DOI 10.18276/978-83-8419-028-9-30

28th European Conference on Artificial Intelligence (ECAI 2025)

CYBER SECURITY AWARENESS AMONG CITY COUNCILORS IN THE ERA OF HYBRID WARFARE

Hubert Pachciarek[a], Maciej Drzonek[b]

[a] *University of Szczecin, Institute of Management, Szczecin, Poland*
[b] *University of Szczecin, Institute of Political Science and Security Study, Szczecin, Poland*

ABSTRACT

Purpose: *The purpose of the article is to examine the awareness of cyber security threats in the era of hybrid warfare among councillors of selected 21 medium and large Polish cities from the West Pomeranian and Subcarpathia provinces.*

Need for the study: *In the era of hybrid warfare, cyberspace is becoming another theatre of warfare. Numerous threats to society flow from cyberspace. A key aspect of defence against threats is awareness, which most often comes from knowledge of the threats.*

Methodology: *The study used methodological triangulation to fully clarify the awareness of cyber threats among city councillors. To this end, anonymous questionnaire surveys were conducted, asking people to rate the likelihood of various threats, including cyber threats. The same group of councillors was then invited to participate in in-depth interviews, during which they were asked to identify three key contemporary threats to Poland and to identify the most important concerns of the residents of the cities they represent. The results for the two provinces were compared and showed statistically significant differences.*

Findings: *The councillors indicated the presence of cyber security threats in the surveys. These threats were the second most indicated and were the fewest of all 14 threats indicated as not present. However, in qualitative research, during in-depth interviews with councillors, these threats were sporadic. This indicates a relatively low awareness of cyber security threats.*

Practical Implications: *The research methodology can be used to conduct analogous research in other regions of the world or in organizations exposed to cybersecurity threats.*

Keywords: cybersecurity, awareness of cybersecurity threats, hybrid warfare, local government, cyberspace, information technologies

1. INTRODUCTION

The hybrid war in Ukraine has been ongoing since February 2014 and has taken on a particularly ruthless character through a full-scale military conflict on February 24, 2022. This means that due to the ongoing war directly across the Polish border, Poland has become a frontline country and, at the same time,

Peer-review under responsibility of the scientific committee of 28th European Conference on Artificial Intelligence (ECAI 2025) and Intelligent Management Workshop.

serves as a key logistical hub for military and humanitarian support for the fighting Ukraine. The Subcarpathia region, which borders Ukraine directly, is particularly important in this regard. Consequently, Poland has also become, to some extent, a theater of hybrid warfare waged by Russia. What is hybrid warfare? Hybrid warfare is a combination of conventional and unconventional warfare such as the use of the regular military, special forces, irregular armed groups, economic pressure, cyber-attacks, information warfare, diplomacy, and the stimulation of social conflict (Steingartner, Galinec, 2021). The dangers of stimulating internal conflicts in countries targeted by hybrid warfare by raising socioeconomic differences, including on ethnic grounds, spreading disinformation, attempting to quarrel with partner countries, and waging information warfare using mass media and electronic media require special attention (Krawczyk et al., 2024). Consequently, it is not necessary to wage war using conventional lethal weapons, a country can become a party to hybrid warfare in the information-social space, for which IT tools, the Internet and artificial intelligence will be used. Thus, information warfare is an important element of modern warfare, affecting the adversary, its information resources, information systems and computer networks (Kus, 2023). Consequently, the adversary in hybrid warfare is non-standard: a state, a state-supported organization, or a private actor, complex and fluid due to the volatile nature of the war coalitions formed, easily adapting to the situation, using advanced information technologies and spreading propaganda using the media and the Internet (Otaiku, 2018). Russia has developed a doctrine of hybrid warfare by moving away from the characteristics of traditional armed conflicts (Mumford, Carlucci, 2023), supplementing the spectrum of activities with the acquisition of direct influence, taking measures for the internal decomposition of the enemy, using irregular forces-"private armies", moving away from the traditional perception of the battlefield in physical dimensions to a multidimensional field, including cyberspace, using informational and psychological superiority, from symmetrical conflict to asymmetrical conflict using political, economic, informational, technological and ecological campaigns, and finally moving away from a limited time of conflict to a permanent state of war (Crowther, 2021).

The development of the doctrine of hybrid warfare became possible due to the emergence of cyberspace, understood as "an unlimited (in terms of reach and freedom of use) means of interpersonal communication" (Herominski, 2024, p. 187). The development of cyberspace was made possible in large part by the emergence of long-distance human communication tools. Today, cyberspace is primarily identified with the development of Internet.(Faruk et al., 2022) In fact, a distinction can be made between physical components (hardware, electronic devices), logical components (software, internet) and a network of interpersonal relations embedded in cyberspace as a non-physical element (Zdzikot, 2022; Jang-Jaccard, Nepal, 2014, Humayun et al., 2020). That is why the dangers of hybrid warfare are particularly associated with this area. This is because cyber warfare is much less visible than the use of regular military units or irregular militarized groups, and mankind has already become somewhat accustomed to the occurrence of armed conflict. In contrast, cyber threats are a new phenomenon. It should be added that engaging in traditional warfare requires entering into direct contact with the enemy; in cyberspace, the enemy can act from anywhere in the world. In traditional terms, the enemy is defined; in cyberspace, the category of the enemy is fluid and illusory, often impossible to identify. After all, we are aware of an enemy that poses a physical threat, an enemy in cyberspace we may not even notice or be aware of its existence. This is why awareness of cyber threats has become of such interest to the article's authors.

2. LITERATURE REVIEW

Hybrid warfare conditions aside, it is important to emphasize the growing risk of cyber threats. This is due to the dynamic development of the e-commerce market, the associated increase in the volume and value of electronic payments, the digitization of services and products, the widespread use of the Internet and mobile devices, and cloud solutions (Kuzior et al., 224; Ahsan et al., 2022). At every level of social life, we collide with digitization processes. Whether we are talking about public services, B2B and B2C relations, or at the individual level. In practice, most modern world citizens use mobile or online devices daily, store sensitive data in cyberspace or make electronic payments. Consequently, each such activity exposes cyber security to cyberattack or cybercrime. The development of information technology leads, on the one hand, to the simplification of everyday life for organizations and citizens. However, on the

other hand, it expands the spectrum of cybersecurity threats. Shestak and Tsyplakova attempted to create a unified classification of such threats, which are presented in Table 1.

Table 1. Classification of cybersecurity threats

Type	Characteristics
Botnet	Hackers operate some systems to coordinate attacks and dissimilate phishing, spam and malware
Organized Criminal Groups	Attacks often aim at monetary gain via spam, phishing, spying- or malware to steal personal data and e-fraud
Foreign Intelligence Service	One of the goals is information warfare and critical infrastructure decommission
Hackers (Including Hacktivists)	Applying malware or other instruments in order to cause failure and serious damage
Insiders	Disgruntled employees of an organization who do not have specific knowledge in IT, but have access to ESM. The motive is often revenge which harms not only the company's reputation, but also critical infrastructure facilities
Phishing	Persons or small groups that steal personal data or information in general in order to take advantage via spam and spy- and/or malware software
Spammers	Persons or organizations that send e-mails with hidden or false information in order to sell produce, activate phishing, spy- or malware software and attacks on the organization
The Authors of Spy- and/or Malware Software	Persons or organizations that create or dissimilate spy- or/and malware software, computer viruses and worms which damage files and hard drives
CyberTerrorism and CyberExtremism	Persons or organizations that seek to destroy, disable or use critical infrastructure to compromise national security, weaken a nation's economy and use phishing schemes or spy- and/or malware to obtain funds or gather sensitive information
Commercial Spies	More professional approach rather than insiders and the motivation is private gain

Source: Shestak, V. A., Tsyplakova, A. D. (2023). Criminological Features of the Cybersecurity Threats. The Law, State and Telecommunications Review, 15(2), 194-195.

In Poland, we can observe an increasing number of cybersecurity incidents yearly. While this is partly because citizens, institutions, and businesses are becoming more aware of this area and the introduction of simplified reporting procedures through automated reporting systems, it does not explain such a dynamic increase in identified incidents (Lisiak-Felicka, 223).In 2023, CERT Poland, a team within the national cyber-security system established to monitor cyber-security threats, handle incidents at the national level and build threat awareness, confirmed 80267 incidents. In 2020, it was still 10420 incidents (CERT, 2024). The jump in confirmed incidents shows the scale of threats to modern societies. The most important threats in the era of hybrid warfare and the growing arsenal of cyber criminals include (Wieczorek, Roszkowski, 2021):

- theft of sensitive data using information technology, not only personal data but also classified information, intellectual property, business secrets,
- cyber-terrorism- actions taken in the cyber world aimed at forcing concessions on the public or public authorities,
- cyber extortion- cyber-attacks on websites leading to their blocking in order to extort a ransom in exchange for restoring the state before the attack,
- economic espionage- the acquisition of confidential information for competitive advantage by private entities or government services. Such activities can range from stealing cutting-edge technology information about strategic decisions made to, for example, the financial health of a particular company,
- cyber warfare- attacks on enemy information systems by specialized services,

Information warfare is the use of manipulation to create social pressure, internal conflicts, and emotional reactions in response to false information or partially false information.

The spectrum of criminal activities undertaken in cyberspace is diverse, and there is still a lack of effective tools to counter cybersecurity threats. Today, we are witnessing a real cyber arms race. Therefore, awareness of cybersecurity threats and avoiding unsafe behaviour seems to play an important role in threat and incident crisis management situations (Franke, Brynielsson, 2014). To date, there have been numerous studies of cybersecurity threat awareness. Zwilling et al. conducted a comparative study of students from Turkey, Slovenia, Israel and Poland, exploring the relationship between IT knowledge, cybersecurity threats awareness and their impact on protective behaviours in cyberspace, postulating in their conclusions to conduct training programs to improve cybersecurity (Zwilling et al., 2020). Students were also studied by Muthisi and Mujinga using the SOTAM model (the student online threats awareness model), which analyzed the impact of foundational factors such as biographical data, institutional practices, and the presence of intervention programs in the form of training programs, for example, on cybersecurity threats awareness and activity in cyberspace (Mothisi, Mujinga, 2025). Research in this area, but among corporate employees, was conducted by Hadlington et al. looking for a relationship between ISA (information security awareness) and FoMO (Fear of Missing Out) (Hadlington, Binder, Stanulewicz, 2020). Their research found that measures aimed at reducing FoMO among employees can lead to more responsible behaviour in cyberspace. The human factor in dealing with cybersecurity threats was also highlighted by Georgiadou et al. by examining the relationship at two levels: individual and organizational (Georgaidou et al., 2020). At the individual level, attitudes, knowledge, awareness and competence were tested through surveys, tests, simulations and observations. In this way, it is possible to build a safety system and minimize the risks associated with risky human behaviour. In the studies analyzed by the Authors, it is clearly indicated that the key risk factor associated with cybersecurity threats is the human individual and his or her propensity for risky behaviour and vulnerability to threats emanating from cyberspace, whether they relate to exploitation of the Internet and establishment of virtual relationships, or electronic purchases and payments, use of risky network sources, or vulnerability to disinformation or even fraud created by cybercriminals. Considering the threats of hybrid warfare and specifically related cybersecurity threats, a threat awareness study was undertaken in two purposely selected regions of Poland.

3. METHODOLOGY. CHARACTERISTICS OF THE SURVEY OF LOCAL AUTHORITIES OF SUBCARPATHIA AND WESTERN POMERANIA.

The surveys described below were conducted in 2024 by the Res Publica Research Team at the University of Szczecin (res.usz.edu.pl). They are one of the elements of research conducted as part of a broader research project in 2023-2026 entitled Local Politicians vs. Patriotism and Threat Perception. A comparison of the cities of Subcarpathia and Western Pomerania.

3.1. Rationale for security and threat surveys among local government officials

In 2014. Russian Federation seized Crimea, and in 2022, the Polish public's views on its sense of security and threats may have changed as a result of the intensification of Russian aggression against Ukraine. In addition, before the full-scale kinetic war between Russia and Ukraine took place, the Russian state, with the cooperation of Belarus, implemented other hostile actions on NATO's eastern flank. These included various hybrid actions, both cyber in nature and in the form of attacks on the borders of Poland and Lithuania. In 2021, the Belarusian (and Russian) authorities from their territory massively enabled the illegal migration to Poland, Lithuania and Latvia of people coming from various African and Asian countries. Illegal transit of illegal migrants via Belarusian territory led to the need to erect barriers on the border with Belarus to impede illegal border crossings.

The 2022 Russian aggression unleashed Poland's multifaceted involvement in aid to Ukraine. The most important elements of this assistance include: political support in the international arena, military support through the provision of military equipment, as well as logistical support by making its territory available for the transit of aid to the fighting Ukraine (Rzeszow-Jasionka airport is of particular importance), and finally, providing shelter to the multi-million refugees, especially in the first months of the kinetic war. A great responsibility in both fostering patriotic attitudes and prudent perception of potential threats lies with local political elites. It is the maturity and awareness of local politicians and their willingness to engage with their local communities that determine what those local communities will be.

It is the maturity and awareness of local politicians and their willingness to engage with local communities that determine what these local communities will be. Thus, on the one hand, Russia and Belarus attempt to create an artificial migration crisis and, on the other hand, the war in the immediate vicinity of the Republic may have transformed Poles' social attitudes regarding their perception of security and threats.

It can be assumed that people holding elected positions in local government (especially councillors) have natural contact with the local communities in which they live on a daily basis and which they represent in the local government structures. It was therefore decided to check the perception of threats and security among local politicians of medium-sized cities (from 20,000 to 100,000 residents) and large cities (over 100,000 residents) in two distant provinces – Subcarpathia and Westpomeranian. The former, which is located in the Subcarpathia region, directly borders the territory of Ukraine, so it can be assumed that the threats, due to the kinetic war going on just across the border, are perceived quite clearly there. The second province, located in Western Pomerania, covers the geographically opposite area of Poland - the northwestern areas bordering Germany, at the same time, the furthest from the border with Belarus and Ukraine.

Therefore, it can be assumed that local government officials of cities in the Subcarpathia region may exhibit specific attitudes regarding various categories of threats already due to the proximity of the border with Ukraine and Subcarpathia's role as a transit corridor for multidimensional aid channelled from various parts of the world. This peculiarity is also compounded by other factors, such as political preferences with a predominance of support for political groups promoting conservative perceptions of reality, and an accompanying higher level of religiosity. On the other hand, in the cities of Western Pomerania to which many refugees were admitted after 24 II 2022, due to the distance from the military action in Ukraine, the perception of security and threats to state security may be somewhat different (although - it is worth noting at the same time that in Western Pomerania the Ukrainian diaspora already resided before 2022).

The perception of threats to state security based on a survey of respondents living and working in the local government of cities in two opposite regions of Poland is justified. This is because the attitudes of local politicians of cities from two different regions were taken for comparison: the conservative, religious Subcarpathia, which, in addition, directly borders the war zone, and the liberal, low-religious West Pomerania, distant from the immediate war threat.

3.2. Characteristics of the surveyed cities

Two categories of cities were taken for the survey: according to the methodology used by the Central Statistical Office, these are medium-sized cities, i.e. with residents between 20,000 and 100,000, and large cities, i.e. with more than 100,000 residents. This selection of cities and local government officials operating in them seems justified. Firstly, units with similar demographic structures are compared; secondly, such categories of cities are subject to systematic, periodic surveys by institutions conducting statistical research; and thirdly, in both regions studied, the number of cities in the identified categories is similar: ten in the Subcarpathian region and eleven in the West Pomeranian region.

In West Pomerania, the following medium-sized cities were singled out: Białogard, Goleniow, Gryfino, Kolobrzeg, Police, Stargard, Szczecinek, Swinoujscie and Walcz. Zachodniopomorskie has two cities in the large city category: the capital of Zachodniopomorskie, Szczecin, and Koszalin. Table 2 presents the surveyed cities with their population in 2021 and 2024.

In Subcarpathia, on the other hand, the following cities were classified as medium-sized cities, according to the criterion adopted after the Central Statistical Office (20-100 thousand inhabitants): Debica, Jaroslaw, Jaslo, Krosno, Mielec, Przemyśl, Sanok, Stalowa Wola and Tarnobrzeg. According to the accepted nomenclature in Subcarpathia, the only large city is its capital, Rzeszów. Table 3 presents the surveyed cities and their populations in 2021 and 2024.

Table 2. Studied cities of West Pomeranian and Subcarpathian province and their demographic size 2021-2024

City	Surface		Population		City	Surface		Population	
	in ha	in km²	2021	2024		in ha	in km²	2021	2024
Białogard	2573	26	23950	22418	Dębica	3383	34	45189	42986
Goleniów	1178	12	21979	21462	Jarosław	3461	35	37073	35298
Gryfino	1181	12	20923	19691	Jasło	3652	37	34542	32727
Kołobrzeg	2567	26	46198	43426	Krosno	4472	45	45948	44060
Koszalin	9834	98	106235	105540	Mielec	4689	47	60075	56972
Police	3731	37	32243	29627	Przemyśl	4617	46	59779	56050
Stargard	4808	48	67579	66604	Rzeszów	12901	129	197863	197268
Szczecin	30060	301	398255	389066	Sanok	3808	38	36999	34345
Szczecinek	4848	48	39827	37557	Stalowa Wola	8252	83	59623	55127
Świnoujście	20207	202	40948	38904	Tarnobrzeg	8540	85	46360	43712
Wałcz	3817	38	24949	23578					

Source: own compilation based on: CSO, Area and population in territorial section in 2021, Warsaw 2021, https://stat.gov.pl/obszary-tematyczne/ludnosc/ludnosc/powierzchnia-i-ludnosc-w-przekroju-terytorialnym-w-2021-roku,7,18.html; CSO, Area and population in territorial section in 2024, Warsaw 2024, https://stat.gov.pl/obszary-tematyczne/ludnosc/ludnosc/powierzchnia-i-ludnosc-w-przekroju-terytorialnym-w-2024-roku,7,21.html.

The research project "Local politicians vs. patriotism and threat perception. Comparison of the cities of Subcarpathia and Western Pomerania" in 2024 used methodological triangulation, in order to increase the ability to explain the phenomena under study. Therefore, the research was carried out in two forms. First, quantitative research was conducted in the form of an electronic survey questionnaire (CAWI) distributed to local government officials of the 21 cities under study. The second form was qualitative research implemented by conducting anonymous in-depth interviews with selected local government officials of the surveyed cities.

3.3. Characteristics of quantitative studies

The quantitative survey was a closed-ended questionnaire. It consisted of several questions, each containing a dozen statements (response options). Respondents' answers were collected on a 5-point Likert scale, with the answer "definitely no" having a value of "1" and "definitely yes" having a value of "5."

The first question was: What do you think could threaten Poland's security shortly, and to what extent? Fourteen response options were formulated for it. The remaining questions were related to separate objectives of the research project.

What do you think could threaten Poland's security shortly, and to what extent? A cafeteria of the following fourteen options was used:

1. Demographic collapse, ageing of the population.
2. Reduced standard of living, need to forgo some expenses.
3. Cyber-attack disrupting state operations, theft, cyber-security threats.
4. Social unrest and protests.
5. Increase in crime, including organized crime.
6. Threats to energy security - shortages in energy, gas supply.
7. Fear of losing jobs.
8. Increased risk of not finding a job.
9. Loss of a sense of economic security for families due to an increase in loan instalments.
10. Migration of refugees to Poland from conflict areas.

11. Spread of some infectious disease, epidemic.
12. Terrorist attack in Poland.
13. Political chaos in Poland.
14. Conflicts between ethnic and Religious groups in Poland

It is worth mentioning that the above question and the options to choose from were prepared based on nationwide surveys conducted by the Center for Public Opinion Research (CBOS). The first time CBOS conducted them was in 2014, when the National Security Office commissioned them to the President of the Republic. It was published in November 2014. In addition, the Res Publica Research Team has conducted similar surveys twice. In 2016, among councillors of ten municipalities and cities in the Lubuskie and West Pomeranian Voivodeships. These were Drawsko Pomorskie, Goleniow, Kamień Pomorski, Kobylanka, Nowogard, Stara Dąbrowa, Stargard, Strzelce Krajeńskie and Świnoujście . The 2022 survey, on the other hand, was conducted among councillors of three West Pomeranian cities with county rights (Koszalin, Szczecin, Swinoujscie).In the 2024 survey discussed here, the virtual survey questionnaire was sent to the 21 surveyed cities multiple times: more than thirty times to individuals from city council offices or city council presidents with requests to distribute to individual city councillors, plus dozens of times to individual local government officials. In the eleven surveyed cities of the West Pomeranian Voivodeship, there are 245 city councillors (see Table 3). In the Subcarpathia Voivodeship, are 220 in the ten surveyed cities (see Table 5). Despite repeatedly expressed encouragement and reminders, the return rate of survey questionnaires averaged 34.69% for eleven cities in West Pomerania and 26.36% for ten cities in Subcarpathia. The average return of questionnaires for the 21-city survey was thus 30.75%.

Table 3. Surveyed cities in the West Pomeranian and Subcarpathian region: number of councillors and percentage of survey returns

City	% return of surveys	No of councilors	City	% return of surveys	No of councilors
Szczecinek	47,62	21	Dębica	90,48	21
Stargard	39,13	23	Krosno	38,10	21
Świnoujście	42,86	21	Jasło	28,57	21
Szczecin	38,71	31	Sanok	23,81	21
Koszalin	43,48	23	Mielec	21,74	23
Gryfino	33,33	21	Stalowa W.	21,74	23
Kołobrzeg	33,33	21	Rzeszów	20,00	25
Wałcz	33,33	21	Jarosław	14,29	21
Białogard	23,81	21	Przemyśl	8,70	23
Police	23,81	21	Tarnobrzeg	0,00	21
Goleniów	19,05	21			
mean	**34,69**	**245**	**mean**	**26,36**	**220**

Source: own compilation based on quantitative research in 2024 within the framework of the project entitled Local politicians vs. patriotism and threat perception. A comparison of the cities of Subcarpathia and Western Pomerania, Project No. NdS-II/SP/0355/2023/01.

3.4. Characteristics of qualitative studies

In addition to conducting a survey questionnaire, qualitative research was conducted in anonymous in-depth interviews. They had the character of semi-structured interviews, although the people conducting them (from the Res Publica Research Team operating at the University of Szczecin) could, if necessary, change the order of the questions asked or formulate additional questions to obtain the maximum in-depth response from respondents. The questions included the perception of the most important threats

to Poland in the coming years and the concerns of the residents of their cities, i.e. their electorate, related to the future of Poland, the region, the city and themselves. These topics were addressed because councillors are directly elected and, as such, are representatives of the residents. Therefore, they should have a direct relationship with their constituents and understand their problems and concerns.

Local government officials from the surveyed cities were generally selected for interviews on a random basis. In most cases, they were local government officials serving as councillors during the interview. Often, they were current or former chairmen or vice-chairmen of city councils. In a few cases, they were individuals who had held council seats in earlier terms. Several respondents in the current term (2024-29) relinquished their councillor seats since they were simultaneously elected mayor/mayor of the city or deputies. In a few cases, local government officials sitting on the councils of the county whose seat was the surveyed city were also invited for interviews. A total of 126 interviews were held in twenty-one cities, of which 67 were held in 11 cities in the West Pomeranian Voivodeship (see Table 4), and 59 were held in 10 cities in the Subcarpathia Voivodeship (see Table 7). Counting the ratio of interviews held to the number of councillors in the surveyed cities yielded an average of 27.35% of interviews in West Pomerania and 26.82% in Subcarpathia.

Table 4. Surveyed cities in the West Pomeranian and Subcarpathia region: number of councillors and percentage of anonymous in-depth interviews conducted.

City	% of interviews	Number of councillors	City	% of interviews	Number of councillors
Białogard	23,81	21	Dębica	52,38	21
Goleniów	9,52	21	Jarosław	19,05	21
Gryfino	23,81	21	Jasło	23,81	21
Kołobrzeg	33,33	21	Krosno	38,10	21
Koszalin	30,43	23	Mielec	17,39	23
Police	23,81	21	Przemyśl	17,39	23
Stargard	21,74	23	Rzeszów	28,00	25
Szczecin	25,81	31	Sanok	33,33	21
Szczecinek	33,33	21	Stalowa Wola	17,39	23
Świnoujście	52,38	21	Tarnobrzeg	23,81	21
Wałcz	23,81	21			
mean	**27,35**	**245**	**mean**	**26,82**	**220**

Source: own compilation based on qualitative research in 2024 within the framework of the project entitled Local politicians vs. patriotism and threat perception. A comparison of the cities of Subcarpathia and Western Pomerania, Project No. NdS-II/SP/0355/2023/01.

It should be emphasized that the researchers did not suggest any choice options during the interviews with councillors regarding real threats to Poland or concerns of residents and their direct constituents. Therefore, the information obtained results from the respondents' free speech. Also, when asking these questions, respondents were asked to assess for themselves the importance and order of priority of the threats they believe exist in Poland and thus to present their reflections on their own perception of potential factors interfering with the security of the Polish state. At the same time, it was made clear to the respondents that the essence of the question about concerns occurring in the city where they held local government positions was to present what the city's residents thought about the issue, not the respondent himself. In other words, the respondent was supposed to recount, as it were, the concerns occurring among the city's residents, that is, to talk about the opinions heard about the sources underlying the concerns of the residents of the city in which the respondent served as a local government official.

A matrix was prepared to analyze respondents' answers given in the qualitative research - both for the question on the three main threats to the Polish state and what the residents of your city are concerned about. The matrix contains fifteen categories of possible responses reflecting the threats and concerns. In other words, the statements made by councillors regarding their perceived significant threats to the Polish state were classified into one of the 15 categories. The concerns respondents mentioned in the

city - that is, the perceived and heard concerns expressed by residents - were also categorized into 15 categories. This is a deliberate effort to compare within the same categories, on the one hand, the threats mentioned by local government officials and, on the other hand, the perceived concerns of residents. It should also be noted that these categories mirrored the threats assessed in the quantitative survey, with the difference that an additional category, "other", was introduced for threats not included in the quantitative survey.

Presented below is a list of categories into which city residents raised the threats identified by respondents and the concerns they believe were classified:

1. Demographic collapse.
2. Economic threats.
3. Cyber threats.
4. Threats of a social nature.
5. Conflicts of an ethnic nature.
6. Crime.
7. Energy security threats.
8. Unemployment.
9. Influx of refugees.
10. Health threats.
11. Terrorist threats.
12. Political divisions.
13. Environmental threats.
14. The threat of war, Russian aggression.
15. Other.

The quantitative and qualitative data obtained in the study were subjected to statistical analysis to determine the awareness of cyber threats among the surveyed city councillors. In addition, a comparison of awareness was made between councillors from the West Pomeranian Voivodeship (northwestern Poland) and those from the Subcarpathia Voivodeship (southeastern Poland - a region bordering Ukraine, an important logistical hub for aid to embattled Ukraine). The results obtained in the surveys and interviews were then compared. It should be noted that in the survey research, the selection of threats was supported by identifying 14 potential threats. At the same time, in the interviews, the researchers relied on the free speech of the respondents.

4. RESULTS & DISCUSSION

The reliability of the surveys was verified by measuring the reliability of the questionnaire. Table 5 presents the measurements of the Cronbach's Alpha index. The obtained value of 0.85 indicates a very high reliability of the measurement and a correct selection of variables; based on the analysis of Cronbach's Alpha index, removing any of the variables is not advisable. Thus, the list of risks was prepared correctly, and the obtained data are reliable and can be the basis for statistical analysis of the results and inference based on them.

143 responses were obtained from respondents, as summarized above. Table 6 presents the results obtained. The number of indications of cybersecurity threats is noteworthy. From the point of view of all the threats analyzed, only "demographic collapse, population ageing" (66 indications) and "migration of refugees to Poland from conflict areas" (61 indications) received more indications of YES. However, if we consider the sum of positive indications (YES +preferably yes), cyber threats are already in second place regarding the number of indications by councillors. It is noteworthy that cyber threats also received the least number of negative indications - the least number of surveyed councillors said there were no such threats. On the other hand, the mean of indications (answers were given values according to the Likert scale from NO = 1 to YES = 5) indicates a high level of awareness of cybersecurity threats among respondents. Given that these are representatives of local communities, the Polish public should be congratulated for their high level of awareness, higher than in other surveys cited in the article.

Table 5. The reliability of the questionnaire

variable	Summary.Scale: Mean=48.4196 standard deviation=9.33222 N weighted:143 (calculation_questionnaire (version 1))Cronbach's alpha: ,851488 Standardized alpha:,848912 Mean cor. between pos: ,296176				
	Mean when excluded	Value when excluded	St. dev. when excluded	Mean cor. between pos	Alfa when excluded
demographic collapse, ageing of the population	44,27273	82,28226	9,070957	0,167747	0,858970
reduced standard of living, need to forgo some expenses	45,03497	75,32046	8,678736	0,466807	0,843657
cyber-attack disrupting state operations, theft, cyber-security threats	44,41259	78,82978	8,878613	0,392505	0,847325
social unrest and protests	44,97902	76,32823	8,736603	0,494108	0,841997
increase in crime, including organized crime	45,17482	71,80859	8,473995	0,673660	0,830731
threats to energy security - shortages in energy, gas supply	44,67133	77,26960	8,790313	0,463191	0,843731
fear of losing jobs	45,36364	71,78385	8,472535	0,637647	0,832662
increased risk of not finding a job	45,50350	71,20103	8,438070	0,701889	0,828848
loss of a sense of economic security for families due to an increase in loan installments	44,93007	75,11399	8,666833	0,516687	0,840566
migration of refugees to Poland from conflict areas	44,51049	75,00513	8,660550	0,489125	0,842242
spread of some infectious disease, epidemic	45,23077	78,26143	8,846549	0,350807	0,850152
terrorist attack in Poland	45,09790	75,48692	8,688321	0,462171	0,843920
political chaos in Poland	44,67133	74,41646	8,626497	0,552708	0,838413
conflicts between ethnic and Religious groups in Poland	45,60140	72,77119	8,530603	0,542516	0,838949

Source: own study.

Table 6. The quantitative survey results

variable	yes	likely yes	neither yes nor no	likely no	no	Total yes	Total no	mean
demographic collapse, aging of the population	66	51	10	13	3	117	16	4,15
reduced standard of living, need to forgo some expenses	30	43	30	32	8	73	40	3,38
cyber-attack disrupting state operations, theft,	48	65	15	13	2	113	15	4,01

cyber-security threats								
social unrest and protests	22	55	33	30	3	77	33	3,44
increase in crime, including organized crime	23	43	30	40	7	66	47	3,24
threats to energy security - shortages in energy, gas supply	36	57	29	20	1	93	21	3,75
fear of losing jobs	19	37	37	33	17	56	50	3,06
increased risk of not finding a job	14	33	41	37	18	47	55	2,92
loss of a sense of economic security for families due to an increase in loan installments	30	47	35	25	6	77	31	3,49
migration of refugees to Poland from conflict areas	61	37	21	19	5	98	24	3,91
spread of some infectious disease, epidemic	21	35	45	34	8	56	42	3,19
terrorist attack in Poland	27	42	33	32	9	69	41	3,32
political chaos in Poland	43	51	24	20	5	94	25	3,75
conflicts between ethnic, religious groups in Poland	20	23	38	35	27	43	62	2,82

Source: own study.

A comparative analysis of the councillors' responses was also undertaken by Western Pomeranian and Subcarpathian provinces. The research assumption was that the residents of Subcarpathia, a region bordering the warfare arena, should be more concerned about the threats of hybrid warfare, including primarily cyber threats. Statistical analysis showed a statistically significant difference between the number of indications of cyber threats by councillors from both regions, with residents of West Pomerania indicating more significant concern in this regard, as shown in Table 7 and Figure 1.

Table 7. Comparison of cyber security threat assessments by councillors from the West Pomeranian and Subcarpathian provinces

Variable	Test U Manna-Whitneya									
	Rank sum SC	Rank sum WP	U	Z	p	Z corr.	p	Sample size SC	Sample size WP	p
cyber-attack disrupting state operations, theft, cyber-security threats	3560,500	6735,500	1849,500	-2,52849	0,011456	-2,71645	0,006599	58	85	0,011075

Source: own study.

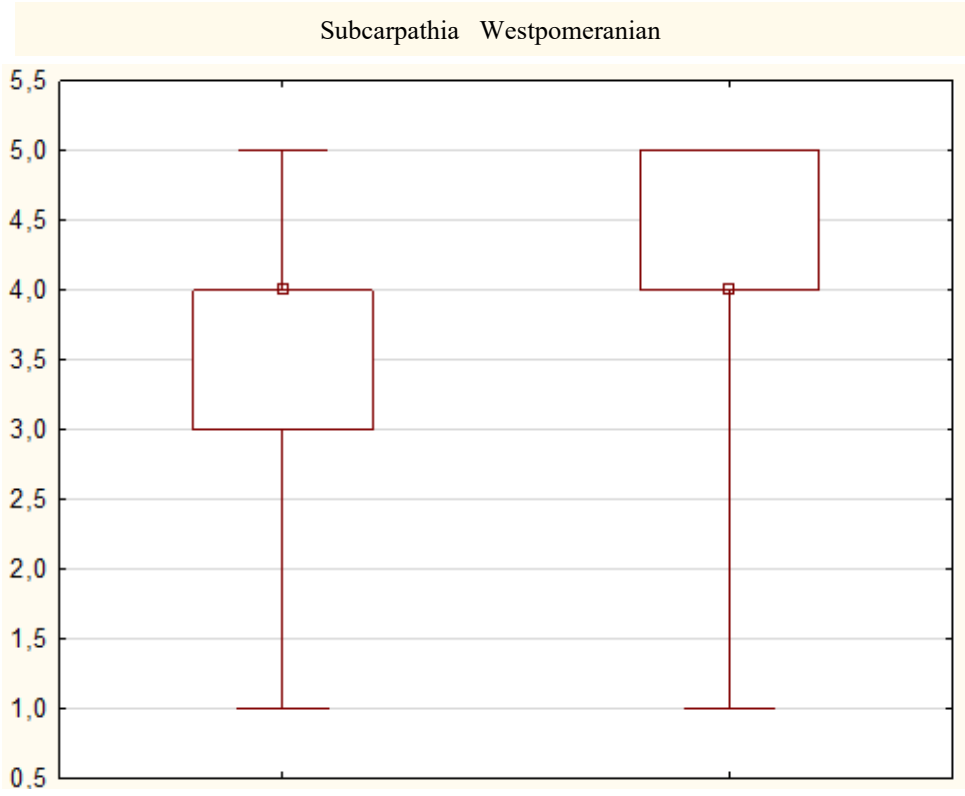

Figure 1. Comparison of cyber security threat assessments by councilors from the West Pomeranian and Subcarpathian provinces
Source: own study.

Consequently, after analyzing the data from the quantitative survey, it would be appropriate to indicate a high level of awareness of cyber threats among councillors, with a preponderance of indications on the side of West Pomeranian councillors more distant from the theatre of war. However, as noted in the research methodology, the researchers' assumption was to carry out methodological triangulation in order to obtain a complete description of the threats indicated by councillors of 21 medium-sized and large cities from two regions located at the two ends of Poland. During the interviews conducted, respondents were allowed to speak freely, so unlike in surveys, no categories of threats were

presented, but only asked to indicate the three most important ones. It would seem obvious to overlap the results of quantitative and qualitative research in the context of the perception of the most important threats and, consequently, to reflect the results of quantitative research in the results obtained during the in-depth interviews, in the free speech of respondents. It should be noted that the research group overlaps in its scope in both surveys, while very often, interview respondents also filled out questionnaires, but they did not fill out a new framework during the interview. Due to the different number of survey feedback received and interviews conducted, we expect there to be three different groups of respondents: councillors who completed the survey and participated in the interview, councillors who only completed the survey, and councillors who only participated in the interview. Based on the free declarations of the councillors who participated in the interviews, it can be expected that the first group is the most numerous, but due to the anonymity of the surveys, it is not possible to provide a detailed calculation. The results of the analysis of the interviews are presented in Table 8.

Table 8. Categories of threats identified by interview respondents

Category	Indication 1	Indication 2	Indication 3	Total no of indications
demographic collapse	5	2	3	10
economic threats	9	14	11	34
cyber threats	1	3	2	6
threats of a social nature	1	12	4	17
conflicts of an ethnic nature	1	1	0	2
crime	0	1	0	1
energy security threats	2	3	6	11
unemployment	0	0	0	0
influx of refugees	5	13	9	27
health threats	0	4	3	7
terrorist threats	0	0	1	1
political divisions	10	9	9	28
environmental threats	1	3	3	7
the threat of war, Russian aggression	64	12	5	81
other	5	17	6	28

Source: own study.

In casual statements, councillors indicated cyber security threats far less frequently than in survey statements suggesting potential threats. Only six respondents identified the area as one of the three most important to Poland, including only one who identified cyber security threats as the most important. By contrast, in terms of the number of indications, cyber-security threats ranked only 11th, a radical disparity from the survey results.

An analysis of responses to the question "What are your city's residents worried about?" yields even more serious results. None of the respondents chose to identify cyber threats as important to city residents, including those who identified cyber security as one of the most serious threats to Poland. They explained such a decision by the fact that residents do not pay enough attention to this area of security. Juxtaposing the real threat posed by hybrid warfare and the high level of indications of cybersecurity threats in the surveys with the results of the in-depth interviews, both in the area of the most important threats to Poland and the concerns of residents, it appears that cybersecurity threats awareness is more declarative than real. Given a choice between a spectrum of different threats, councillors accurately indicated the most important threats, including those related to cybersecurity. Still, the lack of indication of these threats in the free statements may indicate that this awareness is relatively low and is not a daily concern. As a result, it may lead to risky and irresponsible behaviour online by those who should serve as local leaders.

Alongside statements indifferent to the area of cybersecurity, however, there was one: x099 "I think such a big threat is the Internet and everything related to the media..., cybercrime is what is worth being afraid of today." Other councillors who identified cybersecurity threats as one of the three most important for Poland pointed primarily to disinformation and the use of fake news to cause social unrest, cyberattacks on state institutions and the media, the theft of sensitive data by cyber criminals, and risks arising from the development of artificial intelligence. The range of risks identified by the councillors is consistent with the list of the most serious cyber risks discussed in the article. So, awareness of the risks is linked to knowledge of the risks, which poses a challenge to contemporary people in raising awareness and knowledge of cyber security in society.

5. CONCLUSION

Modern times have brought the dynamic development of the virtual world, through which cyberspace has significantly expanded its scope of influence. In the era of hybrid warfare, for which the natural theatre of operations is precisely cyberspace, it is necessary to constantly improve the knowledge and awareness of societies in the field of cybersecurity threats. The research undertaken by the authors clearly indicated a very high level of declarative awareness of these threats. Surveys indicated a high frequency of indications of cyber security as a source of the most important threats. However, the results of the survey research were not confirmed in the qualitative research when the same group of councillors was asked in in-depth interviews to indicate the most important contemporary threats to Poland. The discrepancy between the second most frequently cited threat in the surveys and the 11th most frequently cited threat in the interviews leads to the conclusion that while declaratively, we do indeed understand cyber threats, they are not a daily concern and, as a result, real awareness of cyber threats is very limited. In addition, it can be assumed that a lack of awareness leads to a lack of self-restraint in online risky actions. At the same time, it should be emphasized that the councillors who pointed out cyber security risks in the interviews were very apt to give specific examples of such risks. This means that the primary path to raising awareness is to educate and promote knowledge on the subject. These words are written in a month when in Szczecin-Western Pomerania Province, at the request of the police, messages warning of the dangers of cybercrime are read in all churches during masses. It seems that any form of outreach with knowledge is important in avoiding threats.

The conducted research faces limitations due to the incomplete research sample of councillors of 21 cities in the West Pomeranian and Subcarpathian provinces. However, it should be emphasized that the analysis of the transcriptions of the conducted interviews leads to the conclusion of saturation of content and obtaining a complete description, which clearly indicates the representativeness of the research sample. In addition, the research was conducted in two marginal provinces of Poland, so extrapolating the results to the whole of Poland involves the risk of lack of representativeness.

Further research directions should extend the research to other regions in Poland and conduct a comparative analysis with other countries, both on the frontline and away from the war. In addition, an in-depth study of the attitudes and online behaviour of the surveyed councillors would be appropriate.

Funding: Co-financed by The Ministry of Science and Higher Education. Project entitled Local Politicians vs. Patriotism and Threat Perception. A comparison of the cities of Subcarpathia and Western Pomerania. (Politycy lokalni a patriotyzm i percepcja zagrożeń. Porównanie miast Podkarpacia oraz Pomorza Zachodniego), no NdS-II/SP/0355/2023/01, Program "Nauka dla Społeczeństwa II".

Funding: Co-financed by the Minister of Science under the "Regional Excellence Initiative".

REFERENCES

Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., Connolly, J.F. (2022). Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning – A Review. *Journal of Cybersecurity and Privacy, 2,* 527–555.

CERT.pl (2024). Raport roczny z działalności CERT Polska 2023. Retrieved from: https://cert.pl/publikacje/#raport (15.03.2025).

Crowther, G. A. (2021). NATO and hybrid warfare: seeking a concept to describe the challenge from Russia. In: M. Weissmann, N. Nilsson, P. Thunholm, B. Palmertz. Hybrid Warfare. Security and Asymmetric Conflict in International Relations, I.B. Tauris, 21-35.

Faruk, M. J. H., Tahora, S., Tasnim, M., Shahriar, H., & Sakib, N. (2022, May). A review of quantum cybersecurity: threats, risks and opportunities. In: *2022 1st International Conference on AI in Cybersecurity* (ICAIC). 1-8. IEEE.

Franke, U., Brynielsson, J. (2014). Cyber situational awareness – A systematic review of literature. *COMPUTERS&SECURITY, 46*, 18-31.

Georgiadou, A., Mouzakitis, S., Bounas, K., Askounis, D. (2020). A Cyber-Security Culture Framework fo Assessing Organization Readiness. *Journal of Computer Infomration Systems*, https://doi.org/10.1080/08874417.2020.1845583.

Hadlington, L., Binder, J., Stanulewicz, N. (2020). Fear of Missing Out Predicts Emplyee Information Security Awareness Above Personality Traits, Age and Gender. Cyberpsychology, *Behavior and Social Networking, 23(7)*, 459- 464.

Heromiński, M. (2024). Wojna I konflikt w cyberprzestrzeni. Piąty teatr wojny. *Przegląd bezpieczeństwa wewnętrznego, 30*. 185-211.

Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. *Arabian Journal for Science and Engineering, 45*, 3171-3189.

Ignasiak, A., Drzonek, M. (2016). Postrzeganie bezpieczeństwa przez samorządowców – wnioski z badań. *Środkowoeuropejskie Studia Polityczne, 3*, 85-119.

Jang-Jaccard, J., Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*, 973-993.

Krawczyk, D., Babenko, V., Yemchuk, L., Lienkov, S., Dzhulii, V., Dzhulii, L., Muliar, I. (2024). Analysis of information security under conditions of hybrid war in Ukraine: social aspects. *Management systems in Production Engineering, 32(2)*, 235-243.

Kuś, B. (2023). Siły Zbrojne Rzeczpospolitej Polskiej a cyberbezpieczeństwo. Zagadnienia organizacyjno-prawne. *Cybersecurity and Law, 2(10),* 32-50.

Kuzior, A., Tiutiunyk, I., Zielińska, A., Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. *Journal of International Studies, 17 (2),* 220-239.

Lisiak-Felicka, D. (2023). A comparative analysis of information security incidents in public administration in selected European union countries. *Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach,134*, 25-34.

Mothisi, D., Mujinga, M. (2025). An Exploration of Students' Cyber Threats Perception in the Digital Age. *Indonesian Journal of Information Systems, 7(2)*, 123-135.

Mumford, A., Carlucci, P. (2023). Hybrid warfare: The continuation of ambiguity by other means. European *Journal of International Security, 8*, 192-206.

Ocena stanu bezpieczeństwa państwa. Raport z badania sondażowego przeprowadzonego przez CBOS w 2014 roku na zlecenie Biura Bezpieczeństwa Narodowego, (2014), Retrieved from: https://www.bbn.gov.pl/ftp/dok/05/ocena_stanu_bezpieczenstwa_panstwa.pdf, (3.03.2016).

Otaiku, A.A. (2018). A Framework for Hybrid Threats, Challenges and Solutions. *Journal of Defense Management, 8(3)*.

Shestak, V. A., Tsyplakova, A. D. (2023). Criminological Features of the Cybersecurity Threats. *The Law, State and Telecommunications Review, 15(2)*, 187-203.

Steingartner, W., Galinec, D. (2021). Cyber Threats and Cyber Deception in Hybrid Warfare. *Acta Polytechnica Hungarica, 18(3),* 25-45.

Wieczorek, S., Roszkowski, M. (2021). *Zagrożenia wynikające z cyberprzestępczości i wojny hybrydowej*. Instytut Jagielloński.

Zdzikot, T. (2022). Cyberspace and Cybersecurity. In: K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński: *Cybersecurity in Poland. Legal Aspects*. Springer.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., Basim, H.N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, https://doi.org/10.1080/08874417.2020.1712269.