วารสารวิชาการผลประโยชน์แห่งชาติ
Thai Journal of National Interest
ISSN (Online): 2730-2393

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

Enhancing Public Participation and Deliberative :Digital Tools in Security Governance the case of Poland - Democracy

Prof. Dr. ***Katerina Veljanovska Blazhevska***
E-mail:veljanovska_katerina@yahoo.com
Faculty of Security Science, MIT University- Skopje(North Macedonia)
Prof. Dr. ***Ryszard Szpyra***
E-mail:r.szpyra@gmail.com
Head of the Department of Information Security
Faculty of National Sceurity, 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.

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

2025/08/12 :Received

: Revised 27/08/ 2025

:Accepted10/09/2025

1. The digital transformation of public life has significantly reshaped the mechanisms **.Introduction** In the domain of national security .through which citizens engage in democratic processes, where decisions often occur behind closed doors, digital tools offer a potential avenue for increasing transparency, accountability, However .and civic engagement, 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, Digital technologies have the potential to increase the visibility of .and digital disinformation security issues in policymaking, promote discussion, and close gaps between government institutions, young civic actors, adopted by students and -especially when they are co—and technical specialists .security experts

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

From a theoretical perspective, s Theory of Communicative Action underpins the value 'Habermas of inclusive discourse, making legitimacy hinges on open-stressing that decision, reasoned ,.g.e) including novices and specialists—communication among diverse stakeholdersstudents and security experts)— ,.McCarthy et al) "ideal speech situation" within an2023).

Decidim, source-an open, free digital infrastructure that was first created in Barcelona to support participatory democracy through processes including referenda, public consultations, assemblies, and participatory budgeting, ,.Barandiaran et al) is one notable example2024 ;Aragón et al. ,201 .(7 making processes across technological-Designed to democratically structure decision, political, and community aspects, ,.Barandiaran et al) platform "technopolitical" Decidim is an example of a2024). In a similar vein, is uses statistical clustering and machine learning to combine vast amounts of citizen .Pol is is an example of how computational .Pol .input into logical patterns of agreement and disagreement Soper) stakes governance domains-tools may scale deliberative processes in high, .(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 ,.g.e) and HabermasRawls' "Polsci Institute) ("ideal speech situation" 'and Habermas "original position, Furthermore .(2024, 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, Davies) and moderator responsibilities& Chandler, .(2013

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

s complex media landscape and evolving digital infrastructure make it a compelling context 'Poland This paper .to investigate how digital tools can foster civic engagement in the realm of security making by -related decision-investigates how digital tools influence public participation in security :The central question guiding this study is .analyzing expert perspectives from academia and practice 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 The study .deliberative democracy and encourage public engagement, 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 method study methodology-Using a mixed .the next several decades, 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, Digital platforms are frequently used for .which reveals a complex participation environment 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 Moderate levels of institutional trust are influenced by media framing .making processes-decision, perceived transparency, leadership skill, .and response to public concerns

The dual nature of digital deliberation is further highlighted by insights from security and While it presents new avenues for inclusivity .governance experts, quick feedback, sector -and cross discussion, it also faces obstacles like low motivation for participation, gaps in digital literacy, and doubts Collectively .about the veracity of online discourse, 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. Digital Transformation :Policy and Media Context, Public Consultation, and Civic Initiatives in Poland and the EU

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

In order to promote public engagement, OECD) the Open Government Data Review of Poland, driven data release to a proactive-emphasized the necessity of shifting from compliance (2015, -value oriented, .government strategy with greater governance and stakeholder collaboration-of-whole Although its framing was more bureaucratic than consultative, the National Integrated Informatization Programme2020 (,(PZIPlaunched in 2016, sought to enhance citizen communication with public European Commission) administration through shared digital infrastructure and ICT deployment, More recently .(2019, the Digitalization Strategy for Poland2035 ,which is presently upfor 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; WBJ, A similar paradigm shift toward systemic societal digitalization beyond .(2025 government services is marked by the Landmark National Digital Strategy-traditional e, which outlines digital infrastructure :four key pillars, cybersecurity, digital competencies, and technological innovation Decent Cybersecurity), .(2025

In anticipation of the Digital Networks Act' s implementation by December2025 ,Poland's 2025 EU Council Presidency agenda places a strong emphasis on bolstering cybersecurity ,AI governance ,and dig Bird) ital infrastructure& Bird, In addition to EUR .(202512. 4billion 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' European Commission) digital skills and limited business adoption of advanced technologies, With around .(20258 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 To legitimize such tools .environmental data, The) design and openness are still crucial-by-privacy Guardian, .(2025

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

:Analysis reveals four important points

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

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

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

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

of technical -The rapid digital transformation of the state has produced a previously unheard capacity for public engagement, but without an equally robust participatory design, these tools risk This .reinforcing service delivery models rather than empowering citizens to shape security policy 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

Cyber resilience is .strengthen and limit governmental control over key infrastructures and cyberspace sectoral responsibility in the Republic of Poland-framed as a cross' s2019- 2024Cybersecurity Strategy ,which calls for state-level monitoring systems, incident response capabilities, and the government identity and service platforms as elements of national critical infrastructure-protection of e Government of Poland), .(2019

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

state interactions in order to improve -It is important that online platforms simplify citizen However .administrative efficiency, value cyber targets whose compromise -they also represent high examples include platforms such as Profil Zaufany) could erode public trust and disrupt essential services ePUAP /, pl.Gov) (mObywatel, 2023a ;Gov.pl, 2023b). 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; pl.Gov, 2023a).

3. Empirical research framework

3.1. Methodology

methods study was conducted directly and via email during June and July-This mixed2025 , combining a quantitative survey and qualitative interviews. The quantitative component involved a survey from the War Studies University in Warsaw (60 = N) administered to sixty students, representing various The instrument comprised [1].s students'academic years and including both undergraduate and master13 Demographics (1) :questions divided into four thematic sections; (Institutional Trust (2; (Digital (3 ;Deliberationand (Future Outlook (4, ended -with responses including both Likert scale ratings and open structured interviews with fifteen experts -The qualitative component consisted of semi .qualitative input in the field of security governance, including academic professionals from the War Studies University, police practitioners, These interviews followed a standard expert questionnaire of .and analysts15 -open ended questions, and the responses were thematically analyzed to identify common patterns, divergent ,viewsand emergent insights. Data was coded manually, and themes were synthesized across three broad democratic deliberation and digital tools (1) :domains; (risks and ethical considerations (2; (3) and .institutional readiness and future outlook

:The main hypothesis of the empirical research is"Increasing institutional capacity, digital literacy, Digital tools .and trust is anticipated to move participants toward more optimistic engagement patterns 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

3.2. Findings - Qualitative research

Table1.

Participant Demographics

[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)

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 Academic respondents cited successful examples like participatory .such as geography and accessibility However .budgeting in Warsaw and the use of the Polis platform in Taiwan, 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, can become a ″ Several academics warned that digital tools .particularly through artificial intelligence dangerous force in the possession of the wrong entities,″ while another emphasized the need for Ethical concerns centered on surveillance .developed platforms to prevent foreign influence-European .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 The generational digital divide also impacts both trust and literacy levels .inclusive digital consultations, While academic experts predicted continued .with older populations more vulnerable to misinformation 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 The optimism of academic respondents contrasts with .security governance but also pose significant risks the cautiousscepticismof the practitioners and analysts , underscoring a gap between theoretical potential Building institutional capacity .level realities-and field, enhancing public digital literacy, and developing Furthermore .robust regulatory frameworks emerge as critical priorities, cultural dimensions of privacy .and security must be integrated into digital tool design to ensure global applicability and legitimacy

Table2

Key Themes and Perspectives on Digital Tools in Security Governance

Theme	**Themes-Sub**	**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 .platforms	“False information will lead to a loss of trust in this type of ”.solution
	Foreign Influence	designed -European platforms preferred to	“Chinese influence on some platforms poses

Theme	**Themes-Sub**	**Key Insights**	**Illustrative Quotes**
		avoid foreign data .control	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 can ...digital migrants 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	building-Trust	Focus on education, transparency, and European control of .digital tools	"safety in 'Citizens 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
Future Outlook	Divergent projections	Academics predict growth; practitioners	"Such tools will not false ...be used

Theme	**Themes-Sub**	**Key Insights**	**Illustrative Quotes**
		foresee decline due to .misinformation	information will lead ".to a loss of trust

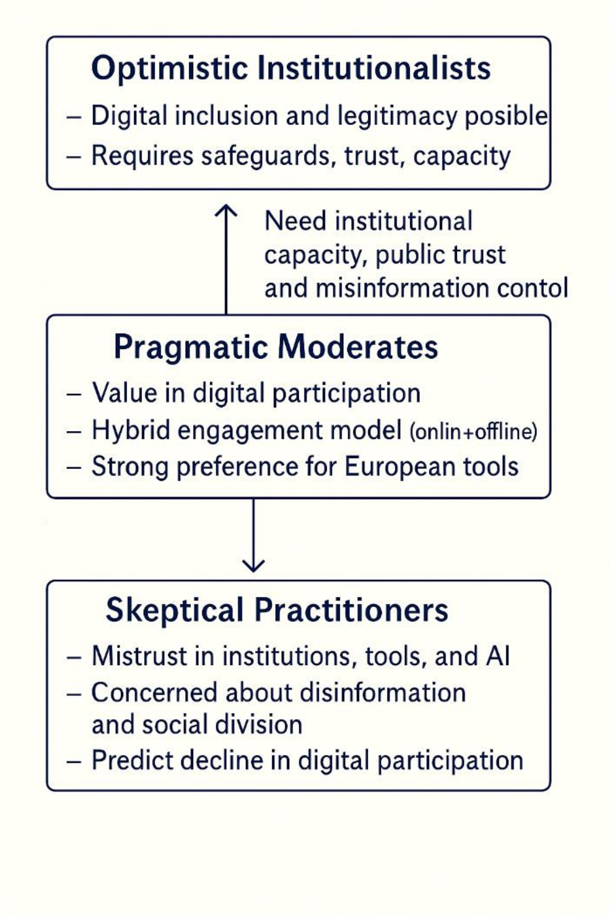
Optimistic Institutionalists
– Digital inclusion and legitimacy posible
– Requires safeguards, trust, capacity
Need institutional capacity, public trust and misinformation contol
Pragmatic Moderates
– Value in digital participation
– Hybrid engagement model (onlin+offline)
– Strong preference for European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

Figure 1. *Attitudinal Groups – Quantitative Analyses*

According the qualitative analysis, respondents can be divided into three different attitudinal (1) :groupsScepticalPractitioners ; (Pragmatic Moderates (2; Optimistic Institutionalists (3) and, in order to examine viewpoints on digital participation, institutional trust, and the role of technology in civic ended survey results-Thematic coding of open .engagement, and interview transcripts produced these Iterative in nature .categories, 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, building strategies-trust, and institutional competence, fall under the category of Optimistic This group .Institutionalists'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 theScepticalPractitioners group have a strong suspicion of organizations , technology, Disinformation hazards .and artificial intelligence, 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 On the other hand .Optimistic Institutionalists, moderates may lean toward theScepticalPractitioner Because public perceptions of digital governance .viewpoint if trust and governance capability deteriorate are dynamic, .this dynamic stance was included in the analysis

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

Table3

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

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

Institution	**Trust .Avg**	**Range**
Police	33.4	5–4
National Security Agencies	33.3	4–3
Government Ministries	00.3	3–3
Judiciary	00.3	3–3
Local Government	33.3	4–3

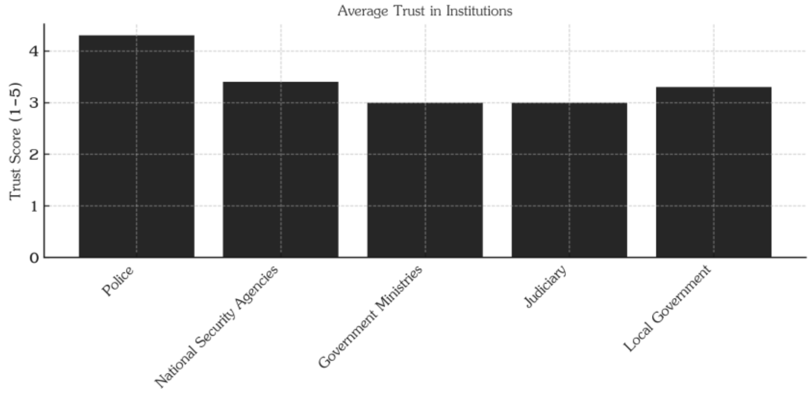

Figure2*. Average Trust in Institutions Chart*

Table5

(Likert Scale Averages) Digital Engagement Perception

Statement	**Score .Avg**	**Interpretation**
Digital tools increase transparency	67.3	Moderate
Willingness to join consultations	25.3	Moderate–Low
Belief that digital tools help influence policy	67.3	Moderate
Confidence to share opinions online	67.2	Low
Suitability of digital platforms for security discussion	25.3	Mixed

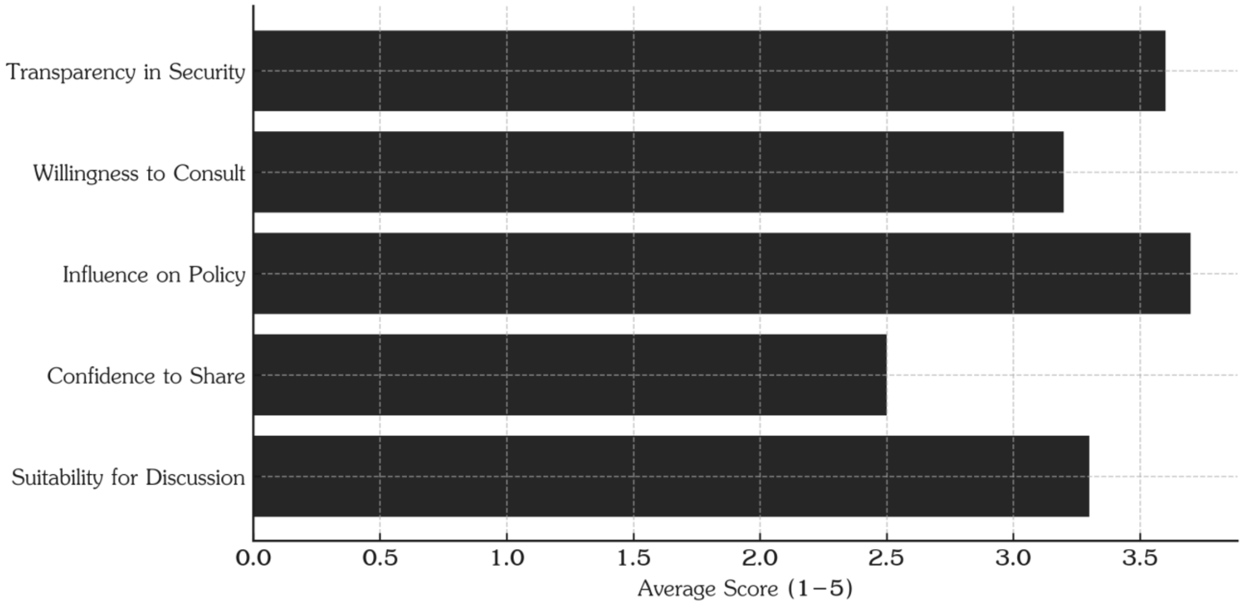

***Figure3**.Likert Scale Averages Chart*

Participation in Digital Platforms

□ 20 :Yes

□ 37 :No

□ 3 :Unanswered

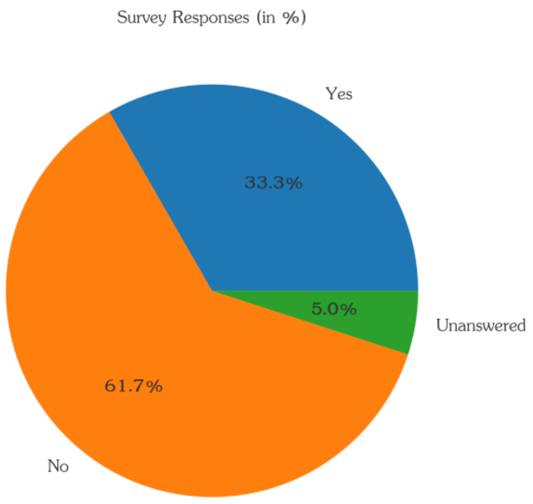

Figure4. *Participation Frequency Pie Chart*

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

□ verified platforms-Government

□ friendly interfaces with anonymity-User

□ Clear evidence of impact from public input

4.Discussion

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

,(5–4) and a tight range (33.4 = M) With the police having the highest average trust scorethe results show a clear hierarchy in respondents 'institutional trust ,indicating consistently high confidence throughout the sample. Conversely, in the level of (4–3) there was a substantial amount of diversity trust in local government and national security services, which reflected mixed but generally positive .(33.3 = M) attitudes

with no range variation (00.3 = M) The court and government departments also had lower scores, A consistent but unenthusiastic appraisal may be indicated .indicating consistently neutral levels of trust 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 police) maintaining public safety, than of those that are linked to political or (security agencies ministries) administrative roles, ,judiciarylocal government). This trend is consistent with research showing that institutions that are visible and focused on providing services typically inspire greater public The consistently low variability across a number of assessments .trust, however, points to deeply ingrained .perceptions of particular organizations that would be difficult to alter in the near term

The findings show that respondents' A .perceptions of digital engagement are largely moderate acknowledgment of digital technologies' -potential significance in governance and participatory decision and promote transparency (67.3 = M) making is indicated by the opinion that they can affect policy These modest scores also suggest that these advantages are not yet thought to be .(67.3 = M) .completely understood or experienced by everyone M) Perceptions of platform fit for security debates moderate to mixed -are in the low (25.3 = M) and willingness to participate in consultations (25.3 = range, This .consuming or delicate participatory activities-suggesting cautious participation in more time could be a reflection of worries about these engagements' perceived effectiveness, accessibility, .or trust

Interestingly, was for online opinion sharing (67.2 = M) the lowest confidence score, suggesting This is consistent with research showing that user .that this could be a barrier to active engagement expression can be restricted by problems like privacy concerns, fear of retaliation, and low confidence

Collectively .in digital discourse environments, 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, of the Faculty of National Security students (%3.33) third-just one said they use digital platforms, said they don (%7.61) whilst the vast majority't, and5% did not Given the increasing significance of digital tools in academic .respond, professional, related -and security contexts, Concerns about information security .this comparatively low level of engagement is noteworthy and privacy, a lack of institutional support and training for efficient use, or a restricted perception of the The high percentage of .relevance of digital platforms to their subject of study are some possible factors participants can indicate a possible lack of digital competency or a cautious approach based on the -non students' The .conscious mindset-security5% response rate may indicate a lack of clarity regarding -non participation" the definition of," which emphasizes the need for more precise definitions and education These results point to a chance for focused interventions to incorporate safe .within this student body 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 Digital tools have the potential to improve .participants toward more optimistic engagement patterns 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:

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

5.Conclusion. Digital platforms can support public participation in national security governance, but only if implemented with strong safeguards, inclusive design, Policymakers .and continuous oversight should invest in digital literacy programs, led technological infrastructure-support European, and involve Future research should expand the .academic and civic institutions in shaping ethical frameworks 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, However .especially among educated youth, to realize this potential, institutions must enhance transparency, demonstrate responsiveness, and adopt secure, National strategies .inclusive platforms 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, Efforts to .and openness in order to increase public engagement 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 Additionally .institutions, particularly for students who are —incorporating training on digital competency into academic programs can aid in closing the gap between potential and —concerned about security Building trust and promoting more active .actual digital engagement, 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.* SpringerBriefs in Political Science. Springer. https://doi.org/10.1007/978-3-031-50784-7

Bird & Bird. (2025). *Poland sets out digital priorities for the next six months: Bird & Bird insight, including Digital Networks Act and EU Council Presidency agenda.* 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.* https://decentcybersecurity.eu/poland-unveils-landmark-digital-strategy-2035-a-comprehensive-roadmap-for-digital-transformation/

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

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

Gov.pl. (2023a). *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

Hasler, S., Chenal, J., & Soutter, M. (2017). *Digital tools and citizen participation: Towards sustainable and responsive urban planning.* https://doi.org/10.5176/2425-0112_UPPD17.18

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 *Digital Government Studies.* OECD Publishing. https://doi.org/10.1787/9789264231442-en

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

Publyon. (2025). *EU digital policy update, No. 25.* 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.*https://wbj.pl/government-presents-draft-of-polish-digitization-strategy-including-ai/post/143895