legitimacy, while Mungiu-Pippidi argues that controlling corruption depends on strong mechanisms of public accountability and institutional oversight [23], [24]. Corruption and organised crime may function as asymmetric security challenges, but they do not constitute hybrid threats in themselves. Their relevance to hybrid action arises from their capacity to undermine institutional integrity, reduce institutional autonomy and effectiveness, and create or deepen vulnerabilities that may be exploited within broader coordinated strategies. The findings of GRECO and Transparency International confirm the significance of corruption as a factor that reduces the resilience of democratic institutions [25], [26].

This conceptual framework enables institutional vulnerabilities to be analysed according to their level and consequences. Weaknesses in integrity, autonomy, oversight, professional capacity, or coordination directly reduce institutional resilience. When their effects extend to the rule of law, political pluralism, legitimacy, public trust, and social cohesion, they affect democratic resilience. When they involve the compromise or misuse of information systems, data, communication channels, and digital services, they also affect digital resilience. When they disrupt the continuity of essential state and societal functions and the capacity for a coordinated response, their consequences extend to national resilience.

3. POLITICAL AND INSTITUTIONAL CONTEXT OF THE REPUBLIC OF NORTH MACEDONIA AFTER THE PRESIPA AGREEMENT

Following the entry into force of the Prespa Agreement in 2019 and the accession of the Republic of North Macedonia to NATO in 2020, the country entered a transformed political, institutional,

geopolitical and security context. The Agreement removed the long-standing bilateral obstacle to Euro-Atlantic integration, unblocked NATO membership and strengthened the country's strategic orientation towards Western political and security structures. Consequently, the Republic of North Macedonia became part of the broader Euro-Atlantic security architecture, in which hybrid threats are recognised as one of the principal contemporary security challenges [14], [27].

The post-Prespa period has been characterised by two interrelated processes. On the one hand, NATO membership and the continuation of European integration provided stronger incentives for reforms in the areas of the rule of law, public administration, the judiciary, the security sector and alignment with European Union law. Integration into Euro-Atlantic structures also created additional obligations and opportunities for institutional coordination, information exchange, security cooperation and the development of national resilience capacities. On the other hand, political polarisation, limited trust in institutions, weaknesses in the rule of law and uneven levels of efficiency across the public administration continued to impede democratic and institutional development [14], [28].

Despite its changed geopolitical and security position, the Republic of North Macedonia did not automatically overcome its existing institutional weaknesses [14], [28]. Their significance became even more pronounced amid deeper Euro-Atlantic integration and intensifying geopolitical competition [27], [29]. In this environment, the rule of law, institutional integrity, professionalism in public administration, digital security and interinstitutional coordination have both democratic and security significance [14], [29]. Weaknesses in these areas may reduce the state's ability to identify contemporary political, information-related, and security pressures in a timely manner and respond to them effectively [27], [29].

The period following the Prespa Agreement also coincided with significant changes in the European and global security environment. Russia's aggression against Ukraine in 2022, the deterioration of relations between Russia and Western democracies, and the intensification of geopolitical competition among major powers brought hybrid threats to the centre of contemporary security policies. Hybrid strategies may exploit political and institutional vulnerabilities in democratic states through the coordinated use of information operations, economic pressure, cyber activities and other instruments of influence [7]. In South-Eastern Europe, the activities of external actors are also linked to domestic political dynamics and the interests of local actors. Consequently, democratic consolidation reforms in the Western Balkan states are taking place alongside intensified geopolitical competition [30], [29].

Under these conditions, institutional resilience becomes an integral component of both democratic stability and national security. Its importance in the post-Prespa period derives from the need for institutions to operate lawfully, professionally and in a coordinated manner, to maintain public trust, and to identify different forms of political, informational, economic and cyber influence in a timely manner. Political polarisation, informal political practices and limited institutional consolidation do not constitute hybrid threats in themselves. However, they may weaken the capacity for a coordinated response and create conditions in which internal weaknesses can be exploited [28], [31].

4. INSTITUTIONAL VULNERABILITIES AND POTENTIAL MECHANISMS OF HYBRID INFLUENCE IN THE REPUBLIC OF NORTH MACEDONIA

Relevant international reports indicate that the Republic of North Macedonia has made progress in several reform areas. Nevertheless, challenges persist regarding the rule of law, the independence and efficiency of the judiciary, the professionalisation of public administration, the

fight against corruption and institutional integrity [14],[25],[26], [32],[33]. These assessments do not constitute evidence of specific hybrid activities. Rather, they identify structural weaknesses that may reduce the capacity of institutions to recognise and respond effectively to complex political, economic, informational and cyber pressures in a timely manner.

Central to institutional and democratic resilience is the rule of law. The consistent application of laws, judicial independence and effective oversight of public office holders limit the scope for political pressure, corrupt and criminal influence, and other forms of institutional undermining [14], [25], [34].

The following analysis examines four case studies: the political and institutional crisis of 2015–2017, the “Reket” case, the “Dvojnik” case and the series of false bomb threats recorded during the periods 2022–2023 and 2025–2026. Although these cases differ in their nature, legal classification and immediate consequences, they reveal different dimensions of institutional vulnerability. Their analysis clearly distinguishes between documented facts, analytical conclusions and potential mechanisms of hybrid exploitation.

The first case study concerns the political and institutional crisis of 2015–2017, one of the most significant turning points in the contemporary democratic development of the Republic of North Macedonia. Although it preceded the post-Prespa environment examined in this paper, the crisis is used as an analytical basis for identifying structural vulnerabilities relevant to understanding institutional and democratic resilience in the subsequent period. It was marked by the release of audio recordings whose content indicated widespread unlawful interception of communications, deepening confrontation among key political actors, prolonged institutional deadlock and a substantial decline in public trust in democratic institutions [35]. The European Commission identified serious weaknesses in institutional functioning, the rule of law and the implementation of reform priorities, while the OSCE/ODIHR described distrust in institutions and the political establishment as one of the dominant features of the political environment at the time [36], [37].

This crisis reduced the capacity of institutions to operate independently, in a coordinated manner and with the necessary degree of public legitimacy. The prolonged political conflict created an environment in which institutional decisions were increasingly perceived through a partisan rather than a legal and professional lens. Keil links such developments in the Republic of North Macedonia to broader regional patterns of state capture, institutional politicisation, and political influence over the media and judiciary [38]. At the same time, weaknesses in the system of checks and balances further diminished confidence in the ability of institutions to perform their functions impartially and effectively [36], [39]. The principal institutional vulnerabilities revealed by this case were therefore institutional politicisation and limited autonomy, weakened oversight mechanisms and diminished public legitimacy.

Political polarisation was evident not only in relations between political parties but also in the functioning of institutions, the media and society more broadly. Prolonged confrontation between the government and the opposition, the absence of constructive political dialogue and the conflictual functioning of national institutions adversely affected the quality of democratic governance [39]. Under conditions of pronounced polarisation, public debate can more easily shift from reasoned discussion to mutual discrediting and competition between opposing political narratives [40]. Such conditions create scope for deepening existing social divisions, increasing distrust in institutions and weakening social cohesion [29].

The crisis also had a significant impact on the media environment. Media reporting frequently followed clearly defined political lines, with some media outlets displaying bias and dependence on political or economic centres of power. Freedom House assessed the media as highly polarised

along political, ethnic and linguistic lines, while the OSCE/ODIHR emphasised the need for structural reforms to ensure independent, professional and balanced reporting [37], [39]. In such a media environment, the selective presentation of facts, the emotional framing of political events and the dissemination of competing narratives may increase the public's susceptibility to disinformation and other forms of manipulative information influence [29], [41].

From the perspective of hybrid threats, political polarisation, weakened institutional autonomy, declining public trust, and a polarised media environment may create vulnerabilities that can be exploited within broader hybrid strategies. Under such circumstances, manipulative narratives, disinformation, and attempts to delegitimise the democratic order may further deepen social divisions and distrust in institutions [12], [27], [29].

The crisis also demonstrated that democratic resilience depends not only on the existence of formal institutions and legal mechanisms but also on their ability to operate independently, transparently and in a coordinated manner under political pressure. Prolonged instability limited the capacity for timely decision-making, hindered interinstitutional coordination and redirected institutional resources towards managing the internal political crisis. Following its resolution, the European Commission emphasised the need to restore democratic institutions, the rule of law and mechanisms of institutional accountability [42]. Functional and credible institutions are also essential for the timely identification, prevention and mitigation of complex political, informational and security pressures [29].

The case demonstrates that political and media polarisation, limited institutional autonomy, and weaknesses in the system of checks and balances may reduce public trust and weaken institutional and democratic resilience. The exploitation of these weaknesses may further deepen social divisions, delegitimise institutions and impede a coordinated state response.

The second case study concerns the "Reket" case, one of the most significant corruption cases in the recent history of the Republic of North Macedonia. The case attracted considerable domestic and international attention because of allegations involving abuse of influence, unlawful intermediation and breaches of the integrity of the judicial system. The proceedings conducted by the competent judicial authorities resulted in final court judgments, while also raising serious questions regarding the rule of law, institutional accountability and public trust in judicial institutions [43], [44].

From the perspective of institutional resilience, the case demonstrated that corruption is not merely a matter of criminal law but also a factor that may reduce the capacity of institutions to act independently, transparently and in accordance with the principles of the rule of law. The principal vulnerability revealed by the case lies in the possibility that informal connections, abuse of influence and breaches of professional integrity may affect either the work of judicial institutions or the public perception of their work. When the public comes to believe that individuals can exert informal influence over judicial proceedings, institutional legitimacy is undermined and confidence in judicial independence and impartiality declines. The European Commission and GRECO therefore emphasise the strengthening of judicial independence, accountability and integrity as an essential prerequisite for democratic stability and institutional resilience [25],[45].

Institutions with diminished public credibility face greater difficulty in resisting political and informational pressures. Declining trust in the judicial system provides fertile ground for narratives concerning selective justice, inequality before the law, political control or the state's inability to protect the public interest effectively. Such narratives need not be entirely fabricated to produce political and societal effects. They may selectively exploit existing suspicions and

documented institutional weaknesses to deepen distrust further. In such an environment, disinformation and manipulative messages are more readily accepted by the public [22], [29].

The media attention attracted by the “Reket” case underscored the importance of timely and transparent institutional communication. In broader theoretical terms, information gaps may create scope for speculation, selective interpretations and disinformation [41]. The “Reket” case illustrates the relationship between corruption, institutional integrity and democratic resilience. Corrupt influence over judicial institutions may undermine their independence, efficiency and public credibility, thereby weakening their capacity to respond to complex political, informational and security pressures. The fight against corruption is therefore not merely a matter of criminal policy but also an important component of institutional and national resilience [29], [46]. The analysis of the “Reket” case reveals vulnerabilities relating to the integrity, independence, accountability and public credibility of judicial institutions. These weaknesses may deepen distrust in the rule of law, delegitimise the judiciary and reduce the state’s capacity to respond credibly to political and informational pressures.

The third case study concerns the “Dvojniki” case, which reveals a significant administrative and security vulnerability relating to the issuance of personal documents, the management of identity data and the functioning of public administration in the Republic of North Macedonia. According to the Public Prosecutor’s Office, between mid-2017 and the end of 2020, Macedonian identity documents were unlawfully issued to several individuals using genuine identity data but photographs of other persons. This enabled them to use legally issued documents containing false visual identities. Several officials from the Ministry of the Interior were implicated in the case, which raised serious questions regarding the integrity of administrative procedures, the security of identification systems and the effectiveness of institutional oversight mechanisms [47].

Evidence from the case indicates that vulnerabilities in state information and administrative systems do not arise solely from their technical characteristics but also from human factors, organisational procedures, and institutional integrity. Even where legally prescribed procedures and technical protection mechanisms are in place, their effectiveness may be seriously compromised in the absence of adequate supervision, internal control, a clear separation of official powers and professional accountability. The principal vulnerability revealed by the case therefore lies in the possibility that official access and administrative powers may be abused because of inadequate organisational and oversight mechanisms. This confirms the need for integrated risk management that simultaneously addresses the technical, organisational, personnel-related and institutional components of security [20].

Compromised identification systems create risks that extend beyond the consequences of an individual criminal case. Compromised integrity of official documents may reduce trust in public administration and the reliability of state identification systems, while also having broader implications for border security, international police cooperation and the fight against organised crime [48]. In this context, the institutional area concerned is not limited to the administrative issuance of personal documents; it also encompasses data-management systems, internal security, control over official access, and cooperation with domestic and international security institutions. From the perspective of hybrid threats, such a vulnerability could be exploited to conceal identities, facilitate cross-border criminal activities, circumvent institutional controls, or undermine trust in official documents and state registers. Its potential exploitation need not involve a conventional cyberattack or direct external compromise of an information system. It may also occur through the abuse of official powers, manipulation of administrative procedures and exploitation of inadequate internal controls. This represents an analytically identified potential mechanism of exploitation, rather than evidence that the “Dvojniki” case formed part of a specific hybrid operation.

The case also highlights the relationship between institutional integrity, digital resilience and public trust in the administration. Such trust depends not only on the existence of an appropriate legal framework but also on the capacity of institutions to prevent abuse, detect irregularities in a timely manner and consistently establish accountability for unlawful conduct. Where these mechanisms are insufficiently effective, institutional credibility is undermined and the state's exposure to complex security risks increases [14].

The analysis of the “Dvojnik” case reveals vulnerabilities in administrative procedures, security mechanisms and digital systems arising from the abuse of official powers, inadequate internal controls and compromised integrity of identification systems. These weaknesses may reduce trust in official documents, facilitate criminal and other unlawful activities, and weaken domestic and international security cooperation.

The fourth case study concerns the series of false bomb threats directed at educational establishments and other institutions in the Republic of North Macedonia during the periods 2022–2023 and 2025–2026. Such unlawful acts may seriously disrupt the functioning of public institutions, create a sense of insecurity among citizens and require the prolonged engagement of the security services. During these periods, numerous electronic threats were recorded, resulting in school evacuations, interruptions to the educational process and the continuous engagement of institutions responsible for public security. According to data obtained from the Ministry of the Interior through a freedom-of-information request, 905 threats were recorded between 26 October 2022 and 2 March 2023. Of these, 876 targeted primary and secondary schools in eight cities and were sent from 76 different email addresses [49].

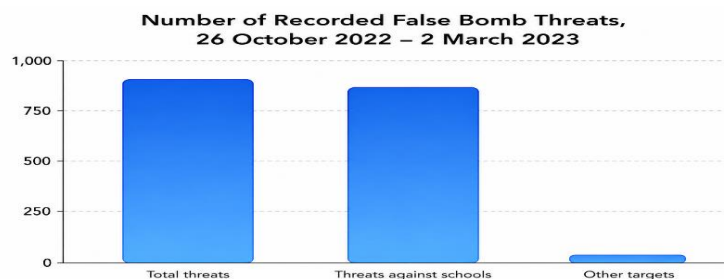


Figure 1. Structure of recorded false bomb threats during the period 2022–2023

Source: Meta.mk [49]

The series of threats also attracted international attention. In March 2023, NATO deployed an expert team to the Republic of North Macedonia to assess the situation and provide support for strengthening national resilience. In its official statement, the Alliance considered the false bomb threats and cyber incidents within the broader context of recent hybrid attacks [50]. However, this general security assessment does not in itself demonstrate that every individual threat formed part of a single, coordinated hybrid operation.

Continued threats in 2025 and 2026 further indicate the diverse nature of the incidents and the possibility that different actors and motives were involved. In October 2025, false bomb threats were recorded in several schools in Skopje and Kumanovo, while in March 2026 five individuals, four of whom were minors, were detained in connection with threats directed at schools in Tetovo [51], [52]. The available evidence therefore does not permit all the threats to be attributed automatically to a single category of perpetrators, a shared intent or a common strategic objective.

From a security perspective, the case demonstrates how relatively limited means may produce disproportionately extensive institutional and societal consequences. The electronic threats resulted in the evacuation of numerous schools, disruption of the educational process, the deployment of substantial police resources and a sense of insecurity among pupils, parents and teaching staff. The principal institutional vulnerability revealed by the case lies in the possibility that standard security protocols—which justifiably require every threat to be investigated—may be exploited to disrupt institutional operations repeatedly and place pressure on human and material resources. The disproportion between the means employed and the effects produced is relevant to the analysis of hybrid threats [29], [53].

The case also highlights the digital dimension of contemporary security challenges. Although false bomb threats do not constitute a conventional cyberattack involving the compromise of an information system, electronic communication channels are used as a means of producing physical, institutional and psychological consequences. The use of multiple email addresses complicates identification and attribution, underscoring the need for enhanced digital investigative capabilities, effective information exchange, and interinstitutional and international cooperation [20], [49]. In the context of hybrid threats, this method of action could be exploited to generate prolonged institutional pressure, exhaust security resources, disrupt public services, create a sense of insecurity and reduce confidence in the state’s capacity to provide security. If such actions were coordinated with disinformation or other forms of political and information influence, their societal effects could be further amplified [27], [29].

In turn, the case reveals limitations in the capacity of security institutions to respond to recurrent electronic threats without prolonged disruption to public services and disproportionate expenditure of institutional resources. Such threats may disrupt the educational process, create a sense of insecurity and reduce public trust.

Table 1. Qualitative comparison of the case studies

Case study	Source and type of vulnerability	Institutional area affected	Potential mechanism of exploitation	Potential effect on resilience	Relevant mitigation measures
Political and institutional crisis, 2015–2017	Political polarisation; politicisation and limited institutional autonomy; weakened system of checks and balances; media polarisation	Democratic institutions, judiciary, oversight mechanisms and media	Exploitation of societal divisions; dissemination of manipulative narratives and disinformation; delegitimisation of institutions	Reduced public trust and institutional legitimacy; weakened coordination; deepened polarisation and diminished social cohesion	Strengthening the rule of law, institutional autonomy and accountability, the system of checks and balances, media pluralism and public trust
“Reket”	Corruption; abuse of influence; compromised professional and institutional integrity	Judiciary and prosecution service	Exploitation of existing distrust through narratives of selective justice, political control and inequality before the law	Delegitimisation of the judiciary; weakening of the rule of law; reduced capacity to respond credibly to political and	Institutional independence, professional integrity, effective oversight and accountability, transparency of proceedings and

				informational pressures	timely institutional communication
“Dvojniki”	Abuse of official powers; inadequate internal controls; human and organisational weaknesses; compromised integrity of identification systems	Ministry of the Interior, public administration, identification systems and personal-data management	Identity abuse; circumvention of administrative and security controls; facilitation of criminal or other unlawful activities	Reduced trust in official documents and public administration; risks to border security and international police cooperation	Control of official access, procedural traceability, regular security assessments, personal-data protection, internal and external oversight, and consistent establishment of accountability
False bomb threats	Limited capacity to manage recurrent threats transmitted through digital channels; pressure on security protocols and resources	Educational establishments, police, security services and other public institutions	Repeated disruption of public services; exhaustion of resources; creation of insecurity; potential coordination with disinformation campaigns and manipulative narratives	Disruption of the educational process; institutional strain; sense of insecurity; reduced confidence in the state’s capacity to provide security	Digital investigative capabilities, proportionate assessment and response protocols, interinstitutional and international cooperation, regular training and coordinated crisis communication

The comparative overview demonstrates that the four cases reveal different sources and forms of institutional vulnerability. The political crisis of 2015–2017 exposes weaknesses associated with political polarisation, institutional autonomy and the media environment, while the “Reket” case highlights the effects of corruption on the integrity and credibility of the judiciary. The “Dvojniki” case demonstrates the relationship between human factors, administrative procedures and the security of information systems, whereas the false bomb threats reveal how digitally mediated threats employing limited means may impose a disproportionate institutional and societal burden.

Despite their differences, the cases share a common pattern: existing internal weaknesses reduce the ability of institutions to operate independently, in a coordinated manner and with the necessary degree of public trust. At the same time, they create opportunities for political, informational, criminal or security exploitation. The comparative analysis therefore supports the paper’s central thesis: institutional vulnerabilities constitute an intermediary mechanism through which various internal weaknesses may increase the state’s exposure to broader hybrid strategies, without the events analysed being automatically classified as hybrid operations.

5. THE ROLE OF NATO AND THE EUROPEAN UNION IN STRENGTHENING NATIONAL RESILIENCE

The concepts of institutional, democratic and digital resilience developed in the paper's conceptual framework acquire concrete political and institutional application within NATO and the European Union. Although they differ in their primary roles and instruments, both organisations share the understanding that contemporary security challenges cannot be addressed through traditional defence measures alone. State resilience also depends on the continuity of institutional functions, the rule of law, the protection of critical infrastructure, the security of information systems and the capacity for a coordinated response to political, informational, economic and cyber pressures [54], [55], [56].

5.1. NATO and national resilience

NATO treats national resilience as an integral component of collective defence and a prerequisite for the performance of the Alliance's core tasks. The 2022 Strategic Concept identifies individual and collective resilience as critical to deterrence and defence, crisis prevention and management, and cooperative security [54]. This approach demonstrates that the Alliance's capacity to respond to complex security challenges depends not only on military capabilities but also on the functionality of civilian institutions, critical infrastructure and essential public services [22], [55]. Within this approach, the Alliance identifies seven baseline requirements for national resilience: assured continuity of government and critical government services; resilient energy supplies; the ability to deal effectively with uncontrolled movement of people; resilient food and water resources; the ability to deal with mass casualties; resilient civil communications systems; and resilient transport systems [22]. These requirements do not constitute a uniform model to be applied mechanically across all countries. Rather, they provide a common framework through which the Allies assess and develop their national capacities.

Resilience is particularly important in addressing hybrid threats, as such activities may seek to undermine institutional capacity, public trust, decision-making processes and the continuity of essential state functions. Hybrid actors may combine political pressure, disinformation, cyber activities, economic instruments and covert influence, while the effects of these measures also depend on pre-existing vulnerabilities within the targeted society [27], [56]. NATO therefore connects resilience with civil preparedness, the protection of critical functions, strategic communications and the capacity for a coordinated response.

For the Republic of North Macedonia, the significance of this approach derives from its membership in the Alliance and from the need for national institutions to ensure continuity of government, the functioning of essential services, the security of communications systems and civil-military coordination during crises [22],[27]. NATO membership facilitates security cooperation, information exchange, expert support and the development of interoperable capabilities. It does not, however, replace the national responsibility to strengthen institutions and reduce internal weaknesses [22].

5.2. The European Union and institutional and digital resilience

The European Union has developed a broader normative and institutional approach to resilience that links security policies with the rule of law, democratic governance, cybersecurity, strategic communication and the protection of critical infrastructure. Unlike NATO, whose primary function is collective defence, the European Union employs regulatory, economic, political, and

institutional instruments to shape standards and practices in its Member States and guide reform processes in candidate countries [57], [58].

Adopted in 2022, the Strategic Compass for Security and Defence identifies resilience as one of the priorities of European security policy. The document emphasises the need for enhanced intelligence analysis, the protection of critical infrastructure, the development of cyber capabilities, and countering foreign information manipulation and interference [57]. This approach reflects the understanding that contemporary hybrid threats may simultaneously affect democratic processes, public administration, economic activity, the information environment and essential public services.

The European Union has also established institutional mechanisms for monitoring and analysing hybrid activities. The Hybrid Fusion Cell, operating within the European External Action Service, provides integrated analysis of potential hybrid threats, while the framework for Foreign Information Manipulation and Interference (FIMI) enables the systematic identification and analysis of coordinated information activities [59]. Within this framework, information influence is examined in relation to the actors involved, their methods of operation, the channels employed, their objectives and their potential effects on democratic processes and institutional trust.

ENISA occupies a distinct position within the European resilience system by providing expert support for the development of cybersecurity policies, risk management and the protection of information infrastructure. ENISA's analyses demonstrate that contemporary threats extend beyond traditional technical categories and may involve combinations of cyber incidents, social engineering, exploitation of human factors and disruption of critical services [20]. Digital resilience therefore requires technical protection to be integrated with organisational procedures, human capacities and institutional coordination [20], [21], [60].

The European normative framework has been further strengthened by the NIS2 Directive, the Critical Entities Resilience Directive and the Cyber Solidarity Act [61], [62], [63]. NIS2 establishes obligations concerning cybersecurity risk management, incident reporting and the accountability of management bodies in the sectors within its scope [61]. The Critical Entities Resilience Directive focuses on identifying critical entities and strengthening their capacity to prevent, withstand and recover from disruptions to the provision of essential services [62]. The Cyber Solidarity Act provides mechanisms for improving the detection of and joint response to significant cyber threats and incidents at Union level [63]. Although these instruments differ in their subject matter, together they contribute to a more integrated approach to institutional, infrastructural and digital resilience.

For the Republic of North Macedonia, these policies are relevant in the context of the accession process and alignment with European Union law. As a candidate country, it does not have the same legal status as the Member States regarding the direct application of all Union mechanisms. Nevertheless, European standards provide important guidance for reforms in public administration, the rule of law, cybersecurity and the protection of critical infrastructure [14].

5.3. Complementarity of the NATO and European Union Frameworks

The NATO and European Union frameworks are complementary, but they are neither identical nor interchangeable. The distinction between them does not consist of a strict division under which NATO operates solely in the security sphere and the European Union solely in the political and normative sphere. Both organisations address the political, institutional, security, and digital dimensions of resilience, but differ in their primary roles and instruments. NATO develops its approach within the framework of collective defence, political and security cooperation, civil

preparedness, and national capacities for responding to hybrid and other complex threats [22], [27], [54]. The European Union develops resilience through common security policies, legal and regulatory instruments, economic mechanisms, cybersecurity, the protection of critical entities, and reforms relating to the rule of law and public administration [14], [57], [61], [62], [63].

Such complementarity is important because institutional, democratic, and digital vulnerabilities do not exist in isolation. Compromised institutional integrity may reduce the capacity to manage security risks; limited public trust may increase the influence of manipulative narratives; inadequate administrative controls may compromise the security of information systems; and weak coordination may hinder responses to incidents affecting multiple institutional areas. National resilience therefore requires the integration of democratic governance, institutional integrity, civil preparedness, cybersecurity and the protection of critical infrastructure [21], [56], [57].

For the Republic of North Macedonia, NATO membership and the European Union accession process create different but complementary opportunities for developing these capacities. NATO provides a framework for security coordination, resilience assessment and the development of crisis-response capabilities, while the European integration process promotes legal and institutional reforms in areas that directly affect the functionality and credibility of state institutions [14], [22], [27].

The effectiveness of the NATO and European Union frameworks depends on their translation into domestic institutional practice. This requires functional oversight mechanisms, a clear allocation of responsibilities, regular interinstitutional information exchange, professional personnel, secure information systems and practical testing of crisis-response capacities. External standards and cooperation mechanisms may support the strengthening of national resilience, but they cannot substitute for political responsibility and the institutional capacity required for their consistent implementation.

Table 2. Key strategic and normative frameworks of NATO and the European Union relevant to national resilience

Organisation	Document or mechanism	Principal area	Relevance to resilience
NATO	2022 Strategic Concept [54]	Collective defence and hybrid threats	Identifies individual and collective resilience as critical to the Alliance's core tasks
NATO	Baseline requirements for national resilience [22]	Civil preparedness and continuity of functions	Covers government functions, energy, communications, transport, food, water and health capacities
NATO	Approach to countering hybrid threats [27]	Prevention, preparedness and response	Connects national responsibility, resilience and collective support
EU	2022 Strategic Compass [57]	Security and defence	Provides for strengthening cyber capabilities, critical infrastructure and resilience against information influence
EU	NIS2 Directive [61]	Cybersecurity	Regulates cybersecurity risk management, incident reporting and institutional accountability
EU	Critical Entities	Critical entities and	Provides for risk assessments and

	Resilience Directive [62]	essential services	measures to ensure the continuity of essential services
EU	Cyber Solidarity Act [63]	Detection of and response to cyber threats	Establishes mechanisms for joint preparedness, detection and response to significant cyber incidents

6. CONCLUSION

Contemporary hybrid threats cannot be fully understood solely through the instruments employed or the immediate actions of the actors involved. Their effectiveness also depends substantially on the political, institutional, societal and digital conditions prevailing in the environment they target. The analysis of hybrid threats should therefore also encompass existing weaknesses that may facilitate political, informational, economic, criminal or security influence.

Overall, the findings support the paper's central thesis that organised crime and corruption do not constitute hybrid threats in themselves but may create and deepen institutional vulnerabilities that can be exploited within broader hybrid strategies. Their relevance derives from their capacity to undermine the rule of law, institutional integrity, professional autonomy and public trust, thereby reducing the ability of institutions to recognise various forms of pressure in a timely manner and respond to them in a coordinated way. This finding does not imply that every instance of corruption, organised crime or institutional weakness constitutes a hybrid activity. Rather, their presence increases exposure to potential hybrid exploitation.

A comparative analysis of the four cases reveals different but interrelated forms of institutional vulnerability. The political and institutional crisis of 2015–2017, examined as a pre-Prespa baseline, demonstrates the structural consequences of political polarisation, limited institutional autonomy, weakened checks and balances, media polarisation and diminished public trust. The “Reket” case demonstrates how corruption and abuse of influence may undermine the integrity and credibility of judicial institutions and provide a basis for narratives concerning selective justice and inequality before the law. The “Dvojniki” case confirms the relationship between human factors, organisational procedures, control over official access and the security of identification systems. The series of false bomb threats demonstrates how digitally mediated actions conducted with limited means may impose disproportionate institutional, resource-related and psychological burdens.

Across all four cases, a common pattern emerges: weaknesses in integrity, autonomy, oversight, professional capacities, digital security, and interinstitutional coordination reduce both institutional functionality and public legitimacy. When their consequences affect the rule of law, political pluralism, social cohesion and public trust, institutional vulnerability develops into a broader challenge to democratic resilience. When information systems, data, communication channels and digitally mediated services are affected, the consequences also extend to digital resilience. Their cumulative impact on the continuity of essential functions and the capacity for a coordinated response, in turn, affects national resilience.

The paper's original scientific contribution lies in the development and application of an analytical framework that positions institutional vulnerability as an intermediary category between internal weaknesses and potential mechanisms of hybrid exploitation. Applying common analytical categories to four cases drawn from different institutional areas enables comparison of the sources of vulnerability, the institutions affected, potential mechanisms of exploitation, effects on different dimensions of resilience and relevant mitigation measures. The contribution also lies in the consistent distinction between documented facts, analytical conclusions derived

from those facts and hypothetical pathways of potential hybrid exploitation. This approach avoids extending the concept of hybrid threats to every institutional crisis or security incident, while still recognising their potential strategic relevance.

Taken together, these findings indicate the need for an integrated approach to strengthening the resilience of the Republic of North Macedonia. First, this requires consistent enforcement of the law, greater independence and accountability of judicial and oversight institutions, and effective mechanisms for preventing and sanctioning corruption. Second, public administration should strengthen internal controls, the management of official access, the traceability of administrative procedures and the protection of personal and institutional data. Third, further development is needed in the areas of cybersecurity, digital investigation, risk assessment and continuity of digital services. Fourth, institutions should establish timely, accurate and mutually coordinated crisis and strategic communications, while also improving media and digital literacy. Finally, regular interinstitutional training, exercises and information-exchange mechanisms are necessary, together with continued use of the political, expert and security support provided by NATO and the European Union.

The study also has several limitations. Its qualitative and documentary nature means that its conclusions are based on academic literature, official documents, international reports and other publicly available sources, without primary data obtained through interviews, surveys or field research. The availability and level of detail of the data are not uniform across all cases, while the different nature of the cases limits the possibility of direct comparison. Furthermore, the study does not attribute specific hybrid activities to particular actors, and its findings cannot be statistically generalised beyond the context examined.

Future research could empirically test the proposed analytical framework through interviews with representatives of relevant institutions, security experts, journalists and civil society representatives. Comparative analyses involving other Western Balkan countries, the development of measurable indicators for different types of institutional vulnerability, and longitudinal research examining their continuity and transformation before and after the Prespa Agreement would provide additional value. Such research would enable a more precise assessment of the conditions under which institutional weaknesses develop from internal governance problems into factors that increase exposure to broader hybrid strategies.

Ultimately, the long-term resilience of the Republic of North Macedonia depends not only on the capacity to identify and counter immediate forms of hybrid action but also on the systematic reduction of vulnerabilities that increase the potential effectiveness of such actions. Functional, professional, independent and digitally resilient institutions, supported by public trust and effective democratic oversight, provide the most important foundation for limiting the scope for hybrid exploitation and building sustainable national resilience.

REFERENCES

- [1] A. Mack, (1975) "Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflict", *World Politics*, Vol. 27, No. 2, pp. 175–200, <https://doi.org/10.2307/2009880>.
- [2] I. Arreguín-Toft, (2001) "How the Weak Win Wars: A Theory of Asymmetric Conflict", *International Security*, Vol. 26, No. 1, pp. 93–128, <https://doi.org/10.1162/016228801753212868>.
- [3] P. D. Williams, ed., (2008) *Security Studies: An Introduction*, Routledge, <https://doi.org/10.4324/9780203926604>.
- [4] L. I. Shelley, (2014) *Dirty Entanglements: Corruption, Crime, and Terrorism*, Cambridge University Press, <https://doi.org/10.1017/CBO9781139059039>.

- [5] Europol, (2021) “European Union Serious and Organised Crime Threat Assessment 2021: A Corrupting Influence—The Infiltration and Undermining of Europe’s Economy and Society by Organised Crime”, Publications Office of the European Union.
- [6] J. K. Wither, (2016) “Making Sense of Hybrid Warfare”, *Connections: The Quarterly Journal*, Vol. 15, No. 2, pp. 73–87, <https://doi.org/10.11610/Connections.15.2.06>.
- [7] O. Fridman, (2018) *Russian “Hybrid Warfare”: Resurgence and Politicisation*, Oxford University Press.
- [8] D. C. North, (1990) *Institutions, Institutional Change and Economic Performance*, Cambridge University Press, <https://doi.org/10.1017/CBO9780511808678>.
- [9] J. G. March and J. P. Olsen, (1989) *Rediscovering Institutions: The Organizational Basis of Politics*, Free Press.
- [10] F. Fukuyama, (2013) “What Is Governance?”, *Governance*, Vol. 26, No. 3, pp. 347–368, <https://doi.org/10.1111/gove.12035>.
- [11] D. Acemoglu and J. A. Robinson, (2012) *Why Nations Fail: The Origins of Power, Prosperity, and Poverty*, Crown Business.
- [12] M. Wigell, (2021) “Democratic Deterrence: How to Dissuade Hybrid Interference”, *The Washington Quarterly*, Vol. 44, No. 1, pp. 49–67, <https://doi.org/10.1080/0163660X.2021.1893027>.
- [13] OECD, (2021) *Government at a Glance 2021*, OECD Publishing, Paris, <https://doi.org/10.1787/1c258f55-en>.
- [14] European Commission, (2024) *North Macedonia 2024 Report*, SWD(2024) 693 final, Brussels.
- [15] L. Diamond, (2015) “Facing Up to the Democratic Recession”, *Journal of Democracy*, Vol. 26, No. 1, pp. 141–155, <https://doi.org/10.1353/jod.2015.0009>.
- [16] S. Levitsky and D. Ziblatt, (2018) *How Democracies Die*, Crown.
- [17] P. Norris, (2011) *Democratic Deficit: Critical Citizens Revisited*, Cambridge University Press, <https://doi.org/10.1017/CBO9780511973383>.
- [18] R. D. Putnam, R. Leonardi and R. Y. Nanetti, (1993) *Making Democracy Work: Civic Traditions in Modern Italy*, Princeton University Press.
- [19] D. Chandler, (2014) *Resilience: The Governance of Complexity*, Routledge, <https://doi.org/10.4324/9781315773810>.
- [20] European Union Agency for Cybersecurity (ENISA), (2023) *ENISA Threat Landscape 2023*, Publications Office of the European Union, <https://doi.org/10.2824/782573>.
- [21] OECD, (2023) *Government at a Glance 2023*, OECD Publishing, Paris, <https://doi.org/10.1787/3d5c5d31-en>.
- [22] NATO, (2024) “Resilience, Civil Preparedness and Article 3”, updated 13 November 2024, <https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3>.
- [23] S. Rose-Ackerman, (1999) *Corruption and Government: Causes, Consequences, and Reform*, Cambridge University Press, <https://doi.org/10.1017/CBO9781139175098>.
- [24] A. Mungiu-Pippidi, (2015) *The Quest for Good Governance: How Societies Develop Control of Corruption*, Cambridge University Press, <https://doi.org/10.1017/CBO9781316286937>.
- [25] Group of States against Corruption (GRECO), (2024) “Fourth Evaluation Round: Corruption Prevention in Respect of Members of Parliament, Judges and Prosecutors—Second Addendum to the Second Compliance Report: North Macedonia”, Council of Europe.
- [26] Transparency International, (2025) *Corruption Perceptions Index 2024*, Transparency International, <https://www.transparency.org/en/cpi/2024>.
- [27] NATO, (2024) “Countering Hybrid Threats”, <https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats>.
- [28] F. Bieber, (2020) *The Rise of Authoritarianism in the Western Balkans*, Palgrave Macmillan, <https://doi.org/10.1007/978-3-030-22149-2>.
- [29] R. Jungwirth, H. Smith, E. Willkomm, J. Savolainen, M. Alonso Villota, M. Lebrun, M. Aho and G. Giannopoulos, (2023) *Hybrid Threats: A Comprehensive Resilience Ecosystem*, EUR 31104 EN, Publications Office of the European Union, Luxembourg, <https://doi.org/10.2760/37899>.
- [30] D. Bechev, (2017) *Rival Power: Russia in Southeast Europe*, Yale University Press.
- [31] F. Fukuyama, (2014) *Political Order and Political Decay: From the Industrial Revolution to the Globalization of Democracy*, Farrar, Straus and Giroux.
- [32] Freedom House, (2024) “North Macedonia: Nations in Transit 2024 Country Report”, <https://freedomhouse.org/country/north-macedonia/nations-transit/2024>.

- [33] Bertelsmann Stiftung, (2024) BTI 2024 Country Report—North Macedonia, Bertelsmann Stiftung, Gütersloh.
- [34] T. Carothers, (2002) “The End of the Transition Paradigm”, *Journal of Democracy*, Vol. 13, No. 1, pp. 5–21, <https://doi.org/10.1353/jod.2002.0003>.
- [35] B. Ceka, (2018) “Macedonia: A New Beginning?”, *Journal of Democracy*, Vol. 29, No. 2, pp. 143–157, <https://doi.org/10.1353/jod.2018.0033>.
- [36] European Commission, (2016) The Former Yugoslav Republic of Macedonia 2016 Report, SWD(2016) 362 final, Brussels.
- [37] OSCE Office for Democratic Institutions and Human Rights, (2017) The Former Yugoslav Republic of Macedonia, Early Parliamentary Elections, 11 December 2016: Final Report, OSCE/ODIHR, Warsaw.
- [38] S. Keil, (2018) “The Business of State Capture and the Rise of Authoritarianism in Kosovo, Macedonia, Montenegro and Serbia”, *Southeastern Europe*, Vol. 42, No. 1, pp. 59–82, <https://doi.org/10.1163/18763332-04201004>.
- [39] Freedom House, (2017) “Macedonia: Nations in Transit 2017 Country Report”, Freedom House.
- [40] J. McCoy, T. Rahman and M. Somer, (2018) “Polarization and the Global Crisis of Democracy: Common Patterns, Dynamics, and Pernicious Consequences for Democratic Polities”, *American Behavioral Scientist*, Vol. 62, No. 1, pp. 16–42, <https://doi.org/10.1177/0002764218759576>.
- [41] C. Wardle and H. Derakhshan, (2017) *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*, Council of Europe, Strasbourg.
- [42] European Commission, (2018) The Former Yugoslav Republic of Macedonia 2018 Report, SWD(2018) 154 final, Brussels.
- [43] Basic Public Prosecutor’s Office for the Prosecution of Organised Crime and Corruption, (2019) “Обвинителен акт за три лица во предметот ‘Рекет’” [Indictment Filed against Three Persons in the ‘Reket’ Case], 10 October 2019, <https://jorm.gov.mk/obvinitelen-akt-za-tri-licza-vo-predmet/>.
- [44] Radio Free Europe/Radio Liberty, (2021) “Апелација ја потврди првостепената пресуда за ‘Рекет’” [Court of Appeal Upholds the First-Instance Judgment in the ‘Reket’ Case], 21 July 2021, <https://www.slobodnaevropa.mk/a/31370222.html>.
- [45] European Commission, (2020) North Macedonia 2020 Report, SWD(2020) 351 final, Brussels.
- [46] OECD, (2017) *Preventing Policy Capture: Integrity in Public Decision Making*, OECD Publishing, Paris, <https://doi.org/10.1787/9789264065239-en>.
- [47] Basic Public Prosecutor’s Office Skopje, (2021) “Поднесено обвинение против 11 лица за злоупотреби при издавање на пасоши” [Indictment Filed against 11 Persons for Abuses in the Issuance of Passports], 14 April 2021, <https://jorm.gov.mk/podneseno-obvinenie-protiv-11-licza-za-zloupotrebi-pri-izdava%D1%9Aeto-pasoshi/>.
- [48] M. Rudner, (2008) “Misuse of Passports: Identity Fraud, the Propensity to Travel, and International Terrorism”, *Studies in Conflict & Terrorism*, Vol. 31, No. 2, pp. 95–110, <https://doi.org/10.1080/10576100701812803>.
- [49] M. Jordanovska and A. Popovska, (2023) “The Pattern of False Bomb Threats: 905 Threats, Eight Cities and 76 Email Addresses”, *Meta.mk*, 28 March 2023, <https://meta.mk/shemata-na-lazhnite-dojavi-za-bombi-905-zakani-osum-gradovi-76-elektronski-adresi-infografik/>.
- [50] NATO, (2023) “NATO Team in North Macedonia to Help against Hybrid Attacks”, 8 March 2023, <https://www.nato.int/en/news-and-events/articles/news/2023/03/08/nato-team-in-north-macedonia-to-help-against-hybrid-attacks>.
- [51] Ministry of Interior of the Republic of North Macedonia, (2025) “Закани за наводно поставени бомби во училишта – констатирано е дека пријавителите се лажни” [Threats of Allegedly Planted Bombs in Schools Determined to Be False], 28 October 2025, <https://mvr.gov.mk/mk-MK/odnosi-so-javnost/novosti/zakani-za-navodno-postaveni-bombi-vo-ucilista-konstatirano-e-deka-prijavite-se-lazni>.
- [52] Ministry of Interior of the Republic of North Macedonia, (2026) “Five Individuals, Four of Whom Are Minors, Detained for False Bomb Threats in Tetovo Schools”, 26 March 2026, <https://mvr.gov.mk/en-GB/odnosi-so-javnost/novosti/liseni-od-sloboda-pet-lica-od-koi-cetiri-se-maloletnici-za-laznite-dojavi-za-bombi-vo-tetovskite-ucilista>.
- [53] F. G. Hoffman, (2007) *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, Arlington, Virginia.
- [54] NATO, (2022) *NATO 2022 Strategic Concept*, adopted at the Madrid Summit, 29 June 2022, <https://www.nato.int/strategic-concept/>.

- [55] W.-D. Roepke and H. Thankey, (2019) “Resilience: The First Line of Defence”, NATO Review, 27 February 2019, <https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html>.
- [56] G. Giannopoulos, H. Smith and M. Theocharidou, eds., (2021) The Landscape of Hybrid Threats: A Conceptual Model, Publications Office of the European Union, Luxembourg, <https://doi.org/10.2760/44985>.
- [57] Council of the European Union, (2022) A Strategic Compass for Security and Defence—For a European Union That Protects Its Citizens, Values and Interests and Contributes to International Peace and Security, Brussels.
- [58] A. Bendiek and R. Bossong, (2020) “Hybrid Threats and the EU’s Foreign and Security Policy”, in B. Lippert and S. Perthes, eds., German Foreign Policy in Transition: Post-COVID-19 European and Transatlantic Perspectives, SWP Research Paper 10/2020, Stiftung Wissenschaft und Politik, Berlin.
- [59] European External Action Service, (2023) 1st EEAS Report on Foreign Information Manipulation and Interference Threats: Towards a Framework for Networked Defence, https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en.
- [60] J. Joseph, (2018) Varieties of Resilience: Studies in Governmentality, Cambridge University Press, <https://doi.org/10.1017/9781316551028>.
- [61] European Parliament and Council of the European Union, (2022) “Directive (EU) 2022/2555 of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union (NIS 2 Directive)”, Official Journal of the European Union, L 333, pp. 80–152, <http://data.europa.eu/eli/dir/2022/2555/oj>.
- [62] European Parliament and Council of the European Union, (2022) “Directive (EU) 2022/2557 of 14 December 2022 on the Resilience of Critical Entities”, Official Journal of the European Union, L 333, pp. 164–198, <http://data.europa.eu/eli/dir/2022/2557/oj>.
- [63] European Parliament and Council of the European Union, (2025) “Regulation (EU) 2025/38 Laying Down Measures to Strengthen Solidarity and Capacities in the Union to Detect, Prepare for and Respond to Cyber Threats and Incidents (Cyber Solidarity Act)”, Official Journal of the European Union, L 2025/38, 15 January 2025, <http://data.europa.eu/eli/reg/2025/38/oj>.

AUTHORS

IlcheDimovski holds a PhD in Political Science from Sofia University “St. Kliment Ohridski” and serves as Secretary of the Faculty of Information and Communication Technologies – Bitola, University “St. Kliment Ohridski” – Bitola. His research interests include hybrid threats, geopolitics, disinformation, institutional and democratic resilience, and Euro-Atlantic integration.



Filip Popovski is a Full Professor at the Faculty of Technical Sciences – Bitola, University “St. Kliment Ohridski” – Bitola. He holds a PhD in Technical Sciences in the field of Graphic Engineering. His research interests include computer graphics, visualisation, graphic engineering, and three-dimensional virtual environments.



Hristina Dimova Popovska holds a Master’s degree in Information Sciences and is an Assistant at the Faculty of Information and Communication Technologies – Bitola, University “St. Kliment Ohridski” – Bitola. Her research interests include computer graphics, information technologies, the Internet of Things, and e-learning systems.

