ISSN 2335-870X
LITHUANIAN ANNUAL STRATEGIC REVIEW
2023 Volume 20

Prof. Žaneta Ozoliņa [*]
The University of Latvia

Sigita Struberga [**]
The University of Latvia

Subjective Perception of Hybrid Threats in Latvia

The concept of hybrid threats plays an increasingly important role in the security studies agenda, as it raises awareness about the multidimensional nature of contemporary security. Hybrid threats are considered hostile activities that involve the simultaneous use of two or more types of threats and are controlled or coordinated by a specific actor, whether state or non-state. Some experts may argue that hybrid threats are the most prevalent type of threat in the European security landscape at present. As a result, the focus of research has shifted to an investigation into this phenomenon and the vulnerabilities that make a country weaker in the face of emerging hybrid threats. However, much less attention has been paid to the subjective perception of hybrid threats in particular societal and historical contexts, as well as their impact on security policy-making. This article analyses the perceptions of Latvian society in regard to its vulnerability to hybrid threats, as well as how these perceptions are reflected in the main security policy documents. It is concluded that the Latvian population recognises certain hybrid threats as being current in their security agenda. This is especially true of information and cyber threats. On the other hand, the analysis of the key national security documents reveals the lack of a well-defined agenda for preventing and combating hybrid threats.

Introduction

The contemporary security environment is unpredictable for a variety of reasons; in particular, potential threats can emanate from state and non-state actors, and they vary in intensity and appearance.

[*] *Prof. Žaneta Ozoliņa*, Senior Researcher at the Advanced Social and Political Research Institute, the University of Latvia, Chairwoman of the Board at the Latvian Transatlantic Organisation. Address: Lauvas Street 4, Riga, Latvia, 1019; e-mail: zaneta.ozolina@lu.lv
[**] *Sigita Struberga*, Researcher at the Advanced Social and Political Research Institute, the University of Latvia, Secretary-General at the Latvian Transatlantic Organisation. Address: Lauvas Street 4, Riga, Latvia, 1019; e-mail: sigita.struberga@lu.lv

https://doi.org/10.47459/lasr.2023.20.6

More and more different experts and politicians are beginning to share the idea that the lines between war and peace have become blurred. As a result, risk assessment becomes an extremely difficult task since it must include a categorisation of each threat by its probability of occurring, as well as the consequences of their impact (Raugh, 2016: 2). Unfortunately, such risk assessment does not work in the case of hybrid threats. This type of threat describes a range of synchronised actions to destabilise the current situation in a target country. What differentiates hybrid threats from other hostile activities is that they are not acknowledged by officials and primarily seek to influence domestic politics (Radin, 2017: 6). Thus, any vulnerability can be exploited by an aggressor to commit such an offence as effectively as possible, which is difficult to predict and deal with the consequences of. For these reasons, an increasing number of hostile actors choose hybrid threats as a tool for achieving their political goals. According to a number of researchers, hybrid threats are currently the predominant form of threat in the European security scene (Giannopoulos, Smith, & Theocharidou, 2021: 4). As a result, the focus of the study has shifted to an examination of this phenomenon. However, less attention has been paid to subjective perceptions of hybrid threats and vulnerabilities, which are important to identify in the context of specific societal and historical contexts and their impact on security policy-making. Thus, the scientific problem of this research is the issue of how members of society perceive different types of hybrid threats and how these perceptions influence security policy decision-making.

Latvia has historically been at the forefront of aggressive hybrid attacks by the Russian Federation, which has also used hybrid threats against Latvia and the other two Baltic states (Estonia and Lithuania) as well as their societies, with the clear aim to re-establish the Baltics within Russia's sphere of influence. As a result, it is not surprising that different types of Russian hybrid operations have been on the daily security agenda in Latvia and the wider region. To achieve its goals, Russia's instruments include: corruption schemes, bribery, cyber-attacks, disinformation and propaganda, economic pressure, energy blackmail and more. At the same time, Russia is not the only actor posing a hybrid threat to the international system. This type of foreign interference is utilised by other state and non-state actors worldwide (Nemr & Gangware, 2019: 2; Pomerantsev, 2020: 90). The Baltic region, for example, is currently facing the activation of another actor — the People's Republic of China.

Latvia possesses certain elements of resilience based on its historical experience that should be considered, as well as a growing body of evidence demonstrating increasing political will to strengthen this resilience. New legislative acts have been enacted, as have policy coordination mechanisms. Different types of societal and other stakeholders' initiatives serve as an example of good practice for many partners in the West. However, several vulnerabilities must still be addressed. One of the main vulnerabilities identified is societal trust in government and participation in democratic processes (Ozoliņa, Reinholde, & Struberga, 2021). It renders the Latvian case study particularly interesting for research.

This article aims to investigate how different societal groups in Latvia perceive hybrid threats and how these subjective perceptions are reflected in implemented policies. The article contributes to the broadening and deepening of security studies by underlining the importance of society in guaranteeing the protection of the country and individuals from potential threats and risks. In the face of increased hybrid attacks, society, which traditionally has been considered a referent object of security, becomes an integral part of security policy-making. Therefore, it is necessary to discover how society in a particular country deals with hybrid threats and whether their perception of threats is consistent with the officially identified security policy. The aforementioned considerations lead us to the following **research question,** which will be answered in the article: **What are the primary hybrid threats identified by the inhabitants of Latvia, and how are these threats reflected in the security policies**?

To answer the research question, the following methodology will be applied:

1.We begin by framing the analytical foundation by examining two concepts: hybrid threats and subjective perception of security.

2.We identify those domains that are relevant for the identification of hybrid threats targeted at potential vulnerabilities in Latvia, such as infrastructure and energy, cyber, societal/social, political, economic, military and informational. These domains were identified in two ways: (1) by examining the methods and means of how the European Centre of Excellence for Countering Hybrid Threats has identified various types of hybrid threats, and (2) by analysing secondary data, primarily opinion polls dedicated to peculiarities of the security environment in Latvia and organising a pilot focus group for further validation of the research methodology. This enabled the development of an analytical framework for further analysis and the creation

of a questionnaire for focus group interviews. Thus, the analytical framework of the research was established through the first two steps of the research and the deductive method of the research.

3.We analysed the results of 11 focus group interviews[10] in different regions of Latvia in 2019. This sample included data from focus-group interviews in the following municipalities: Ādaži, Daugavpils, Gulbene, Jaunjelgava, Liepāja, Ļaudona, Madona, Rīga (2), Rēzekne and Talsi. The municipalities were chosen to cover different socio-political, economic, and geographical contexts[11]. In 2021, focus group interviews were conducted in Daugavpils, Liepāja, Ļaudona and Rīga. This made it possible to test the conclusions of the first round of focus group interviews, as well as to identify changes in the respondents' perceptions as a result of the COVID-19 pandemic. Both times, the questionnaires were created in a systemic manner. The questionnaire began with engagement questions to establish the topic of discussion with participants and make them comfortable with the focus group setting and with one another. These questions focused on such issues as 'What are the main threats you face?' and 'What are the main threats your community/society/country face?' Thus, these open-ended questions allowed the establishment of the subject and tone of the focus groups, as well as for the first reflections of interviewees on the threats they face. Afterwards, the interviewers turned to exploratory questions with a focus on different types of threats, their sources, and their eventual influence. The interviewers explored assessments about threats in the following dimensions: energy, cyber, societal/social, political, economic, military, informational and ecological. These domains were identified in two ways. The interviewees' opinions about the intensity and actuality of these threats were measured, and their sources were identified. The interviewers did not frame the discussion in such a way that the sources of threats or the significance of threats to the national security agenda were initiated by them. The final part of the focus group interviews included exit questions to ensure that there was nothing else the focus group members wanted to discuss about the subject.

4.Finally, we validated the data collected during the focus group interviews in the context of the two main national security documents, the National Security Concept (2019) and the State Defence Concept (2020), which serve as the foundations for Latvian national security policy. The aim of these documents is multi-layered and provides insight into how a country ensures security for the state and its society and provides a clear strategy or so-called national security concept. Thus, it reflects not only an approach towards security matters but also demonstrates decision-makers' attitudes towards the population and level of involvement in developing the national security agenda.

By performing these steps of analysis, we have conducted a study with a solid empirical foundation, thus providing a basis for future research and the development of knowledge in areas where gaps are identified. It means that existing research has engaged with security policy primarily through the analysis of security policy documents or reflection on the security policy goals or perceptions of Latvian decision-makers. Other areas of security scholarship, such as more focused approaches to the perceptions of security and the readiness of society to engage in the implementation of total defence, are still waiting to be aligned with the domain of security studies.

In this paper, the authors introduce the basics for studying subjective perceptions of security and threat perception, thereafter extending this framework to the sphere of security policy and mitigating hybrid threats in particular. The authors explain the relevance of subjective perceptions of security and threat perception to understanding different dimensions of effective implementation of security policies, including those related to the mitigation of hybrid threats.

Defining Hybrid Threats

Debates on the importance of hybrid threats in the Baltic Sea region and other European countries became particularly salient after the beginning of the crisis in Ukraine. The events in Crimea and the Donbas region acted as a warning for the wider European security community as they demonstrated the unpreparedness and vulnerability of the West to these threats (Keršanskas, 2021: 7; Kalniete & Pildegovičs, 2021: 23). The activities that followed could have been insufficient as the present situation has become more complex and dangerous since 2014. Russian aggression has taken on ever new and intolerable forms, which has led to primarily reactive policies from many European countries, including Latvia.

The recently established terms 'hybrid threats' and 'hybrid warfare' might be seen as innovations; however, the activities that are included under the conceptualisations of these terms are as old as conventional warfare or diplomacy (Dunay & Roloff, 2017: 1; Nyberg, 2018; Giannopoulos et al., 2021: 6). Despite that, both terms have no consistent definitions and are used by stakeholders in different ways, and as such, they are interpreted in various forms according to specific contexts. Simultaneously, there are certain characteristics that are relevant to all of the cases demonstrated in related research:

1) hybrid threats consist of one or several types of threats; 2) hybrid threats and hybrid warfare mainly have low predictability, deception, variable intensity, hidden tactics, are long-lasting and difficult-to-prevent consequences; 3) they attack democracies by deepening polarisation in national and international dimensions, deepening mistrust of governments, undermine the images of political leaders and the capability of democratic decision-making, and challenge the core values of democratic societies (Shea, 2018: 11; Giannopoulus et al., 2021: 6); 4). The subject identifies the specificities of geographical, political and socio-cultural contexts in the historical setting of the target society, and only after such calculations does it make decisions regarding further steps to plan hybrid attacks based on these and other relevant indicators (McCulloh & Johnson, 2013: 14-17). According to the US General Dempsey, hybrid conflicts serve to increase ambiguity, complicate decision-making, and slow the coordination of effective responses (U.S. Department of Defense, 2015). It means that the sphere of hybrid operations refers to the grey area of war, where the division between war and peace is blurred, and confusion and disorientation are present. In other words, notions such as 'grey zone conflict', 'hybrid warfare', 'hybrid threats' or 'non-linear warfare' are synonymous in describing this type of situation. It became especially evident after the 2014 annexation of Crimea (Balcaen, Du Bois, & Buts, 2021: 1). States, societies, or certain social groups can become the targets of hybrid attacks. Coordinated action by all national security authorities may also be insufficient, as forces have been set in motion to target the weaknesses identified by the adversary in the system.

In this article, 'hybrid threats' are operationalised as a term that describes a range of synchronized destabilising actions targeted against the current situation or regime in a specific country. What makes hybrid warfare different from other hostile activities is that it is not admitted by the officials and primarily seeks to influence domestic politics (Radin, 2017: 6). Thus, any vulnerability can be used by the aggressor to commit an offence as effectively as possible.

It is important that pending hybrid threats are detected as early as possible. Governmental institutions, security, the private sector, media and civil society must strengthen recognition of the new security environment, different types of threats, how to detect these threats and analytical capabilities related to them, as well as develop an awareness of the eventual consequences in case efforts to resist hybrid threats fail. Such a project undeniably requires more resources and investments, as well as more comprehensive interactions

between the military and civilian, national and regional governments, government officials and representatives of society. The private sector and members of society have the potential to play an important role in helping national governments in the implementation of modern security strategies. Therefore, a key governmental priority should be to identify the types of assets that can help prevent and counter any attacks, including hybrid ones. It means it is only possible to address this phenomenon through a whole-of-state approach.

The main forms of hybrid attacks are: malign information campaigns (propaganda, disinformation, fake news, etc.), cyber-attacks, economic influence, symbolic gestures based on the elements of either historical memory or certain dimensions of identity, corruption and others. The disaggregation of the hybrid threats into different categories makes it more feasible to evaluate the vulnerabilities and the needed responses by target countries. It might help to analyse specific pieces of the system in order to conceptualise and evaluate the entire situation (Dunnay & Roloff, 2017: 2; Radin, 2017: 6).

Such a division makes it easier to identify and comprehend the phenomenon of this threat to the general public outside of a narrow circle of experts. For the development of the analytical framework of the article, several groups of hybrid threat indicators and related domains have been identified. Those domains are as follows: infrastructure, the cyber domain, community/social domain, the informational domain, the policy domain, public administration, the economic domain, and the military domain (see Table 1). This allocation is based on how the European Centre of Excellence for Countering Hybrid Threats, together with the ISPRA, has identified the different types of hybrid threats (Giannopoulos et al., 2020: 13) and is adapted to the perceived hybrid threat landscape by the Latvian society as identified by secondary data - mainly opinion polls dedicated to peculiarities of the Latvian security environment and the organisation of a one pilot focus group for the further validation of the research methodology (Struberga & Ceple, 2021: 169–200). At the same time, it should be noted that this division does not cover all domains of public life nor all varieties of hybrid conflict or hybrid instruments. The table aims to highlight the types of hybrid threats that were identified during the study, analysing the threats and challenges, as well as the fears regarding certain security dimensions that are characteristic of those held by the Latvian population.

Table 1: **Location of hybrid threats in security domains and hybrid threat tools (adapted from Giannopoulos et al., 2020: 13)**

Domain	Examples of hybrid threat types	Examples of mechanisms used for hybrid threats
Infrastructure	Physical intervention in the infrastructure's process Cyberthreats Dependency development of the infrastructure's process	Physical intervention Economic Instruments Development of energy dependency Cyberattacks on infrastructure Investments
Cyber domain	Cyberthreats	Cyberattacks Data Theft Spying Cyber operations
Societal/social domain	Weaponisation of culture, ethnicity, identity	Exploiting social and cultural cleavages Manipulation of cultural and minority organisations and think tanks Creating social unrest Exploitation of diaspora Influencing schooling and academia
Information domain	Informational threat Cyberthreat	Development of media discourse Introduction of hostile narratives through the media Cyberattacks Disinformation campaigns and propaganda
Political domain	Intervening in internal affairs Use of instruments of external affairs Special task force operations	Discrediting of political leaders Manipulation of political forces Corruption Developing and broadening of political cleavages Developing political unrest Weaponiation/instrumentalisation of migration
Public administration	Intervening in internal affairs Cyberattacks Special task force operations	Exploiting vulnerabilities in public administration Cyberattacks Corruption Espionage Exploiting legislation loopholes
Economics	Economic threats Cyberthreats Use of external affair instruments	Development of economic dependency Corruption Creating and deepening economic difficulties Sanctions (Official and unofficial) Investments Use of economic leverage to create political pressure Cyberattacks

Military domain	Military threats Cyberthreats Special operations	Military exercises Cyberattacks Use of paramilitary organisations Military and civil operations of the Special Forces Territorial violations over airspace and waters Cyberespionage
Environment/ Ecology	Man-made catastrophes Cyberthreats	Cyberattacks Polluting Nuclear threats

Regarding the table, it is worth mentioning that the examples of these threats and tools should be allocated in the context of other domains identified here, as well as in other domains not directly mentioned. The main emphasis has been put on those threats and tools identified either by the inhabitants of Latvia or the national security documents analysed in this article.

What is the Subjective Perception of Security Matters?

The resilience of individuals and the ability of a society to interact and cooperate with the public institutions responsible for security policy is of particular importance for national security. A state's resilience and coordinated action in the case of external intervention or crisis becomes functional and efficient if state policies and established security mechanisms reflect the society's subjective perceptions of security before tensions or aggression occur. This means that public policies must be sensitive to citizens' concerns and accumulated security experiences.

Several scholars from the realm of security studies have already underlined the relevance of the subjective perception of security. For instance, Arnold Wolfer indicated the objective and subjective aspects of security already during the Cold War. He emphasised that there are two important dimensions of security to be considered objective — measuring the absence of threats to acquired values, and subjective — measuring the absence of fear that they might be attacked (Wolfers, 1962: 149). This analysis demonstrated a significant distinction between security, which is measurable through objective indicators, neutral parameters and a sense of security, which is subjective and can be volatile depending on several psychological and other difficult-to-measure variables. On the one hand, this dichotomy is contradictory and can spark a wide-ranging existential debate on ontological differences between

reality and opinion. On the other hand, however, it is impossible to discuss security in isolation from subjective indicators, which not only determine the direction of national security strategy but also individual strategies of the population to strengthen their own personal security. The research on this issue within the security studies has principally demonstrated the tradition of viewing subjective security perceptions in the context of decision-making processes as realised by the political elite when organising national, foreign and security policy.

An additional intellectual space in security studies was created only with the development of the Copenhagen School, which emphasised individual-level explanations. This paradigm shift created a common starting point to identify different types of threats and organise them comprehensively. No less important is the role of integrating different dimensions of security, starting from the individual and progressing up to the international, while also building a common point of reference for a broadened comprehension of security.

Criminological research shows that the perception of the security of the population is not determined by the high readings of the criminogenic situation but mainly by order in public spaces. These studies also highlight a growing sense of insecurity in European societies despite an overall improvement in the criminogenic situation (Gullien-Lasierra, 2021: 1, 3). At the same time, as Boby Duffy rightly points out, few studies of subjective perceptions have been conducted that address the misinterpretation of perceptions. He explains this lack by the relatively recent inclusion of this topic in the research agenda and, consequently, by an absence of empirical evidence. Public opinion polls on the perception of social reality have been initiated only recently, beginning in the middle of the 20th century. Even afterwards, the number of relevant polls has remained relatively small (Duffy, 2018: 7-8).

Many studies show that subjective perceptions of security largely depend on individual factors such as age, gender, ethnicity, ideological or religious affiliation or psychological profile (Gullien-Lasierra, 2021: 6). It is for this reason that it is important to look for broader answers through research methods such as focus group interviews, in-depth interviews or snowball research. Due to an in-depth understanding of the population's subjective perception of security, it is possible to better understand the public view of threats that may differ from those defined in national policies to develop security and defence policies that reflect synergies between security professionals' responses and threats. 'The existence of such synergy is a condition for the change of attitudes and behaviour of civilians, which increases the ability of the population to protect themselves' (Ozoliņa, Reinholde, & Struberga, 2021: 19).

Furthermore, knowledge about societal perceptions and how

these perceptions are being taken into account in the decision-making process has particular importance. The national security might be characterised as a whole community enterprise. Thus, it is possible to strategically define it as 'a concerted national effort: a nation-wide comprehensive activity, including all of the government across federal, state, local, territorial and tribal levels of government; all first responder communities; the private sector; and a vigilant public' (Siedschlag, 2021). It means that the total security system in the country relies on each stakeholder and its readiness to act. However, the readiness to act and follow governmental regulations depends on how the government is perceived, how the particular threats are evaluated, and how much an individual believes his or her views and evaluations are implemented in these policies. The COVID-19 pandemic has demonstrated how indispensable it is to be aware of public perceptions and understanding, as well as the particular needs members of society have. It is also important to know how communities perceive and react towards particular threats and to the security policies that could counter them. The success of security policy can ultimately be defined not only by the value of its goals but rather from a perspective of implementation, meaning that security policy might be self-explanatory in its implementation, delivered to the members of society in their everyday lives, and perceived as responding to security concerns.

Subjective Perception of Hybrid Threats in Latvia

Latvia, like other transatlantic countries, is facing a full spectrum of hybrid threats. The rise of hybrid challenges, which began in 2014 with Russia's occupation of Crimea and interventions in Eastern Ukraine, is one of Latvia's most serious security concerns. The contemporary regional security environment, when taking into consideration the unpredictable and increasingly hostile activities of the Russian Federation, necessitates the urgent need to fill knowledge gaps, including those related to the investigation of how hybrid threats are perceived by different groups of society, and how these views and fears are reflected in the main national security strategic documents that establish the direction of national security policy development.

One of the main findings of the research is that the Latvian population understands the importance of certain types of hybrid threats. These perceptions are consistent with how these threats are described in the National

Security Concept and the National Defence Strategy. Both focus group interviews and national strategic documents identify the Russian Federation as the main external threat to national security. When analysing secondary data, the results of different public opinion polls show that during the pre-pandemic period, most Latvians acknowledged their concern that war and conflict could endanger their lives (Krumm et al., 2019: 44-45). More than half of the Latvian population considered the Russian Federation to be the most significant external threat to the security of Latvia and Europe in the period from 2016 to 2019 (Diamant, 2017; Krumm et al., 2019: 44). The population of Latvia has identified the hybrid threat as significant among the various types of threats. The population is particularly concerned about the threat to the information environment. For example, in the 2015 survey of the market research company 'Latvijas Fakti' for the needs of the Security and Strategic Research Centre of the Latvian National Defence Academy, 61 per cent of Latvian respondents considered that one of the most important measures to strengthen national security is to provide Latvian media broadcasting at the border regions (Bērziņa, 2015: 15). However, according to the Eurobarometer survey for 2018, 74 per cent of Latvians were concerned about disinformation and misinformation on the Internet (Eurobarometer, 2018).

The results of secondary quantitative data analysis in the context of the pandemic demonstrate that this crisis increased public anxiety and concern. Anxiety about the future causes people to perceive the world as a less safe place. The crisis caused by the COVID-19 pandemic has created new debates about the moral and subjective nature of insecurity (Guillen-Lassiera, 2021:30). Latvia is no exception in this regard, and the analysis in this article demonstrates that, on the one hand, the security challenges that Latvians face in the context of hybrid threats are constant, but on the other hand, it shows the dynamic nature of subjective perceptions.

In four of ten municipalities where the focus group interviews were conducted, residents identified hybrid threats as one of the three most significant types of threats. At the same time, it is worth noting that none of the residents of these municipalities identified this type of threat as the most significant. The Russian Federation was mentioned as the most significant external source of hybrid threats in all regions. In other focus groups, people also named the People's Republic of China. However, in none of the cases was the country viewed as a deliberate and immediate source of threat, but rather as a significant unknown factor with rapidly growing international power that could pose security challenges in the near future. Non-state actors were not identified as a potential source of hybrid threats by any of the focus groups polled.

It is worth mentioning that during the focus group interviews,

respondents rarely, if ever, used the term 'hybrid threat' to describe their concerns about the threats described as hybrid threats in security studies. Other terms and various styles of articulation were used to describe it. It can be concluded that the Latvian population generally considers specific forms of hybrid threats as significant for them. However, it is not possible to speak of comprehensive knowledge that would allow it to be contextualised and seen in the broader context of the damage caused by hybrid threats. At the same time, this circumstance is not regarded as a significant obstacle because it has no effect on its substance.

The National Security Concept and the National Defence Concept both identify Russia as the major source of external threats in a number of domains, as well as express concern regarding rising insecurity in the region due to increasing hostile activities. Hybrid threats are mentioned as one of the main sources of anxiety in line with military and other threats (The National Security Concept, 2019; The National Defence Strategy, 2020). Although the term 'hybrid threats' is used not so extensively in both documents (especially in the National Defence Concept), the most common types of hybrid threats are identified and analysed as permanent sources of security concerns.

Hybrid Threats in the Infrastructure Domain

The most common threat mentioned by the Latvian population in connection with hybrid threats in the infrastructure domain was related to transport infrastructure. Here, the respondents identified the low quality of Latvian roads as the most significant source of vulnerability.

A respondent in Daugavpils municipality: The infrastructure in Daugavpils municipality is not safe. The bridge over the river is also, sorry, regarded as safe. I'd like to see how a tank can cross our bridge.

A respondent in Gulbene municipality: Roads are in critical condition. Practically unusable. There was a reason the president flew here by helicopter… So that he would not have to travel on these roads.

The network of petrol stations is noted, among other issues with the transport system.

A respondent: We do not have a gas station here. Fuel supply is a problem for the people here. You have to ride far to get it.

In other regions, residents were concerned about the network of hospitals in the country. Such concerns have been caused by the limited availability of healthcare services in remote parts of the country. For example, it is not possible to receive the services of an on-call traumatologist due to the lack of specialists

in some regions of the country. Hospitals in rural regions do not have the necessary equipment to provide a range of necessary healthcare services.

A Respondent in Ļaudona municipality: Neither we nor our nearest counties can receive certain essential medical services; this poses many challenges for the people of the region.

The results of the two groups of focus group interviews in 2021 showed identical concerns. The responses indicated that the problem was long-lasting and systematic and that the challenges posed by the COVID-19 pandemic had exacerbated it. It can be concluded that the hospital network, as a part of the critical infrastructure, is associated with several vulnerabilities from the point of view of the population.

Only in a few cases was the infrastructure of national defence objects considered a source of vulnerability. Citizens were more often persuaded that the responsible authorities to provide could provide the necessary protection. For example, in a municipality where a hydropower plant is located, respondents indicated a sense of security and a high level of awareness of potential risks and their prevention.

A respondent in Aizkraukle municipality: I rely on the responsible authorities — they know what to do; there is a plan, and safety is ensured.

However, in a municipality adjacent to the district where the hydroelectric power plant is located, there are some concerns of the population regarding this critical infrastructure. Its citizens associate it with potential risks in the event of an accident, as well as with uncertainty about how to act in a crisis.

Two other municipalities included in the study have the largest military bases in the country. It is interesting to note that, while the location of these objects is related not only to national but also personal security in both cases, the threats identified by respondents in this regard were mainly related to the military and not to any other aspect.

Focus group interviews conducted in 2019 revealed a lack of interest in potential threats to national border security. This is also relevant to municipalities bordering Russia and Belarus. Respondents indicated a preference for more local cross-border cooperation without national intervention.

In a focus group interview conducted in September 2021 in the same Belarusian border municipality mentioned above, respondents stated that they felt threatened and alone in the face of the Lukashenko regime's migration crisis. According to the respondents, neither national nor European political leaders have taken the issue seriously enough.

A respondent in Daugavpils municipality: We are on the front lines. Migrants are here next door, but we do not see any support from either the national level or Europe. When a migration crisis hit southern Europe, Frontex was present. Where is it now?

None of the discussions on infrastructure security issues identified cyber threats as significant. In both the 2019 and 2021 focus groups, hybrid threats in the energy sector were not mentioned as significant. The findings in both cases indicated that rising energy prices appeared to be a more realistic threat than energy issue weaponization against Latvia.

The National Defence Concept refers to infrastructure in terms of military infrastructure with the need for the development of a well-organized and strengthened network of them (National Defence Concept, 2019). In turn, the National Security Concept specifies such hybrid threats as new types of spying on military objects, e.g., the use of drones or cyber espionage. Cyberinfrastructure itself and the potential risks of the increasing interconnectivity and new technologies such as 5G internet networks are receiving equal attention. Contrary to public perception, policy documents identify threats to energy infrastructure and supply as an important source of security concerns. The need for diversification of supply is seen as the most important step toward reducing reliance on deliveries of non-renewable energy resources from Russia.

Cyber Threats

In the scope of this article, the cyber environment domain is highlighted as a separate analytical unit, yet at the same time, cyber threats, as potential hybrid threats, are also considered in the context of other domains, such as potential threats to public critical infrastructure or public administration.

According to the findings of a 2019 focus group interview, Latvians have generally considered cybersecurity challenges. At the same time, it should be noted that the primary concern is related to personal internet security rather than potential cyberattacks that could jeopardise other aspects of social life or pose a threat to national security. Respondents in all Latvian municipalities where focus group interviews were conducted expressed concern about the security of personal data in cyberspace. In particular, the majority of respondents were concerned about the security of their data. This is especially true for bank data and individual savings.

Focus group interviews also highlighted concerns about the content of social networks. During these interviews, respondents also expressed concerns about a lack of direct marketing and personal data protection, as well as a

careless approach to the use of social networks and other Internet resources, and the impact of artificial intelligence on information space.

A respondent Madona municipality: Artificial intelligence is an issue that needs to be addressed at the national level because we are not aware of how we put our security at risk.

Interestingly, respondents who expressed concern about security on social media also expressed confidence that this type of threat posed potentially less risk than others, especially for respondents of other generations. Adolescents and young people are most often identified as the most vulnerable portion of society for several reasons: the large amount of time that young people spend online, lack of media literacy, and various forms of cybercrime (mobbing, blackmail, extortion, and sexual and emotional abuse).

A respondent from Talsi municipality: It is very easy to fool people who do not have experience with critical thinking in the Internet environment. For example, hidden advertising can be found in music that leads children to harmful habits. It has a very serious impact.

However, representatives of the younger generation are of the opposite opinion, stressing that the representatives of the older generations lack the necessary knowledge and competencies.

A young man from Madona Municipality: Young people already know how to act online. But the older generation is more at risk. Many know of examples of older people's communication with false Nigerian princes.

The results of the 2019 focus groups showed some carelessness and inaction in strengthening personal safety in the online environment among all generations.

Respondent, Valmiera municipality: Such a possibility of cyber threats, of course, exists. But I don't want to think about it and worry about it.

In 2019, three municipalities discussed the introduction of the most recent 5G mobile communication technology as one of the potential security challenges for Latvian society. Interestingly, two of the municipalities discussed the potential risks to public health associated with the introduction of new technologies. Meanwhile, the third municipality discussed a conspiracy theory regarding the negative effects of 5G. In the results of the focus group interviews in 2021, this issue was no longer identified as significant. This is not surprising, given that the introduction of technology in the country has begun, and this issue is no longer on the public agenda. At the same time, conspiracy theories are currently focused on topics related to the COVID-19 pandemic,

such as its origins, its spread, and government action to prevent it.

From September to November 2021, the focus group interviews highlighted dissatisfaction with the Latvian government's response to the pandemic, distrust of official morbidity rates, and concerns about the resilience of the Latvian economy to the crisis.

> *A respondent, Madona municipality: No one doubts that there is a pandemic, but this testing is kind of weird. The government does strange things, it only informs us on what it wants us to know. We do not get valid information. It stays there, in Riga.*

It can be concluded that respondents did not see cyber threats as a priority challenge for national or local security in both 2019 and 2021, which differs significantly from policymakers' views. In both policy documents, cyber threats are regarded as one of the most difficult threats. Nonetheless, citizens are viewed as "clients," learners to be reached, and the greatest emphasis is placed on system improvement, promotion of cooperation among public administration institutions, and civil servant training (National Security Concept, 2019; National Defence Concept, 2020). The role of civil society in strengthening cybersecurity is rather underestimated. According to regional and global tendencies, cyberattacks on the civil society sector are on the rise, and the main challenge is that few of the civil society representatives have even basic security policies or procedures (Christine & Thinyane, 2021). Strengthening civil society's cybersecurity capabilities and cyber competence is not only about its own security or that of certain groups within society. Eventually, the involvement of civil society in creating mechanisms of national cyber defence against malign operations can have valuable and far-reaching consequences. As previously concluded, using 'multistakeholder processes, states can support civil society engagement on many other aspects of cyber risk reduction, including in discussions on norms, consideration of regulatory practices, procurement, and other incentives structures that foster support for collective action on cybersecurity' (Stifel, 2019).

The National Security Concept (2019) recognises the importance of creating well-organised monitoring of the content created by individuals. At the same time, the role of active citizens in monitoring cyberspace and taking care of their cyber hygiene is not mentioned as an integral part of the common cyber defence system. It may have negative consequences, given Latvian society's overall low level of cyber competencies, because it excludes grassroots-level monitoring carried out by active citizens, who may be able to provide certain early warning capabilities.

Hybrid Threats in the Information Space

The challenges identified in the cyber threat analysis for social media are not only closely linked to the cyber domain but also to the security of the informational environment. Latvian residents most often recognise the threats in the informational space mainly by associating them with the information campaigns by the Russian Federation. The negative effects of fake news are particularly emphasised.

Respondent in Valmiera municipality: Information war is proceeding. We have no tools to fight against it. How can one control public and digital space?

This pattern was evident in both 2019 and 2021. However, the results of the 2021 focus groups revealed a distrust of Latvian national media. Several respondents stated that they felt they were subjected to propaganda from both sides. This echoes the narrative forwarded by the Russian Federation - "everyone lies, no one can be trusted".

The results of focus group interviews in 2019 showed that the subjective assessment of the relevance of these threats in an individual's life and different regions of the country differs between the residents of different regions of Latvia. For example, in the Western and Central regions of Latvia, the respondents surveyed in focus groups believe that information threats such as propaganda and misinformation are mainly related to the Eastern (Latgale) region of Latvia.

A respondent, Ādaži municipality: The state is not doing enough in the field of security. There is no state radio and television in Latgale. But it is an ideological weapon that resounds across borders ... there are even members who do not realise it.
A respondent, Liepāja municipality: Russian propaganda and the information war applies to Latgale.

In turn, the assessment of the greatest vulnerability of the Latgale region to information threats in other regions is determined by comprehension of the peculiarities of the national composition in the region, together with its physical proximity to the Russian Federation, as well as the discourse offered by the Russian-language media.

Residents of Eastern Latvia noticed a significant, but not a priority, threat to the security of the information space in 2019. Simultaneously, in both 2019 and 2021, the respondents in the Eastern regions of Latvia expressed awareness regarding the opinion of the residents of Riga and other regions regarding themselves. At the same time, these groups were aware of manipulation in the information space, which they found to be undesirable and negatively affecting the informational environment. Thus, participants

in focus groups interviewed in Rezekne and Daugavpils municipalities, for example, indicated that they are aware of Russia's threats to the information space, such as the dissemination of propaganda and false news.

A respondent, Daugavpils municipality: I would like to disagree that our neighbour has no interest in Latvia because then no one would build television towers on the border. It is all for us and, therefore, makes us wonder why something like that is needed.

Neither in the east of the country nor elsewhere has this hybrid threat been identified as a major security challenge. However, the assessment of the significance of hybrid threats varied by location. There could be several explanations for these differences in a subjective assessment between regions. First, in regions with a more difficult socioeconomic situation, the population's attention is drawn to other issues. Second, the subjective self-assessment of the population about personal media literacy and resistance to various issues of informational manipulation in Latvia, in general, is characterised by optimism. They believe that the challenges of media literacy or critical thinking are typical for others - another generation, representatives of other regions, or other nationalities (Latvijas Fakti, 2017; results of focus groups).

A respondent, Daugavpils municipality: I watch television very rarely, I use the computer more, and it is more accessible. I think that is safe.

A respondent, Valmiera municipality: The information war is already ongoing all the time. And we have lost in some way. Russian propaganda has been spread, and people have seen and believed it. For example, they believed that we did not need NATO. It is not good.

The findings of the 2021 focus groups demonstrated the growing significance of informational threats to citizens' concerns about their security. Anxiety about being in an information war intensified in all focus groups. However, the respondents did not see this as a significant personal challenge. Surprisingly, in the context of the migration crisis, residents in the municipality bordering Belarus indicated that they felt competent enough to distinguish false information from true information.

A respondent, Daugavpils municipality: We are in an information war. But this does not mean that we would not be able to distinguish propaganda from the truth, as it might seem to someone in Riga.

In all focus groups, in both 2019 and 2021, respondents were asked about the influence of the Russian media and agreed that it should be assessed negatively. Most respondents agreed that Russian media content led to disinformation and the consumption of propaganda.

A respondent, Rēzekne municipality: In the border areas, they watch Russian media and feel more emotionally belonging to the Russian media space.

A respondent, Rīga municipality: I recently spent five days in Kyiv. What the Russian media are telling us is that Fascists roam the place, Nazis are stealing everything, and homeless people have nowhere to turn to. Those media are driving people in fear, saying that, for example, if one starts speaking Russian aloud on the streets, they will get beat up. It is nothing like that. The Russian media destabilizes your inner sense of safety.

The Latvian population chooses the Latvian media as its main source of information. In general, they enjoy a relatively higher level of public trust than other social or political institutes (Zelče, 2018: 510). In 2019, some focus groups expressed concern about the activities of the local, especially regional, media, and, in the opinion of the respondents, they served some hidden political interests.

Respondent, Daugavpils: At the regional level, the media are used as mouthpieces for political forces that slander each other. National media are not used here.

Significantly, some people with more radical views were confident that the media had a negative, if not destructive, effect on public perceptions of security. In both focus group interviews in Riga in 2019, some respondents mentioned attempts by the Latvian media to deliberately create negative public perceptions about certain specific events or foreign policy actors. Examples include the general portrayal of the migration crisis in Europe and the intensity of negative news about Russia's aggression on the Internet portal "Delfi" to intimidate the population. In Aizkraukle, on the other hand, respondents pointed to such views as the result of spreading conspiracy theories, which are a threat in and of themselves. No other informational manipulation was identified as an existing or potential threat in any of the focus groups.

In the focus group interviews of 2021, not only were there more concerns about the spread of misinformation, but separate respondents from all groups made assumptions that could be considered a result of misinformation. For example, in the municipality of Madona, a respondent expressed the view that the COVID-19 crisis was artificially created to serve the interests of the Western economic elite. In Daugavpils municipality — the East of Latvia — a respondent pointed out that the European Union had purposefully destroyed the manufacturing industry. In turn, for example, in Daugavpils, almost all the respondents discussed NATO as an instrument for the realisation of US interests, emphasising that the national interests of small countries such as Latvia are suppressed. All these views coincide with the narratives of

disinformation campaigns offered by Russia.

Several focus group interviews were confident in the significance of the role of social media in raising security awareness. It was considered that if any threats are portrayed in the media, it leads to wider reflection and discussion among the population, as well as changes in the agenda of local governments. Considering several important factors, this dual treatment of media is not surprising. First, distrust of the media, like any other social institution, is a historical legacy of the Soviet Union. Second, the current multidimensional, highly interactive, and intense media environment creates conditions in which individuals have particular difficulty in distinguishing opinion from facts, manipulative messages from news, and propaganda from objective strategic communication. Third, misinformation and false news, as well as conspiracy theories, have gained support among the Latvian population. If in 2019, it was possible to relate this phenomenon mainly to the less educated population of the regions, then the 2021 population surveys, as well as the focus group interviews conducted within the framework of this study, show a more complicated picture. In the autumn of 2021, some highly educated and well-off respondents made several assumptions that are also related to false information and conspiracy theories. This leads to the conclusion that in the conditions of a pandemic, the population has become more susceptible to various types of information manipulation.

Hybrid threats in the information environment were identified and interpreted as one of the most significant challenges in all focus group interviews. Most respondents believed that media literacy and critical thinking were the most effective tools for combating the effects of propaganda and misinformation. The results of the surveys in 2019 and 2021 confirm that the population understands the importance of these two competencies in strengthening security.

The National Security Concept (2019) has a special chapter dedicated to the threats in the informational space. This type of threat is considered one of the major, if not the most topical, threats to national security. Special emphasis is placed on the need to protect the diversity of the media space as a guarantor of democratic processes. The policy document acknowledges the challenges associated with the need to support local media in Latvia's regions. At the same time, there are no clear mechanisms in place to support local journalism, and the informative newspapers of local municipalities are chastised for including private advertisements (National Security Concept, 2019). The National Defence Concept (2020) pays equal attention to the security of information space. Promotion of media literacy and strengthening of strategic communication are seen as tools for strengthening it.

The Russian Federation is widely recognised as the most active actor in creating hostile narratives against the state and the stability of the society. Both Concepts acknowledge malign information campaigns and disinformation as the most common attributes of hybrid attacks. The tools for promoting this type of information campaign are mainly television channels and social media platforms. These are significant conclusions that lay the groundwork for the further development of appropriate policies. On the other hand, while the paper acknowledges the inability to transmit national broadcasting at the Eastern border regions, no solutions are offered to resolve this issue after 30 years of debate.

Hybrid Threats in the Societal Domain

Exploiting social and societal vulnerabilities is one of the most common types of hybrid threats used by both governmental and non-governmental actors. Focus group interviews in 2019 and 2021 reveal that Latvians are concerned about social security threats. The Russian Federation was named as the most serious external threat to public safety. The most significant type of hybrid threat identified by 2019 focus group respondents was societal division based on linguistic affiliation. It was also noted that Russia promotes ill-natured coexistence of two distinct communities — Latvian and Russian-speaking — not only through various influence campaigns but also through conditions unrelated to the hybrid threat. The most important of these were the government's policies.

The instrumentalisation of the Latvian Russian-speaking community to achieve political goals is the focus of many studies on Russia's influence. In this respect, the 2019 focus group interviews did not reveal anything novel. Comparatively, the focus group interviews of 2021 brought new nuances to the deepening divisions in society due to new internal societal contradictions and the formation of mutually hostile groups — COVID-19 vaccine advocates and anti-vaccine supporters, nationalists and globalists, and defenders of traditional values and liberal freedoms. In the context of hybrid threats, such a wide-ranging division and deepening of contradictions make the societal domain one of the most vulnerable domains of social life in Latvia.

The National Security Concept (2019) emphasised societal security issues as well. Special attention has been paid to the need to strengthen social cohesion and to promote the inclusion of the Russian-speaking community in the national socio-political processes. According to the Concept, this type of activity has the potential to strengthen the sense of belonging and promote psychological resilience against external ideological and informative activities. An important issue discussed in the concept is the involvement of

non-governmental organisations that represent ethnic minorities within the environment of the Latvian mainstream NGO networks. Another critical issue is the continued promotion of Latvian language familiarisation among non-Latvians. However, the concept's motivation to do so, to provide the ability to communicate with the entire population in Latvian during crises (National Security Concept, 2019), raises concerns.

Hybrid Threats in the Domains of Politics and Public Administration

In focus group interviews, hybrid threats aimed at destabilising the political system in the country and questioning the legitimacy, stability, or ability of the existing political system to make decisions of public importance were the least discussed topics in both the 2019 and 2021 focus group interviews. Although there are concerns in the media discourse about possible attempts by external forces, in this case, Russia, to sow distrust of the government or to otherwise destabilise the socio-political situation in the country with the support of political parties or non-governmental organisations, Latvians do not see this as an immediate threat to national security.

A respondent, Valmiera municipality: Well, it is clear that Russia is trying to interfere in Latvia's internal political affairs daily. It happens all the time. Yet, during the last 20 years, they have not needed us all that seriously.

The 2019 focus group interviews covered many discussions about corruption and unclear deals in municipalities. Respondents frequently mentioned government instability, as well as the gap between the population and the government or the centre and regions, as well as other challenges related to this group of threats. However, it was mainly domestic that seemed to be more important to the respondents rather than the role of possible external actors in fomenting such issues. In fact, no one in the focus groups mentioned that the perpetrators of corruption, political order, or a schism between the population and politicians, or the regions and the creators of the centres could be found outside the country. In turn, the Riga focus group repeatedly expressed concerns about Western pressure, particularly the United States, as a result of which important political decisions are made in Latvia, and the policies in the interests of this actor are implemented, for example, in the public finance sector. Simultaneously, political dependence, particularly on the banking sector, was highlighted. In 2021, focus group interviews revealed that such anti-American sentiments were noted in several interviews. However, in most cases, it was stated that the United States is also the guarantor of Latvia's

military security, and the two issues were regarded as one.

Looking at the potential threats associated with the work of state and municipal administrations in the digital environment, neither in 2019 nor in 2021 was the population particularly concerned about potential threats related to attempts to stop their activities through cyberattacks.

A respondent, Valmiera municipality: I know that cyber security on the websites of institutions is a daily issue, also in my workplace. However, I am not worried about it; others are being paid to worry about it.

In addition, the results of the 2021 focus group surveys also demonstrate that citizens do not consider digitalisation a priority. However, these responses also indicate that the general public is unaware of the opportunities and risks associated with the digitalisation of public administration.

A respondent, Daugavpils municipality: It is not relevant at all in Latvia. Everything is fine with digitalization. We have the fastest internet in Europe, as was reported somewhere.

In general, the results of the focus groups in 2019 and 2021 concluded that, despite the growing gap between the population and the government, as well as the regional and national level, the surveyed Latvians do not see external interference as a significant factor. Dissatisfaction with the work of the government is highlighted, as is corruption — mainly at the national level. Concerns about the potential dangers of political unrest have been raised during concentration group interviews in 2021. The rise of populist forces in politics, as well as the use of various manipulative information techniques to gather votes, were cited as sources of discontent.

In 2021, the weaponization and instrumentalization of migration were also discussed. A focus group interview near the Belarusian border highlighted this particularly. Interestingly, despite these reservations, respondents emphasized the importance of continued cross-border cooperation with both Russia and Belarus, deeming it critical for the region's economic development. During the interview, respondents expressed a desire to separate political issues from economic ones, as well as an assumption that manipulation in the information space stems from both sides. Such distrust in the strategic communication of Latvian public administration institutions is the natural result of the government's communication mistakes and other internal problems in the political system. However, this does not mean that there is no external intervention or no external negative factors.

The level of trust towards political institutions in Latvia is considered a source of threat by the National Security Concept (2019), which is a significant issue to be considered. The need for a strong, cohesive society is mentioned as

an important element for safeguarding internal security and the constitutional order. On the other hand, the concept itself could have the potential to stress the deeper involvement of an active citizenry in strengthening different security dimensions that could potentially provide a stronger foundation for building trust between security policy decision-makers and the population.

Hybrid Threats in the Economic Domain

Latvians are concerned about threats to the economy, as well as about their economic well-being, but the threat is not mentioned at all or is rarely mentioned in conjunction with possible hybrid threats, according to the data gathered from focus group interviews in both 2019 and 2021. In the focus group interviews of 2019, interference in the internal affairs of the state using economic or financial instruments was mentioned as a potential threat in two focus group interviews in the Talsi and Rēzekne municipalities. In both cases, the Russian Federation was mentioned as the source of this type of threat.

A respondent, Talsi municipality: Russia will not come here with war. Russians invest a lot in Latvia. They will come differently — through companies, buying property.

A respondent, Rēzekne municipality: There is a probability that the Ukrainian scenario could be repeated, but it rather depends on internal policy — how much support Riga could provide to Latgale. Latgale is not being supported enough to feel safe - financially.

In 2021, in addition to the Russian Federation, people also mentioned the People's Republic of China in the context of the economic sphere of hybrid threats as a possible source of danger. In an interview with the Riga Municipality focus group, participants pointed out the challenges in securing the supply of critical goods in the early stages of a pandemic.

A respondent, Rīga municipality: The pandemic crisis has clearly shown how dependent we are on China in the context of critical supplies. If China wants to force Europe to do something, the government will not have too many choices. Now, those negotiations on building strategic independence sound somewhat overdue. Is that even possible anymore?!

According to the study's findings, the Latvian population is aware of the country's current economic challenges, but they rarely pay attention to the potential risks associated with hybrid economic threats. In the municipality of Madona, for example, when asked about possible hybrid economic and financial threats, respondents primarily focused on their sales opportunities for Latvian agricultural products in neighbouring countries such as Russia

and Belarus. In turn, the Daugavpils focus group emphasized the importance of promoting trade with these countries while ignoring their political backgrounds. At the same time, it is important to note that members of the public are not required to understand the mechanisms for imposing sanctions and their effectiveness, as well as the country's macroeconomic indicators or the full range of national security challenges confronting security policymakers.

The National Security Concept (2019) stressed the importance of economic threats in the Latvian security landscape. The main sources of threats are mentioned as follows: energy supply chains, shadow economies, and the political ambitions of certain regional and global players (mainly Russia) to interfere in the internal political processes of Latvia through economic pressure. A wide range of solutions is offered in the concept to deal with this type of threat, which means that the country demonstrates high interest and readiness for the prevention of potential risks in the economic sector.

Hybrid Threats in the Military Domain

Hybrid threats in the military domain include external influence instruments such as military exercises, cyber-attacks, the instrumentalization of paramilitary organisations, military and civilian operations of special forces, air and water territorial violations, and cyber espionage. One of the most recognisable types of these hybrid threats among the Latvian population is the hidden interference of foreign military personnel in the internal affairs of the country or supporting armed rebels. In 2019, respondents identified this hybrid threat as the 'Ukrainian scenario', meaning the annexation of Crimea by the Russian Federation and the aggression in eastern Ukraine when armed people of obscured or disguised nationalities attacked or put pressure on public authorities, thus overthrowing the then active bodies of power. A repeat of such a 'Ukrainian scenario' in Latvia was not ruled out by any of the focus groups polled. However, most respondents admitted that this possibility was remote, citing Latvia's membership in NATO as a security guarantee or Russia's lack of interest.

A respondent, Talsi municipality: If Russia wanted to carry out a serious military attack, it would have happened a long time ago, and nothing could stop it.

The Latvian population interviewed in the 2021 focus group interviews was no longer so optimistic, and the devolution of Russia-Europe or Russia-West relations was emphasized in each of the interviews. However, at the same

time, respondents also indicated that they would prefer to build a favourable relationship based on economic interests. In the Daugavpils municipality, members of the focus group pointed out NATO pressure as a reason for Russia's military exercises on the border. The focus group in Ļaudona discussed that, from their point of view, the aggressive rhetoric of the West had provoked a sharply negative reaction in Russian foreign policy, also aimed at Latvia. At the same time, however, these respondents considered the 'Ukrainian scenario' to be impossible.

Despite the fact that Latvia is regularly subjected to territorial violations of its airspace and water by Russian military forces, the Latvians interviewed in focus group interviews did not perceive it as a significant threat. However, this does not imply that respondents regard this as normal but rather as a form of 'vandalism' of great power.

The National Security Concept (2019) provides a comprehensive insight into potential military threats, as well as further steps to strengthen military security through deterrence, international cooperation, and developing national military capabilities. Hybrid threats are not mentioned in this context but rather seen as an integral part of the possible military intervention scenarios. The National Defence Concept (2020) is more precise in this aspect. It underlines Russia's inability to challenge NATO in the form of a full-scale global conventional war. Therefore, hybrid warfare is considered to be one of the most realistic options for Russia. The Defence Concept characterizes hybrid threats as permanently present and creating high risks for Latvia, which necessitates the promotion of societal resilience and the ability to react quickly in ordinary life, as well as in the case of military aggression (The National Defence Concept, 2020). Simultaneously, the document itself focuses primarily on military forces, military-civilian cooperation, and governmental organisations. Citizens are viewed as thinkers rather than full-fledged stakeholders.

Hybrid Threats and Environmental Security

The results of focus group interviews in 2019 and 2021 showed that Latvian residents do not consider environmental security issues a priority. Respondents have also given little thought to the potential challenges and patterns of their behaviour in the event of a hybrid threat, such as an environmental disaster or a technological crisis. Even less thought was given to the possibility that such crises could be the result of intentional action by an external hostile actor. The responses of respondents to the 2019 focus group interviews show that the population lacks sufficient knowledge in their self-assessment of how to react in crises, nor are they prepared for them. Respondents, for example, were unable to answer the question of where water

would be available in a crisis.

A respondent, Liepāja municipality: If we, as a society, are not ready for smaller-scale crises, would we be ready for something of a more significant scale? There is a lot to do here in this matter.

According to the respondents, they have not received enough information about this type of potential challenge. The most important factor in this issue is the national level of public administration, not the local municipal level. Consequently, public administrations are expected to take responsibility for this communication.

A respondent, Ādaži municipality: The state does not have a clear vision of what it wants from the population in a crisis.

The mood of the respondents in Valmiera and Aizkraukle municipalities was more positive than elsewhere in Latvia. The residents of Valmiera were convinced that they would feel quite safe in the event of possible threats in crises, as the municipality, the National Guard, and other responsible parties had participated in joint exercises and gained knowledge on how to act in the event of a technogenic disaster. They surveyed Valmiera residents, who are also pleased with the municipality's observed activities in crisis prevention (for example, the operation of the Gauja River water level measuring station).

A respondent, Valmiera municipality: I know that in Valmiera, the National Guard works in the Civil Protection Council. And the council is always planning and thinking about possible crisis situations.

Residents of Aizkraukle noted that they know where to turn in case of a significant threat situation. However, in comparison with Western warning systems, the need to improve the existing procedures in Latvia and to introduce notifications utilising text messages on impending dangers and appropriate instructions on how to act in the event of a crisis was noted. Respondents believe that the introduction of such a form of communication is a matter for the state, not the municipality. In two settlements — Talsi and Ļaudona (Madona district) — respondents indicated that they would feel safe even in the event of a possible disaster. In the first case, the answer was that Talsi is a safe city. The people of Ļaudona, on the other hand, emphasized that both their geographical location and public policy had isolated them from the rest of the world.

The results of the 2021 focus group interviews show that the population's interest in and awareness of behavioural algorithms in a crisis has grown. For example, in the Ļaudona focus group, one of the key issues in which the European Union should get involved in improving the state of the environment in the waste management industry. At the same time, the general population

in the country is still unaware of the potential risks that may arise from hybrid threats in the context of environmental security.

Respondents know very little about the functions of the state and municipality in the described situations. There is especially little information on personal responsibility and preferred patterns of behaviour in times of crisis. The results of the 2021 focus group interviews show that the Ministry of Defence's implementation of the Comprehensive National Defence Initiative has yielded some results; however, there is still much work to be done. For example, while it is encouraging that a small proportion of respondents have heard about what should be done at home to survive 72 hours in the event of a crisis, not all, even a small proportion, have prepared everything. Even fewer know how to respond after this preparation or what other behavioural procedures should be followed in different crises. In most cases, the national administration is blamed for a lack of information and is expected to take active action during such a crisis.

National security strategic documents, on the other hand, focus on the crisis from the standpoint of military intervention or war, for which the 72-hour readiness is more suited. It does not work the same way in other contexts, such as the ecological security dimension or ecological cataclysms. Thus, while ecological disasters are mentioned as a source of insecurity, neither the National Security Concept (2019) nor the National Defence Concept (2019) includes a deeper analysis of potential ecological threats or the impact of hybrid threats on the environment (2020). One might conclude that this security sector is not a priority for Latvia's security agenda.

Conclusion

Over recent years, Latvia has permanently increased its efforts to build up resilience to hybrid threats. Despite significant progress, there are still many challenges and tasks ahead. Latvia must address issues associated with the mapping of hybrid threats in order to facilitate targeted and effective countermeasures. This means that to respond effectively to hybrid threats, it is necessary to collect as many pieces of the security environment puzzle as possible in order to be aware of the context and situational issues. Identification of changes in an environment that indicate an impending hybrid threat is critical for these processes. As a result, understanding the challenges that citizens face can be critical in developing such proactive and preventive security policies. Citizens' concerns can not only serve as an indicator of temperature and an early warning system, but they can also become active security system makers

if they recognise looming hybrid threats, keep their fingers on the pulse, and know how to act in cases of potential hybrid danger.

The analytical section of the article confirms that the population of Latvia can identify certain hybrid threats and sees them as challenges to their own and national security. The most widely recognised hybrid threats are related to informational space and cyber. At the same time, there are several other types of hybrid threats that Latvia faces or could potentially face, and they are not recognised or considered relevant among the population. However, anxiety about the challenges posed by hybrid threats has increased over the last two years. This can be explained by several circumstances — from the crisis caused by the COVID-19 pandemic to the worsening conditions of the geopolitical situation, in which Latvia is directly embedded due to the artificial migration crisis at its borders, together with other hybrid threats.

The Russian Federation was identified as the most important external source of hybrid threats by the population. The People's Republic of China is mentioned as well. Concerning Russia, the interviewed residents highlighted the immediate security challenges that they or, in their opinion, Latvian society faces in their daily lives or that they could potentially face, clearly defining potential scenarios. Respondents, on the other hand, described the potential threats posed by China as unclear and difficult to understand, as well as those that Latvia will face in the future.

Hybrid threats related to the information space are the most recognisable and urgent for the Latvian population. The most widely identified threats were propaganda and misinformation, especially fake news. In the self-assessment, respondents are generally optimistic about their ability to distinguish true information from false information or manipulation, while their peers — other generations, other regions, or other social groups — are considered to be weak in their own media literacy and critical thinking skills. Over the last two years, the spread of false news and misinformation has increased, as has the number of members of the public who have fallen victim to this manipulation of information. The situation is similar to cyber threats. It should be noted that the preventive measures described by the surveyed population to ensure data security reflect a rather light-hearted approach to cyber security issues. Citizens, despite being aware of the potential risks and dangers, choose not to pay enough attention to the use of safe internet strategies. This indicates a lack of public awareness of the dangers themselves rather than the consequences that may result.

Citizens and local decision-makers consider the potential for hybrid threats to create vulnerability in critical infrastructure objects as the least serious threat. This is not only due to the population's poor knowledge about the risks posed by critical infrastructure and their role in the event of a crisis but also

because of poorly developed planning documents and generalized regulations provided for public use. In this context, researchers have limited information and thus cannot evaluate it. The least recognised threats are hybrid threats that could have an impact on the environment. During the focus group interviews, respondents admitted that they had no idea what would happen or how to deal with such situations, nor did they know who to turn to for information or assistance. This means that the population is ill-prepared for emergencies. At the same time, they have an interest in what everyone should do in X hours (for example, in the event of a cyberattack, an electronic payment outage, a power outage, a natural disaster, including a chemical spill, or a covert or overt military invasion). Therefore, such comments from the population should not be used to satisfy the expressed interest but to improve the security system of Latvia.

The study leads to two major conclusions. First, the future of the security environment is rather challenging and unpredictable. The hybrid threats and hybrid wars pose dangers for Latvia and other European democracies in general. There are no easy, effective, or cheap methods to prevent or counter hybrid threats. Not only political decision-makers but other stakeholders, including wider society, should be involved in resilience-building measures against them. Although Latvian security decision-makers recognise the strategic value of resilience, its construction alongside the members of society and the level of the added value of these activities still have the potential to grow. Its precise relationship to national preparedness to counter hybrid threats, as well as the whole-of-society approach, necessitates more intensive strengthening. The balanced organisation of this mix of capacity, capability, and readiness provides total defence in a new and proactive manner. As a result, understanding residents' security perceptions is an important resource for developing better and more competitive security policies while also building resilience.

Second, Latvian society demonstrates an increasing commitment to democratic values, yet there are still several challenges that it faces for further democratisation and resilience building. Hybrid threats pose a significant challenge to the continued development of these processes. By hearing and feeling society and understanding their fears and security challenges, the government will be able to not only develop and promote a competitive and positive counter-narrative to hostile foreign narratives but also demonstrate how, by involving society in security decision-making, their policies are tailored to achieve concrete measures for resilience. The article shows that the key stakeholders — the government and society — do not share a common understanding of the security situation, and the threat assessment is not shared by both sides. The example of subjective perception of hybrid threats shows an active awareness of the number of hybrid threats and the

eventual consequences for the nation and individuals. Campaigns for better communication and training should be launched. Furthermore, hybrid defence and resilience are neither static nor traditional. Common, interactive learning of all the stakeholders is the future imperative of state security

References

Balcaen, P., Du Bois, C., & Buts, C. (2021). The Hybridisation of Conflict: A Prospect Theoretic Analysis. *Games,* 2021, 12, 81. https://doi.org/10.3390/g12040081.

Bērziņa, I. (Ed.). (2015). Sabiedrības destabilizācijas iespējamība Latvijā: potenciālie nacionālās drošības apdraudējumi. Rīga: Latvijas Aizsardzības akadēmijas Drošības un stratēģiskās pētniecības centrs.

Buffy, B. (2018). *The Perils of Perceptions. Why We're Wrong About Nearly Everything.* Atlantic Books.

Christine, D.I., & Thinyane, M. (2021, November 17). Opinion: Why Civil Society Remains So Vulnerable to Cyber-Attack. *Devex*. https://www.devex.com/news/opinion-why-civil-society-remains-so-vulnerable-to-cyber-attacks-102016.

Diamant, J. (2017, July 24). Ethnic Russians in Some Former Soviet Republics Feel a Close Connection to Russia. *Pew Research Center*. https://www.pewresearch.org/fact-tank/2017/07/24/ethnic-russians-in-some-former-soviet-republics-feel-a-close-connection-to-russia/.

Dunnay, P., & Roloff, R. (2017). Hybrid Threats and Strengthening Resilience on Europe's Eastern Flank. *Security Insights*, No 16.

Giannopoulos, G., Smith, H., & Theocharidou, M. (2020). The Landscape of Hybrid Threats: A conceptual model. *European Commission*, Ispra, PUBSY No. 123305.

Gullien-Lasierra, F. (2021). The Fallacy of Objective Security and its Consequences. *International E-Journal of Criminal Sciences, 1*(16). https://ojs.ehu.eus/index.php/inecs/article/view/22531.

Kalniete, S., & Pildegovičs, T. (2021). Strengthening the EU's Resilience to Hybrid Threats in European View. *Wilfried Martens Centre for European Studies*, *20*(1), 23 –33.

Keršanskas, V. (2021 April). Deterring Disinformation? Lessons from Lithuania's Countermeasures Since 2014. *Hybrid CoE*. https://www.hybridcoe.fi/publications/deterring-disinformation-lessons-from-lithuanias-countermeasures-since-2014/.

Krumm, R. et al. (2019). *Security Radar 2019. Wake-up Call for Europe.* FES

Regional Office for Cooperation and Peace in Europe.

Latvijas Fakti (2017). Latvijas Iedzīvotāju medijpratība. Latvijas Republikas Kultūras ministrijas mājaslapa. https://www.km.gov.lv/uploads/ckeditor/files/mediju_politika/petijumi/Medijpratiba_petijuma%20rezultati_Latvijas%20Fakti_18_07_2017.pdf.

McCulloh, T., & Johnson, R. (2013). Hybrid Warfare. *Joint Special Operations University Report*, No. 13-4, 14-17. https://www.hsdl.org/?view&did=744761.

Nyemann, D. (2021). Hybrid warfare in the Baltics. In M. Weissmann , N. Nilsson , B. Palmertz & P. Thunholm (Authors), Hybrid Warfare: Security and Asymmetric Conflict in International Relations (pp. 195–213). I.B. Tauris. http://dx.doi.org/10.5040/9781788317795.0020

Ozoliņa et. al. (2021). Latvijas iedzīvotāju subjektīvā drošības uztvere: ietekme uz drošības politikas veidošanu. Rīga: latvijas Universitātes Akadēmiskais apgāds.

Raugh, D. L. (2016). Is the Hybrid Threat a True Threat? *Journal of Strategic Security*, 9, No 2.,1-13. http://dx.doi.org/10.5038/1944-0472.9.2.1507.

Shea, J. (Ed.). (2018). Hybrid and Transnational Threats. Discussion Paper. Friends of Europe. https://www.friendsofeurope.org/wp/wp-content/uploads/2019/04/FoE_SEC_PUB_Hybrid_DP_WEB.pdf.

Siedschlag, A. (2021). Public Perception of Homeland Security and Societal Limits to the Whole-Community Approach: The Example of Pennsylvania, 2016-2020. https://www.linkedin.com/pulse/public-perception-homeland-security-societal-limits-siedschlag/.

Stifel, M. (2019, December 17). The Importance of Civil Society in the World of Cybersecurity. Global Cyber Alliance. https://www.globalcyberalliance.org/the-importance-of-civil-society-in-the-world-of-cybersecurity/.

U.S. Department of Defence (2015). The National Military Strategy of the United States of America 2015. https://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf.

Wolfers, A. (1962). National Security as an Ambiguous Symbol. In A. Wolfers, Discord and Collaboration. Essays on International Politics. John Hopkins University Press.

Zelče, V. (2018). Latvijas mediju patēriņa daudzveidība un ekspozīcija. *Latvijas mediju vides daudzveidība.* LU Akadēmiskais apgāds.

Notes

[1] The choice of focus group interviews was based on the considerations of validity. Focus groups tend to be strong on validity. It is believed that it is reasonably certain that people are talking about what they think. Furthermore, focus groups generate data at three units of analysis, namely: the individual, the group and their interaction. This means that the individual unit is appropriate for triangulation; the group unit is useful as a pre-test measurement of validity (in this case, results of each focus group were used to reflect on clarification and development of questions), and the interactive unit is a reasonable tool for exploration.

[2] The method used for selecting participants for focus groups was purposive sampling. This means that those members of the community who were in a position to provide the most relevant information for the research were selected. This time, this relevance was measured in the context of the diversity of society and, accordingly, diversity of opinions and perceptions. The focus groups were made up of 8 to 12 participants. The social, educational, gender, and age balance was taken into consideration to provide an insight into different perspectives of different societal groups. The locations of focus group interviews were chosen in order to cover the different regions in Latvia. The urban areas were chosen- starting from villages up to towns and cities. Therefore, different extant perceptions, needs, and contexts within society were accommodated.