วารสารวิชาการผลประโยชน์แห่งชาติ
National Interest
ISSN (Online): 2730-2393

DOI: https://doi.org/10.14456/ni.2025.14

Digital tools in security governance: enhancing public participation and deliberative democracy - the case of Poland

Katerina Veljanovska Blazhevska
E-mail:veljanovska_katerina@yahoo.com
Professor at Faculty of Security Science, MIT University – Skopje (North Macedonia)
Ryszard Szpyra
E-mail:r.szpyra@gmail.com
Professor in the Department of Information Security
Faculty of National Security, War Studies University of Warsaw (Poland)

ABSTRACT

Poland's rapid digital transformation reshapes democratic engagement in national security governance, offering opportunities and challenges. Despite expanding e-governance, digital identification, and consultation tools, barriers like unequal digital literacy and limited transparency hinder inclusive participation. This study, grounded in Habermas' deliberative democracy theory, explores how digital tools can enhance accountability and public involvement in security decision-making. Using a mixed-method approach—expert interviews, student surveys at War Studies University in Warsaw, and analysis of policy documents and media—it reveals limited civic engagement despite widespread use of digital platforms for information access. Institutional trust, influenced by transparency, leadership, and media framing, remains moderate. Experts highlight the potential and limitations of digital deliberative mechanisms for democratic legitimacy. The study recommends developing secure, transparent digital platforms to improve public consultations in security policy-making. While Poland's technological infrastructure supports digital inclusion, uneven participation underscores the need to strengthen capacities for genuine democratic co-creation in security governance.

KEYWORDS: National security, governance, digitalization, deliberative democracy, Poland

Received: 12/08/2025
Revised : 27/08/2025
Accepted: 10/09/2025

1. Introduction. The digital transformation of public life has significantly reshaped the mechanisms through which citizens engage in democratic processes. In the domain of national security, where decisions often occur behind closed doors, digital tools offer a potential avenue for increasing transparency, accountability, and civic engagement. However, the integration of such tools into security governance presents complex challenges, particularly concerning misinformation, institutional capacity, and ethical oversight.

Governance institutions must change to incorporate wider participation and guarantee open policy responses in an increasingly complex security context that includes cybersecurity, surveillance, public safety, and digital disinformation. Digital technologies have the potential to increase the visibility of security issues in policymaking, promote discussion, and close gaps between government institutions, young civic actors, and technical specialists—especially when they are co-adopted by students and security experts.

Moreover, in the digital era, governments worldwide are increasingly exploring e-governance tools to enhance citizen engagement in public policy, including national security. Yet, the effectiveness of these tools depends heavily on public trust in institutions and the perceived legitimacy of digital participation mechanisms.

From a theoretical perspective, Habermas's Theory of Communicative Action underpins the value of inclusive discourse, stressing that decision-making legitimacy hinges on open, reasoned communication among diverse stakeholders—including novices and specialists (e.g., students and security experts)—within an "ideal speech situation" (McCarthy et al., 2023).

Decidim, an open-source, free digital infrastructure that was first created in Barcelona to support participatory democracy through processes including referenda, public consultations, assemblies, and participatory budgeting, is one notable example (Barandiaran et al., 2024). Designed to democratically structure decision-making processes across technological, political, and community aspects, Decidim is an example of a "technopolitical" platform (Barandiaran et al., 2024). In a similar vein, Pol.is uses statistical clustering and machine learning to combine vast amounts of citizen input into logical patterns of agreement and disagreement. Pol.is is an example of how computational tools may scale deliberative processes in high-stakes governance domains (Soper, 2014).

The significance of inclusive, logical discourse as a foundation for valid policy decisions is emphasized by foundational theories of deliberative democracy as defined by academics such as Rawls and Habermas (e.g., Rawls' "original position" and Habermas' "ideal speech situation"; Polsci Institute, 2024). Furthermore, empirical research demonstrates that the quality and efficacy of civic discourse are strongly impacted by the design of online debate, including choices regarding anonymity, media richness, and moderator responsibilities (Davies & Chandler, 2013).

Although digital platforms for involvement are becoming more and more popular, their effectiveness in real governance settings still depends on the circumstances. Deliberative outcomes, for instance, depend on how well platforms incorporate debate, accountability, and meaningful feedback loops. These observations imply that digital tools such as Decidim and Pol.is have the capacity to revolutionize security governance through the structuring of citizen participation, the development of wider legitimacy, and the facilitation of evidence-based policy debates. However, in order to realize this potential, careful planning, institutional integration, and continuous assessment are needed to make sure that these instruments promote genuine deliberative democracy rather than only token or surface-level involvement.

Poland's complex media landscape and evolving digital infrastructure make it a compelling context to investigate how digital tools can foster civic engagement in the realm of security. This paper investigates how digital tools influence public participation in security-related decision-making by analyzing expert perspectives from academia and practice. The central question guiding this study is: What are the opportunities and limitations of using digital platforms for deliberative democracy in the context of national and public security?

In the context of Polish security governance, this study examines how digital tools might improve deliberative democracy and encourage public engagement. The study, which sits at the nexus of democratic practice and digital transformation, gives special attention to the viewpoints of future policymakers because it acknowledges their potential impact on how governance systems develop over the next several decades. Using a mixed-method study methodology, it incorporates media narratives, structured student surveys, expert interviews, and a thorough examination of national policy texts.

Students from War Studies University's Faculty of National Security in Warsaw participated in the poll, which reveals a complex participation environment. Digital platforms are frequently used for information retrieval and policy discourse monitoring, but they are still mostly underutilized for active civic involvement, such as participating in policy consultations, starting public debates, or contributing to decision-making processes. Moderate levels of institutional trust are influenced by media framing, perceived transparency, leadership skill, and response to public concerns.

The dual nature of digital deliberation is further highlighted by insights from security and governance experts. While it presents new avenues for inclusivity, quick feedback, and cross-sector discussion, it also faces obstacles like low motivation for participation, gaps in digital literacy, and doubts about the veracity of online discourse. Collectively, these results add to larger discussions about how digital spaces might be strategically used to strengthen democratic legitimacy in security policies, but they also highlight structural and cultural obstacles that need to be removed in order for their full potential to be achieved.

2. Policy and Media Context: Digital Transformation, Public Consultation, and Civic Initiatives in Poland and the EU

Poland has made consistent attempts to modernize public administration and advance open government, according to an analysis of national policy documents. However, there are still obstacles in utilizing digital tools for civic engagement, especially in the area of security governance.

In order to promote public engagement, the Open Government Data Review of Poland (OECD, 2015) emphasized the necessity of shifting from compliance-driven data release to a proactive, value-oriented, whole-of-government strategy with greater governance and stakeholder collaboration. Although its framing was more bureaucratic than consultative, the National Integrated Informatization Programme 2020 (PZIP), launched in 2016, sought to enhance citizen communication with public administration through shared digital infrastructure and ICT deployment (European Commission, 2019). More recently, the Digitalization Strategy for Poland 2035, which is presently up for public comment, lays out a comprehensive agenda that includes the adoption of AI technologies, cybersecurity, digital skills development, fair digital transformation, and seamless administrative system integration (Algolytics, 2025; Warsaw Business Journal, 2025). A similar paradigm shift toward systemic societal digitalization beyond traditional e-government services is marked by the Landmark National Digital Strategy, which outlines four key pillars: digital infrastructure, cybersecurity, digital competencies, and technological innovation (Decent Cybersecurity, 2025).

In anticipation of the Digital Networks Act's implementation by December 2025, Poland's 2025 EU Council Presidency agenda places a strong emphasis on bolstering cybersecurity, AI governance, and digital infrastructure (Bird & Bird, 2025). In addition to EUR 12.4 billion in planned measures for advancing quantum computing, artificial intelligence, cybersecurity, and digital literacy, the Digital Decade Country Report recognizes strong fixed internet infrastructure but also points out ongoing deficiencies in citizens' digital skills and limited business adoption of advanced technologies (European Commission, 2025). With around 8 million users, Poland's leading digital identity platform, mObywatel, exemplifies service innovation by providing digital ID, driver's license, polling station details, car history, and local environmental data. To legitimize such tools, privacy-by-design and openness are still crucial (The Guardian, 2025).

Analyses of documents and the media show that although there are institutional structures for consultation, their actual application varies. The media, civil society, and citizens did not actively participate in establishing data priorities, according to the OECD evaluation (OECD, 2015). Poland has implemented creative local-level methods, like citizens' budgets, according to comparative studies of European public consultation practices; nonetheless, digital e-consultation is still disjointed and uneven when compared to more comprehensive EU models (Council of Europe, 2024). While highlighting modernization and ease, media coverage of programs like as mObywatel frequently echoes privacy campaigners' worries that a lack of transparency could erode public confidence (The Guardian, 2025). According to polls, individual individuals' engagement in digital policy, including consultations on the Digital Markets Act or infrastructure strategies, is still low in the larger EU discourse (Publyon, 2025).

Analysis reveals four important points:

1. Robust but bureaucratic policy architecture – Poland's digital plans offer state-of-the-art services and infrastructure, but they often do not include formalised consultation processes, especially when it comes to security management.

2. Uneven consultation procedures: While formal frameworks exist, they are not always supported by easily accessible, secure digital platforms at the federal level.

3. Tensions in media framing: Reporting highlights the advantages and disadvantages of digital tools, illustrating the interplay between concerns about democratic legitimacy and technological optimism.

4. Comparative EU context: Poland is well on its way to promoting meaningful digital civic engagement, yet there is some lag among groups with lower levels of digital skill, even while following EU trends in infrastructure and service implementation.

The rapid digital transformation of the state has produced a previously unheard-of technical capacity for public engagement, but without an equally robust participatory design, these tools risk reinforcing service delivery models rather than empowering citizens to shape security policy. This combined political and media context highlights a fundamental paradox for Poland, but also in many other European countries.

2.1 Security Governance in Poland

Digital tools are being used more and more in Poland's security administration to both strengthen and limit governmental control over key infrastructures and cyberspace. Cyber resilience is framed as a cross-sectoral responsibility in the Republic of Poland's 2019–2024 Cybersecurity Strategy, which calls for state-level monitoring systems, incident response capabilities, and the protection of e-government identity and service platforms as elements of national critical infrastructure (Government of Poland, 2019).

Operating within the Research and Academic Computer Network (NASK), CERT Polska serves as the operational hub for Poland's Computer Security Incident Response Team ecosystem. As the primary instrument for identifying, coordinating, and responding to cyber occurrences inside the national domain, CERT Polska carries out incident handling, threat analysis, and public advisories (CERT Polska, 2024). National cybersecurity systems complement these operational capabilities by enhancing situational awareness for public agencies and operators of critical services through real-time monitoring and integrated warning (National Centre for Research and Development, 2022).

It is important that online platforms simplify citizen-state interactions in order to improve administrative efficiency. However, they also represent high-value cyber targets whose compromise could erode public trust and disrupt essential services (examples include platforms such as Profil Zaufany / ePUAP, mObywatel) (Gov.pl, 2023). Consequently, security governance in Poland links cyber defense measures directly to the design and operation of such services. Through a combination of legislative measures, sectoral obligations for vital service operator, CSIRT op erations, training, and innovation assistance, the Cybersecurity Strategy places these capabilities inside a n integrated governance framework from a policy standpoint.
The NIS Directive, which binds domestic capacities to larger transnational governance regimes, is one o f the EU regulations that this framework is in line with (Government of Poland, 2019).

There are three research and policy evaluation implications that follow:

- As demonstrated by CERT Polska's incorporation into national response strategy, the sociotechn ical coupling of platforms and governance necessitates concurrent technical and institutional exa mination (CERT Polska, 2024).
- There is a tradeoff between centralization and resilience; unified identity services and centralize d monitoring enhance cooperation, but they may also introduce single points of failure (Govern ment of Poland, 2019).

- The lack of publicly available data on incident response results continues to hinder the measure ment of policy execution, underscoring the necessity of more operational metrics openness (CE RT Polska, 2024; Gov.pl, 2023).

3. Empirical research framework

3.1. Methodology

This mixed-methods study was conducted directly and via email during June and July 2025, combining a quantitative survey and qualitative interviews. The quantitative component involved a survey administered to sixty students (N = 60) from the War Studies University in Warsaw, representing various academic years and including both undergraduate and master's students.[1] The instrument comprised 13 questions divided into four thematic sections: (1) Demographics; (2) Institutional Trust; (3) Digital Deliberation; and (4) Future Outlook, with responses including both Likert scale ratings and open-ended qualitative input. The qualitative component consisted of semi-structured interviews with fifteen experts in the field of security governance, including academic professionals from the War Studies University, police practitioners, and analysts. These interviews followed a standard expert questionnaire of 15 open-ended questions, and the responses were thematically analyzed to identify common patterns, divergent views, and emergent insights. Data was coded manually, and themes were synthesized across three broad domains: (1) democratic deliberation and digital tools; (2) risks and ethical considerations; and (3) institutional readiness and future outlook.

The main hypothesis of the empirical research is: "Increasing institutional capacity, digital literacy, and trust is anticipated to move participants toward more optimistic engagement patterns. Digital tools have the potential to improve public participation and deliberative democracy in security governance, but their actual impact is limited by perceived platform safety, institutional trust levels, and cultural attitudes toward privacy."

[1] The empirical analysis presented in this study was conducted during a research stay funded by the STSM Grant at War Studies University, Warsaw, Poland, June 2025, within the framework of COST Action CA22149 — The Research Network for Interdisciplinary Studies of Transhistorical Deliberative Democracy (CHANGECODE)

3.2.Qualitative research – Findings

Table 1.

Participant Demographics

Gender

Category	**n**	**%**
Male	33	55.0
Female	25	41.7
Unspecified	2	3.3

Age Range (years)

Category	**n**	**%**
20	5	9.1
21	37	67.3
24	6	10.9
<35	7	12.7

Study level

Category	**n**	**%**
Graduate students	45	75.0
Master students	10	16.7

Democratic Deliberation and Digital Tools

Experts noted that digital tools can enhance participatory democracy by reducing traditional barriers such as geography and accessibility. Academic respondents cited successful examples like participatory budgeting in Warsaw and the use of the Polis platform in Taiwan. However, few police practitioners expressed skepticism, citing social polarization and limited political cooperation as major obstacles to meaningful digital engagement.

Risks and Ethical Considerations

All participants highlighted the dangers posed by misinformation, disinformation, and manipulation, particularly through artificial intelligence. Several academics warned that digital tools ″can become a dangerous force in the possession of the wrong entities,″ while another emphasized the need for European-developed platforms to prevent foreign influence. Ethical concerns centered on surveillance and cultural differences in privacy expectations.

Institutional Readiness and Future Outlook

There was consensus that public institutions are not yet adequately equipped to handle secure and inclusive digital consultations. The generational digital divide also impacts both trust and literacy levels, with older populations more vulnerable to misinformation. While academic experts predicted continued growth in digital participation, the practitioners anticipated a decline due to public distrust and unchecked disinformation.

The findings reveal a nuanced landscape in which digital tools hold promise for democratizing security governance but also pose significant risks. The optimism of academic respondents contrasts with the cautious scepticism of the practitioners and analysts, underscoring a gap between theoretical potential and field-level realities. Building institutional capacity, enhancing public digital literacy, and developing robust regulatory frameworks emerge as critical priorities. Furthermore, cultural dimensions of privacy and security must be integrated into digital tool design to ensure global applicability and legitimacy.

Table 2

Key Themes and Perspectives on Digital Tools in Security Governance

Theme	**Sub-Themes**	**Key Insights**	**Illustrative Quotes**
Digital Tools & Deliberative Democracy	Accessibility, Inclusion	Digital tools broaden access to deliberation, especially for traditionally excluded groups.	“Digital platforms can bring more voices into democratic discussions.”
	Political Division	Polarization reduces the feasibility of constructive digital dialogue.	“It is unrealistic to expect society to work together with politicians.”
Risks & Vulnerabilities	Misinformation, AI manipulation	Disinformation threatens legitimacy and trust in digital	“False information will lead to a loss of trust in

Theme	**Sub-Themes**	**Key Insights**	**Illustrative Quotes**
		platforms.	this type of solution.”
	Foreign Influence	European-designed platforms preferred to avoid foreign data control.	“Chinese influence on some platforms poses a threat to democracy.”
Institutional & Public Readiness	Institutional capacity	Institutions lack the technical and governance tools to implement secure digital deliberation.	“In most cases, public institutions are not yet fully equipped.”
	Digital literacy gap	Generational digital divide affects participation and trust.	“Digital natives and digital migrants... can complement and learn from each other.”
Ethical and Governance Gaps	Legal frameworks	Surveillance and privacy expectations vary across cultures.	“In Europe, surveillance enters a sphere that many want to keep private.”
	Regulatory shortcomings	Current legal systems lag behind technological developments.	“There are many legal loopholes.”
Policy & Institutional Recommendations	Trust-building	Focus on education, transparency, and European control of digital tools.	“Citizens’ safety in the use of digital tools must be ensured.”
	Role of academia	Experts should act as educators and mediators.	“Academic institutions should serve as knowledge translators and watchdogs.”

Theme	**Sub-Themes**	**Key Insights**	**Illustrative Quotes**
Future Outlook	Divergent projections	Academics predict growth; practitioners foresee decline due to misinformation.	“Such tools will not be used… false information will lead to a loss of trust.”

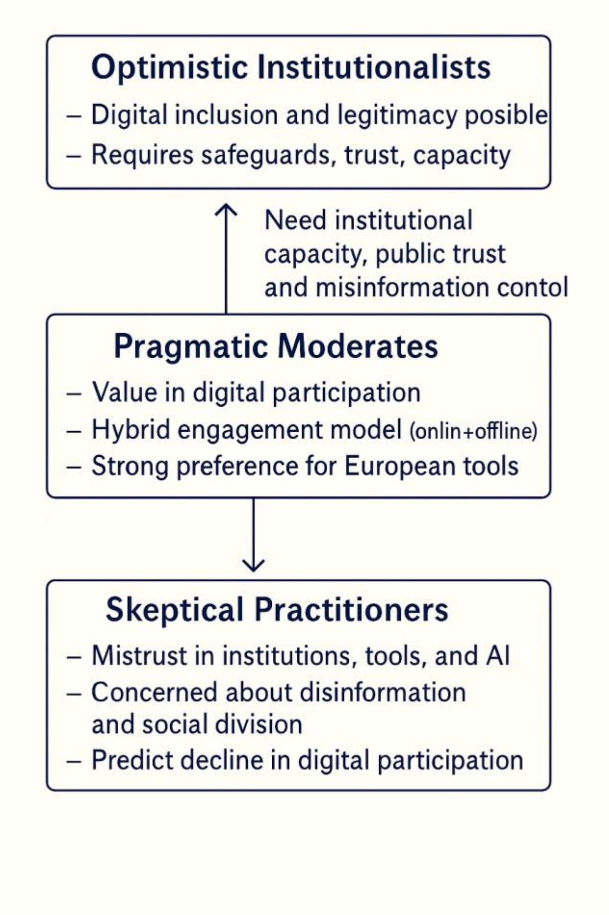
Optimistic Institutionalists
– Digital inclusion and legitimacy posible
– Requires safeguards, trust, capacity
Need institutional capacity, public trust and misinformation contol
Pragmatic Moderates
– Value in digital participation
– Hybrid engagement model (onlin+offline)
– Strong preference for European tools
Skeptical Practitioners
– Mistrust in institutions, tools, and AI
– Concerned about disinformation and social division
– Predict decline in digital participation

Figure 1. *Quantitative Analyses – Attitudinal Groups*

According the qualitative analysis, respondents can be divided into three different attitudinal groups: (1) Sceptical Practitioners; (2) Pragmatic Moderates; and (3) Optimistic Institutionalists, in order to examine viewpoints on digital participation, institutional trust, and the role of technology in civic engagement. Thematic coding of open-ended survey results, and interview transcripts produced these categories. Iterative in nature, the classification procedure used both inductive codes based on participants' own language and emphasis and deductive codes influenced by earlier research on digital democracy

Participants who express optimism that digital inclusion and legitimacy are feasible, given sufficient safeguards, trust-building strategies, and institutional competence, fall under the category of Optimistic Institutionalists. This group's responses focused on how technology might improve institutional legitimacy and public involvement, provided that disinformation is effectively managed and access is fair. Participants that support a hybrid engagement paradigm that combines online and offline resources but acknowledge the importance of digital participation make up the Pragmatic Moderates group. Participants in this group showed a clear preference for platforms created in Europe, pointing to higher perceived standards for data privacy and conformity to democratic values.

Participants in the Sceptical Practitioners group have a strong suspicion of organizations, technology, and artificial intelligence. Disinformation hazards, growing societal divide, and anticipated drops in future internet engagement rates were the main topics of their comments.

The visual framework's flow depicts possible group movement, emphasizing that if institutional capacity, public trust, and misinformation control increase, Pragmatic Moderates may move toward Optimistic Institutionalists. On the other hand, moderates may lean toward the Sceptical Practitioner viewpoint if trust and governance capability deteriorate. Because public perceptions of digital governance are dynamic, this dynamic stance was included in the analysis.

The three-group typology compresses a range of attitudes into distinct categories, even though it offers a helpful heuristic. When analyzing results, it is important to take into account the possibility of overlap, especially between Pragmatic Moderates and the other two groups. The study also recognizes that respondents' opinions are influenced by particular technological, cultural, and political circumstances, which may restrict generalizability.

Table 3

Participant Demographics

Gender

Category	**n**	**%**
Male	8	53.3
Female	7	46.7

Age Range (years)

Category	**n**	**%**
20-35	6	40.0
36-55	7	46.7
Over 56	2	13.3

Profession

Category	**n**	**%**
University professors	7	46.7
Analyst	3	20.0
Police practitioners	5	33.3

Institutional Trust

Table 4

Respondents were asked to rate their trust (1–5) in five key institutions

Institution	**Avg. Trust**	**Range**
Police	4.33	4–5
National Security Agencies	3.33	3–4
Government Ministries	3.00	3–3
Judiciary	3.00	3–3
Local Government	3.33	3–4

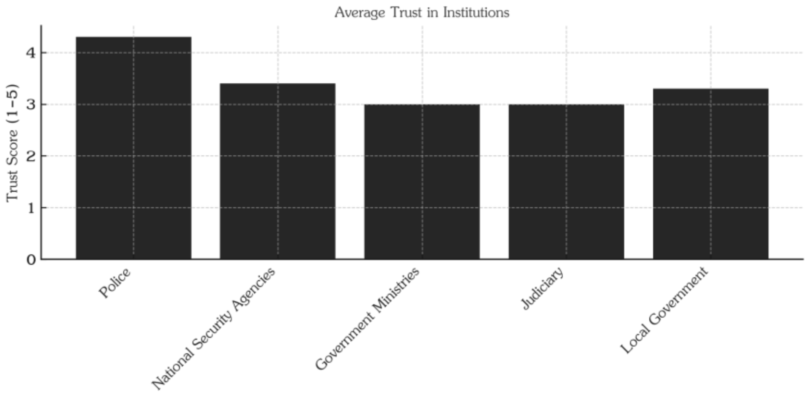

Figure 2. *Average Trust in Institutions Chart*

Table5

Digital Engagement Perception (Likert Scale Averages)

Statement	**Avg. Score**	**Interpretation**
Digital tools increase transparency	3.67	Moderate
Willingness to join consultations	3.25	Low–Moderate
Belief that digital tools help influence policy	3.67	Moderate
Confidence to share opinions online	2.67	Low
Suitability of digital platforms for security discussion	3.25	Mixed

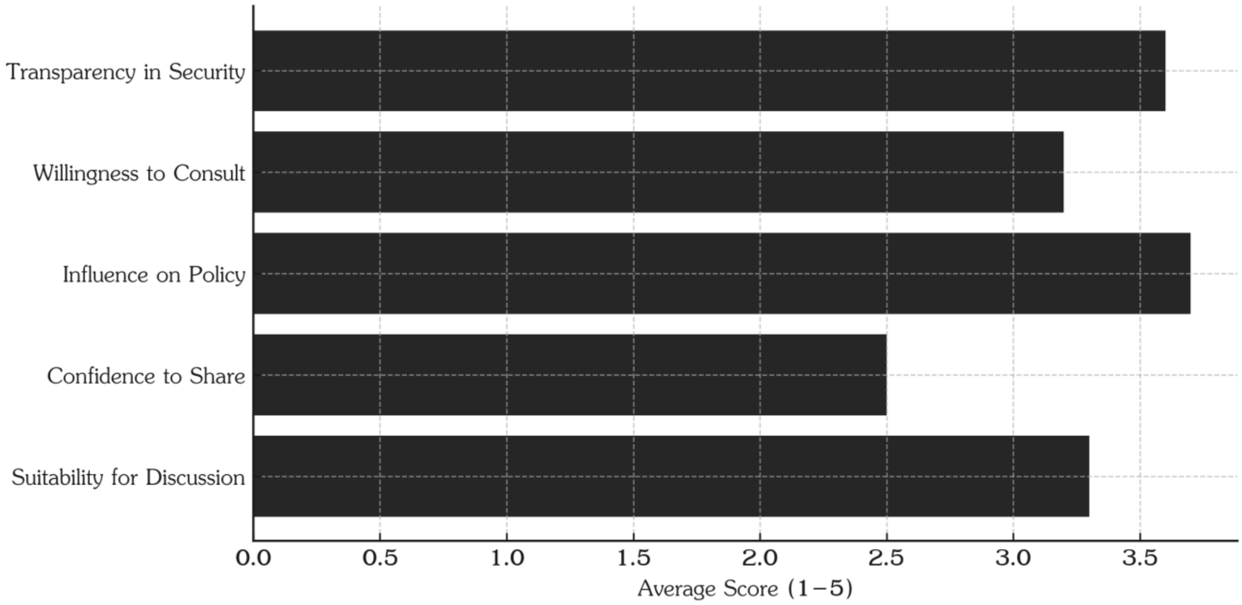

***Figure 3**. Likert Scale Averages Chart*

Participation in Digital Platforms

- Yes: 20
- No: 37
- Unanswered: 3

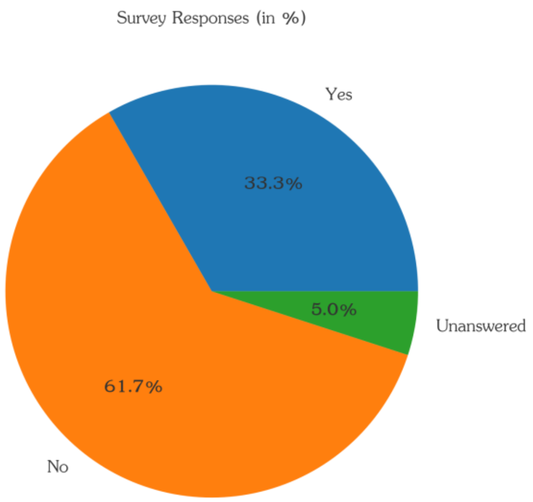

***Figure 4**. Participation Frequency Pie Chart*

Thematic Analysis

1) Factors Influencing Institutional Trust:

- Media polarization and propaganda
- Lack of transparency and political neutrality
- Institutional leadership and competence
- Crisis response and communication quality

2) Concerns About Digital Participation:

- Surveillance and data privacy risks
- Misinformation and extremist narratives
- Limited impact of public input
- Lack of personalization in digital interactions

3) Features Encouraging Digital Civic Engagement:

- Awareness campaigns
- Government-verified platforms
- User-friendly interfaces with anonymity
- Clear evidence of impact from public input

4.Discussion

The data indicates a generational openness to digital engagement, albeit coupled with skepticism about institutional responsiveness and digital safety. While students trust the police more than other institutions, their willingness to engage is contingent on how seriously their input is taken. The findings underscore a need for improved civic digital infrastructure, transparency, and communication strategies from government bodies.

With the police having the highest average trust score (M = 4.33) and a tight range (4–5), the results show a clear hierarchy in respondents' institutional trust, indicating consistently high confidence throughout the sample. Conversely, there was a substantial amount of diversity (3–4) in the level of trust in local government and national security services, which reflected mixed but generally positive attitudes (M = 3.33).

The court and government departments also had lower scores (M = 3.00) with no range variation, indicating consistently neutral levels of trust. A consistent but unenthusiastic appraisal may be indicated by the lack of variance in these two institutions, which could be a reflection of judgments of inefficiency, bureaucracy, or inadequate response.

Overall, the results indicate that people are more trusting of organizations that are seen as directly maintaining public safety (police, security agencies) than of those that are linked to political or administrative roles (ministries, judiciary, local government). This trend is consistent with research showing that institutions that are visible and focused on providing services typically inspire greater public trust. The consistently low variability across a number of assessments, however, points to deeply ingrained perceptions of particular organizations that would be difficult to alter in the near term. The findings show that respondents' perceptions of digital engagement are largely moderate. A acknowledgment of digital technologies' potential significance in governance and participatory decision-making is indicated by the opinion that they can affect policy (M = 3.67) and promote transparency (M = 3.67). These modest scores also suggest that these advantages are not yet thought to be completely understood or experienced by everyone. Perceptions of platform fit for security debates (M = 3.25) and willingness to participate in consultations (M = 3.25) are in the low-moderate to mixed range, suggesting cautious participation in more time-consuming or delicate participatory activities. This could be a reflection of worries about these engagements' perceived effectiveness, accessibility, or trust.

Interestingly, the lowest confidence score (M = 2.67) was for online opinion sharing, suggesting that this could be a barrier to active engagement. This is consistent with research showing that user expression can be restricted by problems like privacy concerns, fear of retaliation, and low confidence in digital discourse environments. Collectively, these results imply that although digital tools are appreciated for their openness and power, contextual and psychological elements may prevent more active and transparent online participation.

According to the statistics, just one-third (33.3%) of the Faculty of National Security students said they use digital platforms, whilst the vast majority (61.7%) said they don't, and 5% did not respond. Given the increasing significance of digital tools in academic, professional, and security-related contexts, this comparatively low level of engagement is noteworthy. Concerns about information security and privacy, a lack of institutional support and training for efficient use, or a restricted perception of the relevance of digital platforms to their subject of study are some possible factors. The high percentage of non-participants can indicate a possible lack of digital competency or a cautious approach based on the students' security-conscious mindset. The 5% non-response rate may indicate a lack of clarity regarding the definition of "participation," which emphasizes the need for more precise definitions and education within this student body. These results point to a chance for focused interventions to incorporate safe and intentional usage of digital platforms into the curriculum, bringing students' abilities into line with the needs of the modern workplace.

According to the findings presented in the qualitative and quantitative research framework, the hypothesis is confirmed, i.e., "Increasing institutional capacity, digital literacy, and trust is anticipated to move participants toward more optimistic engagement patterns. Digital tools have the potential to improve public participation and deliberative democracy in security governance, but their actual impact is limited by perceived platform safety, institutional trust levels, and cultural attitudes toward privacy."

These findings have a direct connection to:

- The three-group typology—Optimistic Institutionalists, Skeptical Practitioners, and Pragmatic Moderates—and the potential for transitioning between them.
- The hierarchy of trust (police at the top, political and administrative institutions at the bottom).
- The measured levels of engagement (online opinion sharing received the lowest scores, while transparency and policy effect received modest marks).
- The student participation gap (low platform use despite relevance to their field).

5.Conclusion. Digital platforms can support public participation in national security governance, but only if implemented with strong safeguards, inclusive design, and continuous oversight. Policymakers should invest in digital literacy programs, support European-led technological infrastructure, and involve academic and civic institutions in shaping ethical frameworks. Future research should expand the participant base and explore longitudinal impacts of digital tools on public trust and democratic legitimacy in the security domain. Digital platforms hold potential as democratic tools in security governance, especially among educated youth. However, to realize this potential, institutions must enhance transparency, demonstrate responsiveness, and adopt secure, inclusive platforms. National strategies should prioritize civic literacy and integrate localized consultations as a foundation for wider digital participation in security matters.

The results from the both qualitative and quantitative research show a generational pessimism regarding digital safety and institutional responsiveness along with an openness to digital involvement. Government agencies should place a high priority on creating a strong digital infrastructure that guarantees accessibility, security, and openness in order to increase public engagement. Efforts to promote engagement should take advantage of these reliable channels while addressing privacy and the efficacy of digital platforms, as police and security organizations are more trusted than political institutions. Additionally, incorporating training on digital competency—particularly for students who are concerned about security—into academic programs can aid in closing the gap between potential and actual digital engagement. Building trust and promoting more active, meaningful participation in digital civic spaces requires clear communication tactics and improved institutional responsiveness.

Recommendations

1. Create civic awareness campaigns using local digital media and educational institutions.
2. Integrate public consultation modules into national and regional security platforms.
3. Enhance data privacy and moderation on civic engagement sites.
4. Expand training in digital policy and cybersecurity within university programs.

References

Algolytics. (2025). *Digitalisation of Poland 2035 – A strategy to shape the future*. https://algolytics.com/digitalisation-of-poland-2035-a-strategy-to-shape-the-future/

Barandiaran, X. E., Calleja-López, A., Monterde, A., & Romero, C. (2024). *Decidim, a technopolitical network for participatory democracy: Philosophy, practice and autonomy of a collective platform in the age of digital intelligence*. Springer. https://doi.org/10.1007/978-3-031-50784-7

Bird & Bird. (2025). *Poland sets out digital priorities for the next six months: Digital Networks Act and EU Council Presidency agenda* [Industry insight]. https://www.twobirds.com/en/insights/2025/poland-sets-out-digital-priorities-for-the-next-six-months

CERT Polska. (2024). *About CERT Polska*. NASK. https://cert.pl/en/

Davies, T., & Chandler, R. (2013). Online deliberation design: Choices, criteria, and evidence. https://doi.org/10.48550/arXiv.1302.5177

Decent Cybersecurity. (2025). Poland unveils landmark Digital Strategy 2035: A comprehensive roadmap for digital transformation [Industry report]. https://decentcybersecurity.eu/poland-unveils-landmark-digital-strategy-2035-a-comprehensive-roadmap-for-digital-transformation/

European Commission. (2019). *National Integrated Informatization Programme 2020 (PZIP)* [Report].

European Commission. (2025). *Digital Decade Country Report*. https://digital-strategy.ec.europa.eu/en/library/digital-decade-2025-country-reports

Gov.pl. (2023). *ePUAP and Trusted Profile (Profil Zaufany)*. https://www.gov.pl/web/profilzaufany

Government of Poland. (2019). *Cybersecurity strategy of the Republic of Poland for 2019–2024*. Ministry of Digital Affairs. https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa

McCarthy, S., Rowan, W., Mahony, C., & Vergne, A. (2023). The dark side of digitalization and social media platform governance: A citizen engagement study. *Internet Research, 33*(6), 2172–2204. https://doi.org/10.1108/INTR-03-2022-0142

National Centre for Research and Development. (2022). *National Cybersecurity Platform*. https://www.ncbr.gov.pl

OECD. (2015). *Open government data review of Poland: Unlocking the value of government data*.

OECD Publishing. https://doi.org/10.1787/9789264231442-en

Polsci Institute. (2024). *Deliberative democracy: The role of reasoned discussion in politics* [Educational resource].https://polsci.institute

Publyon. (2025). *EU digital policy update* (No. 25) [Policy brief]. https://publyon.com/eu-digital-policy-update-no-25/

Soper, T. (2014). Startup spotlight: Pol.is uses machine learning, data visualization to help large groups spur conversation. *GeekWire*.https://www.geekwire.com

The Guardian. (2025, January 26). Convenient or intrusive? How Poland has embraced digital ID cards. https://www.theguardian.com/technology/2025/jan/26/poland-digital-id-cards-e-government-app

Warsaw Business Journal. (2025). *Government presents draft of Polish digitization strategy, including AI* [News article].https://wbj.pl/government-presents-draft-of-polish-digitization-strategy-including-ai/post/143895