FEMINIST ENCOUNTERS
A JOURNAL
OF CRITICAL STUDIES
IN CULTURE AND POLITICS

Feminist Encounters: A Journal of Critical Studies in Culture and Politics, 2026, 10(2), Article 11
eISSN: 2468-4414

lectito

Research paper

Algorithmic Visibility and Gendered Security Discourses in Postdigital Communication: From Digital Camouflage to Feminist Resistance

Marija Gombar [1]*, Maja Križanec Cvitković [2]

[1] *General Staff of the Armed Forces of the Republic of Croatia,* CROATIA
[2] *Primary school "Sračinec", 1st Private Gymnasium Varaždin,* CROATIA

*Corresponding Author: gombar.ma@gmail.com

Citation: Gombar, M., & Križanec Cvitković, M. (2026). Algorithmic visibility and gendered security discourses in postdigital communication: From digital camouflage to feminist resistance. *Feminist Encounters: A Journal of Critical Studies in Culture and Politics, 10*(2), Article 11. https://doi.org/10.20897/femenc/18718

Published: June 24, 2026

ABSTRACT

This article examines how female university students perceive algorithmic personalization as shaping gendered visibility in digital security communication. Drawing on postdigital feminism and feminist security studies, it conceptualises perceived algorithmic visibility as a postdigital security condition through which users interpret which bodies, voices, and critiques become more or less legible in militarized digital spaces. Empirically, the study is based on an online survey with 425 female university students in Croatia. The questionnaire measured subjective algorithmic awareness, institutional media trust, feminist engagement, and reported encounters with security-related content, and included open-ended questions on participants' perceptions of algorithmically mediated security communication. Statistical analyses identify four user segments—mainstream security consumers, neutral observers, critical analysts, and digital activists—who differ in levels of trust, subjective algorithmic awareness, and feminist engagement. Results show that 72% of respondents report primarily encountering security narratives through social media feeds they perceive as algorithmically curated, while active information seeking is rare. Higher institutional trust is associated with lower subjective algorithmic awareness, whereas greater subjective algorithmic awareness correlates with feminist engagement and scepticism toward mainstream military narratives. Qualitative responses indicate that participants perceive feminist security perspectives as less visible in their feeds and describe a dominance of state-centered and militarized content. The article argues that, in postdigital security publics, algorithmic systems are not only technical infrastructures but are also perceived and anticipated as epistemic actors that shape users' sense of visibility, legitimacy, and communicative agency. It calls for critical algorithmic literacy, more accountable platform governance, and feminist-informed policy approaches that safeguard epistemic diversity in postdigital security communication.

Keywords: algorithmic visibility, postdigital feminism, feminist security studies, digital activism, military communication

As military institutions embrace digital platforms for communication, the visibility of feminist perspectives in security discourse remains trapped behind algorithmic walls. The digital landscape has transformed how security discourses are constructed, disseminated, and interpreted. In an era where algorithmic personalization shapes information flows, the visibility of women in military and security narratives becomes increasingly contingent

upon opaque digital infrastructures. The intersection of postdigital feminism (Jandrić et al., 2018; Ross, 2022) and algorithmic visibility (Noble, 2018; Bucher, 2018) reveals significant power dynamics that influence the representation of gendered actors in security-related discussions. This study critically examines how young women perceive algorithmic systems as mediating their exposure to military discourses and security communication. In doing so, the article contributes to feminist media studies by framing algorithmic visibility as a gendered security infrastructure that organises how women and feminised bodies become knowable, governable, and resistant within postdigital communication.

Postdigital feminism acknowledges that digital spaces are not inherently liberatory but are embedded in broader sociotechnical power structures that reproduce inequalities (Costello et al., 2025; Lindberg & Johansson, 2023). While feminist activism has leveraged digital platforms for visibility and mobilization, these platforms operate within algorithmically governed ecosystems that often deprioritize or marginalize counter-narratives (D'Ignazio & Klein, 2020). Barnetz (2015) highlights the role of radical imagination as a tool for creating alternative security narratives that challenge hegemonic structures. As Banet-Weiser (2018) argues, the entanglement of popular feminism and widespread misogyny within digital spaces further complicates the visibility of feminist interventions, as platforms simultaneously promote feminist narratives while enabling forms of algorithmic suppression and backlash. This dual function of platforms highlights their role as neutral intermediaries and active participants in shaping security discourses. Through algorithmic curation, content moderation policies, and strategic partnerships with defense institutions, digital platforms perpetuate gendered security narratives, reinforcing militarized epistemologies while limiting the reach of feminist critiques (Gillespie, 2018; Benjamin, 2019). Furthermore, research has demonstrated that algorithmic curation creates ideological silos that limit users' exposure to diverse perspectives in security debates (Macgilchrist et al., 2024). Automated moderation systems disproportionately filter feminist and critical security perspectives, thus reinforcing dominant geopolitical narratives (Crawford, 2021). These tendencies are not merely technical limitations but structural enforcements of epistemic closure — mechanisms that prioritise engagement-maximizing content over epistemic diversity and inclusivity (Suzor, 2019). The influence of platform capitalism on security-related digital content raises urgent concerns about how algorithmic governance regulates epistemic authority in security communication (Broussard, 2018; Crawford, 2021). This aligns with Appadurai's (2000) argument about grassroots globalization, in which digital infrastructures enable and constrain knowledge flows in global security discourses.

This study builds on an interdisciplinary framework synthesizing feminist security studies, digital media research, and algorithmic governance to critically examine gendered power structures in security communication critically. The concept of sociological imagination (Atkins & Grant, 2022; Mills, 1959/2000; Palmer, 2023) is helpful in this regard, as it allows for a nuanced analysis of how individuals navigate algorithmically structured digital environments. By integrating perspectives from these fields, the study highlights how gendered power dynamics operate in digital security communication and influence online feminist activism. The concept of platform patriarchy (Banet-Weiser, 2018; D'Ignazio & Klein, 2020) is particularly relevant in this context, as digital infrastructures systematically prioritize institutionalized security narratives over alternative or feminist perspectives. This reinforces a data colonialism (Zuboff, 2019) paradigm in which feminist critiques of militarization remain algorithmically peripheral, even as platforms present themselves as neutral hosts for public debate. The concept of algorithmic visibility (Bucher, 2018; Noble, 2018) is central to understanding the digital curation of security narratives. Platforms such as social media, search engines, and news aggregators employ personalized content delivery systems that reinforce dominant perspectives while limiting exposure to alternative or feminist viewpoints (Zuboff, 2019; Crawford, 2021). This process shapes the perceived legitimacy of security institutions, the normalization of military narratives, and the extent to which gendered perspectives are included or excluded from public discourse (Sjoberg & Gentry, 2007). Furthermore, the gendered nature of security discourse is evident in how women's roles in military settings are framed. Traditional representations often oscillate between invisibility, victimhood, or exceptionalism, reinforcing binary gender hierarchies (Cohn, 1987; Enloe, 2000). Eichler (2012) examines how militarization reinforces gendered conscription policies and exclusionary security frameworks that privilege masculinized forms of defense. Feminist security scholars highlight the importance of disrupting these portrayals to ensure more inclusive and diverse security policies (Duncanson, 2013; Parashar, 2014). However, algorithmic mediation complicates these efforts, as personalized digital environments prioritize narratives that align with dominant power structures, constraining feminist critique and engagement (Bucher, 2018; Sjoberg, 2010).

This study investigates the role of algorithmic personalization in shaping young women's perceptions of military and security discourses, situating this inquiry within the broader framework of postdigital feminism and digital activism. Specifically, it examines how young women report and interpret algorithmic personalization as influencing their exposure to security and military narratives, how they perceive feminist perspectives as being promoted or restricted within military communication, and what barriers they associate with digital activism

related to security and defense. By integrating quantitative and qualitative methodologies, this research provides an empirical foundation for understanding the interplay between algorithmic systems and gendered security discourses. Through survey data and thematic analysis, it highlights both the constraints and opportunities for feminist engagement in security communication, ultimately contributing to broader discussions on the politics of visibility in postdigital societies (Jandrić et al., 2023; Macgilchrist et al., 2024).

This research makes three critical contributions. First, it enhances the understanding of gendered dynamics in algorithmic personalization within security discourses. Second, it exposes structural barriers to online feminist activism in the context of defense and military communication. Finally, it provides recommendations for more inclusive digital strategies that enhance the visibility of diverse perspectives in security debates. By bridging postdigital feminist theory, algorithmic governance, and security communication, this study expands ongoing discussions on how digital infrastructures shape epistemic authority, gendered visibility, and security narratives in the 21st century (Shepherd, 2008). To ensure more inclusive digital strategies, policymakers should prioritize the implementation of algorithmic transparency laws that prevent the systemic marginalization of feminist security perspectives (Gillespie, 2018). Platforms should also integrate participatory design mechanisms that involve feminist activists in shaping content-curation processes, thereby fostering a more equitable distribution of digital visibility (Suzor, 2019). Finally, investing in digital literacy initiatives that educate users about algorithmic bias is crucial for empowering diverse communities to critically engage with security discourses online (Jandrić et al., 2023; Oyewole, 2026). This is also consistent with recent postdigital work that uses speculative and future-oriented approaches to examine how digitalization reorganizes educational, social, and civic imaginaries (Hrastinski & Jandrić, 2023; Suoranta et al., 2022). It critically interrogates how digital infrastructures condition feminist engagement with security narratives and proposes methodological pathways for future research in postdigital feminist security studies. Graeber (2009) conceptualizes direct action as a means of bypassing institutional barriers and challenging dominant power structures, offering an alternative framework for feminist resistance in digital security spaces.

THEORETICAL FRAMEWORK

The study of military communication and security discourses has long been shaped by institutional structures that reinforce dominant geopolitical and national security paradigms. Castoriadis (1987) conceptualizes the imaginary institution of society, arguing that dominant ideologies shape collective perceptions, including security narratives. Haiven and Khasnabish (2014) explore how radical imagination fuels social movements by envisioning alternatives beyond hegemonic structures, reinforcing its relevance in feminist security activism. Kind (2016) examines the philosophy of imagination, showing how constructed realities shape perceptions of security and defense. More recent anthropological work on imagination similarly frames imaginaries as socially situated practices through which possible futures, risks, and collective orientations become thinkable (Rohrer & Thompson, 2023).

This emphasis on imagination is also consistent with broader philosophy of science debates that treat scientific imagination as central to modelling, explanation, and the construction of possible worlds (Levy & Godfrey-Smith, 2020). However, in the postdigital era, these discourses are increasingly mediated by algorithmic infrastructures that determine visibility and influence public engagement. Postdigital feminism offers a critical framework for understanding the digital reproduction of gendered inequalities, emphasizing that digital platforms are not neutral but instead operate within pre-existing power asymmetries (Raza et al., 2026; Ross, 2022). At the same time, recent postdigital scholarship shows that digital participation, civic agency, and knowledge production are increasingly shaped by data-driven infrastructures, making visibility and participation unevenly distributed within platformed environments (Jandrić et al., 2025).

Similarly, recent work on postdigital futures emphasizes that data-driven educational and communicative environments are not merely technical developments but contested sociopolitical arrangements in which agency, visibility, and participation are unevenly distributed (Buch et al., 2024). Bassett (2015) highlights that the postdigital condition requires rethinking feminist engagement with technology, as digital infrastructures shape and constrain possibilities for feminist resistance within contemporary algorithmic ecosystems. Koro-Ljungberg (2016) extends this perspective by critiquing traditional qualitative research frameworks and calling for adaptive, imaginative, and reflexive approaches that align with feminist epistemologies in digital contexts. While feminist activism has historically utilized digital spaces to challenge dominant narratives, the algorithmic curation of content often prioritizes mainstream security discourses over alternative or feminist perspectives, reinforcing existing gender hierarchies in military communication (Costello et al., 2025; Lindberg & Johansson, 2023). Jacobsen, Drake, and Petersen (2016) explore the role of creativity and rhetoric in social research, demonstrating its relevance in rethinking security discourses.

Algorithmic visibility, as a concept, highlights how personalized content delivery shapes public perception by selectively amplifying some voices while marginalizing others (Bucher, 2018; Noble, 2018). Previous studies have

demonstrated that algorithmic curation favors dominant geopolitical and military narratives while sidelining feminist perspectives on security (Crawford, 2021). This asymmetry in visibility reinforces the marginalization of critical feminist voices and restricts public engagement with alternative security frameworks (Zuboff, 2019; Macgilchrist et al., 2024). Furthermore, digital platforms' reliance on engagement-driven algorithms disproportionately amplifies content that aligns with mainstream defense discourses, limiting exposure to feminist critiques (D'Ignazio & Klein, 2020). Digital platforms such as social media, search engines, and news aggregators employ algorithmic filters that structure access to security-related content, often reinforcing dominant military narratives at the expense of diverse perspectives (Zuboff, 2019; Crawford, 2021). As feminist scholars have argued, these digital mechanisms contribute to the epistemic exclusion of women and feminist security analysts from mainstream discussions on defense and national security (Sjoberg, 2010; Enloe, 2000). The politics of algorithmic curation thus play a decisive role in determining which security narratives gain legitimacy and which are relegated to the margins.

The representation of women in military and security discourses is historically shaped by binary constructions that oscillate between invisibility, victimhood, and exceptionalism (Cohn, 1987; Duncanson, 2013). Women in military communication are often positioned within protective or supportive roles rather than as active agents of security policy and defense strategy. The feminist critique of military communication emphasizes the need for inclusive narratives that recognize women's contributions beyond essentialist gender frames (Shepherd, 2008; Parashar, 2014). However, the personalization algorithms that curate digital security content frequently reinforce traditional security frameworks that center on masculinity, authority, and hierarchical power structures, leaving little room for feminist reinterpretations of security and defense (Bucher, 2018; Sjoberg & Gentry, 2007).

Beyond representation, algorithmic governance also affects the potential for digital activism within security communication (wessalowski et al., 2025). While feminist security studies have called for greater inclusion of gendered perspectives in national defense debates, digital infrastructure often constrains these efforts through structural biases embedded in algorithmically mediated information flows (D'Ignazio & Klein, 2020). Feminist activists engaging in digital security debates frequently encounter algorithmic suppression, content de-prioritization, or targeted disinformation campaigns that undermine feminist security advocacy (Crawford, 2021). Chowdhury and Lakshmi (2023) further document how AI-driven moderation and algorithmic suppression disproportionately impact feminist activism, as automated systems often fail to distinguish between advocacy and harmful content, leading to the unjust de-platforming of feminist voices. These barriers contribute to a broader crisis of representation in digital security spaces, where feminist critique struggles to gain algorithmic traction against dominant geopolitical narratives (Sjoberg, 2010; Whitworth, 2004).

The convergence of postdigital feminism, algorithmic visibility, and gendered security discourses underscores the need to examine how military communication is shaped in digital environments. This study situates its analysis within this broader intersection. It draws upon feminist security theory and algorithmic media studies to investigate how security discourses are curated, disseminated, and consumed by young women engaging with online defense narratives. In doing so, it contributes to the ongoing scholarly dialogue on the political economy of digital visibility and the structural conditions that shape feminist engagement with military communication (Macgilchrist et al., 2024).

METHODOLOGY

The main objective of this study is to examine how young women perceive algorithmic personalization as shaping the visibility of gendered perspectives in military and security communication, and how these perceptions relate to their engagement with security-related discourses on digital platforms. Rather than measuring algorithmic behavior directly, the study investigates perceived algorithmic influence: that is, how participants report encountering, interpreting, and responding to security-related content within social media environments they understand as algorithmically curated. Specifically, the research aims to examine: (1) how young women report encountering and interacting with security-related content on digital platforms; (2) how they perceive the visibility or marginalization of feminist perspectives within digital military and security communication; and (3) how institutional media trust and subjective algorithmic awareness vary across user segments.

Based on prior research, the study formulates two hypotheses:

H1: Participants will report encountering security-related narratives more frequently through social media feeds they perceive as algorithmically curated than through active information-seeking.

H2: Institutional media trust will be negatively associated with subjective algorithmic awareness across user segments.

Perceived algorithmic influence as the object of inquiry

This study does not claim to measure algorithmic behavior directly. Instead, it treats perceived algorithmic influence as the central empirical and theoretical object of inquiry. This distinction is crucial because platform algorithms are largely opaque to ordinary users, researchers, and even public institutions. In such conditions, users rarely know with certainty why a particular item appears in their feed, why some perspectives receive greater visibility, or why others appear marginal or absent. However, this uncertainty does not make user perceptions analytically irrelevant. On the contrary, perceived algorithmic logic shapes how users interpret digital environments, evaluate the legitimacy of information, and decide whether to speak, remain silent, search further, or disengage (Gombar & Boban, 2026).

This epistemological position also resonates with Haraway's (1988) account of situated knowledges, in which partial and embodied perspectives are not treated as methodological distortions but as legitimate standpoints from which knowledge is produced. In the context of opaque platform infrastructures, participants' accounts therefore matter not because they reveal algorithmic operations directly, but because they show how algorithmic visibility is lived, anticipated, and acted upon. Following Bucher's concept of the anticipated algorithm, the study approaches participants' accounts as evidence of how algorithmic systems are imagined, anticipated, and incorporated into everyday communicative behavior. A participant who believes that feminist security perspectives are less visible may adjust her own behavior accordingly, regardless of whether such suppression can be technically verified at the platform level. In this sense, perceived algorithmic influence has real communicative consequences: it shapes expectations, self-censorship, trust, resistance, and interpretative agency (Acar, 2025).

This approach is consistent with postdigital feminism, which understands digital infrastructures not as external technical systems but as embedded conditions of social, political, and epistemic life. The study examines how young women make sense of security-related content within environments they perceive as algorithmically curated. The survey captures reported exposure, subjective algorithmic awareness, institutional trust, and feminist engagement, rather than verified platform operations. This methodological choice strengthens rather than weakens the study, because it foregrounds the lived epistemic consequences of algorithmic opacity in gendered security communication.

This study employs a mixed-methods approach, integrating quantitative and qualitative analyses to explore how algorithmic personalization influences the visibility of women in military narratives and security communication. Hesse-Biber (2014) advocates for imaginative and creative research methodologies that transcend epistemic barriers and open new analytical perspectives. Kara (2015) provides a practical guide to using creative methodologies in the social sciences, reinforcing their applicability in feminist security research. This approach aligns with Back and Puwar's (2012) concept of *"live methods,"* which emphasizes the dynamic and performative aspects of social inquiry. Koro-Ljungberg (2016) critiques traditional qualitative research frameworks, advocating for more flexible and adaptive methodologies.

Grounded in postdigital feminist theory and digital activism, the research situates security perceptions within broader algorithmically mediated public discourses. This methodological approach aligns with feminist digital epistemologies (D'Ignazio & Klein, 2020), emphasizing the need to critically interrogate algorithmic governance and its impact on gendered knowledge production in security discourses. By incorporating a feminist digital epistemological lens, this study also considers how algorithmic filtering mechanisms shape the production and circulation of security knowledge in gendered ways (D'Ignazio & Klein, 2020; Noble, 2018). This approach recognizes that algorithmic bias is not merely a technological limitation but a structural issue that intersects with broader epistemic inequalities in security communication (Benjamin, 2019; Macgilchrist et al., 2024).

The study is based on an online survey conducted in December 2024 among 425 female university students in Croatia. A structured questionnaire was distributed through closed social media groups and direct peer-to-peer digital channels, targeting women aged 18–30 enrolled at public universities. The survey included closed- and open-ended questions assessing perceptions of security, algorithmic personalization, media trust, and feminist engagement with military narratives.

The survey instrument (Appendix A) was developed by the author, drawing on the conceptual frameworks of algorithmic awareness (Bucher, 2018), institutional media trust (Newman et al., 2023), and feminist digital engagement (D'Ignazio & Klein, 2020). The items were not treated as direct replications of validated scales; rather, they operationalised key constructs identified in the cited literature and were tested for internal consistency and exploratory construct validity in the present sample. The instrument consisted of 24 items in total, including 21 closed-ended statements and 3 open-ended questions. The closed-ended items were measured on a five-point Likert scale (1 = strongly disagree; 5 = strongly agree) and captured three main constructs: subjective algorithmic awareness, institutional media trust, and feminist engagement. Internal consistency was acceptable to good across the three composite scales: subjective algorithmic awareness ($\alpha = .82$), institutional media trust ($\alpha = .79$), and feminist engagement ($\alpha = .84$). These reliability values supported the use of composite scale scores in the subsequent correlational, exploratory factor, and cluster analyses.

The questionnaire examined how security narratives are algorithmically mediated and how female students engage with these topics in digital environments, focusing on trust in media, sources of security-related information, perceptions of global conflicts and geopolitical instability, awareness of algorithmic personalization in security communication, engagement with military and defense-related discourses, and future career aspirations in defense and security sectors. The dataset captures both passive algorithmic exposure and active engagement with security narratives, enabling a multi-layered analysis. The convenience sample of Croatian female university students limits generalisability; self-reports and the cross-sectional design capture associations rather than causal effects. To assess passive algorithmic exposure, the survey included items on the frequency of exposure to recommended security content, the perceived relevance of algorithmically suggested posts, and the retrospective recall of engaging with security narratives through automated content curation. This approach builds on previous methodologies for analyzing algorithmic content exposure (D'Ignazio & Klein, 2020) and adapts them to a survey-based framework for investigating user perceptions of algorithmic influence.

The quantitative analysis followed a multi-layered strategy, integrating descriptive statistics, exploratory factor analysis (EFA), hierarchical cluster analysis (HCA), and correlational testing. Descriptive statistics examined distribution trends in key security-related perceptions, media trust, and attitudes toward military engagement. An exploratory factor analysis using principal axis factoring with Varimax rotation was performed to identify latent dimensions underlying user perceptions. The Kaiser-Meyer-Olkin (KMO) measure verified sampling adequacy (KMO = .83), and Bartlett's test of sphericity was significant ($\chi^2 = 1650.22$, $p < .001$). The factor analysis yielded a three-factor structure that explained 61.4% of the total variance: (1) algorithmic awareness, (2) institutional media trust, and (3) feminist critical engagement. Based on factor scores, a hierarchical cluster analysis was conducted using Ward's method and squared Euclidean distance. The final agglomeration steps and dendrogram supported a four-cluster solution and are reported in Appendix B to document the basis for retaining this segmentation.

The resulting clusters were thematically interpreted and labeled as mainstream security consumers, critical analysts, neutral observers, and digital activists. These audience profiles offer a typology of female user engagement with algorithmically mediated military narratives. Pearson's correlation coefficients were calculated to explore associations between key variables. Statistically significant correlations (Appendix C) were observed between institutional media trust and alignment with dominant security narratives ($r = 0.51$, $p < .01$), and a significant negative correlation emerged between algorithmic awareness and institutional trust ($r = –0.46$, $p < .01$). These patterns suggest that algorithmic exposure and critical feminist engagement intersect with levels of trust in mainstream security discourses.

Beyond statistical classification, the study integrates postdigital feminist theory to critically examine the limitations of digital activism in military communication and the structural biases embedded in algorithmically mediated security discourses. This interdisciplinary approach ensures that the findings offer both empirical insights and broader theoretical reflections on the politics of algorithmic visibility in military communication.

Ethics statement

Participation in the study was voluntary and anonymous. Before completing the online questionnaire, participants were informed about the purpose of the study, the approximate duration of the survey, the type of data collected, and their right to discontinue participation at any point. No identifying personal data was collected, and responses were analyzed only in aggregated form. The study involved adult university students and did not include deception, intervention, or the collection of sensitive personal identifiers.

RESULTS

The findings from the survey of 425 female university students in Croatia illustrate how respondents perceive algorithmic personalization as shaping their exposure to security and military narratives. This study, employing descriptive statistical analysis and exploratory segmentation, identified key patterns in how female audiences engage with security-related discourses in digital environments. Descriptive analysis indicates that 72% of respondents primarily encounter security-related content through social media platforms, with respondents interpreting this exposure as shaped by algorithmic curation. Only 24% actively seek out security-related content, while the remaining 4% report minimal engagement with military or defense narratives. These findings suggest that respondents perceive algorithmically mediated exposure as outweighing deliberate engagement, supporting H1 as a claim about reported information behavior rather than verified platform behavior.

An exploratory segmentation analysis identified four key audience types based on their engagement with security discourses and trust in digital media ecosystems. Mainstream security consumers (38%) demonstrate high trust in institutional security sources and frequently engage with traditional security narratives, exhibiting limited awareness of algorithmic mediation. Critical analysts (22%) are skeptical of dominant security discourses,

actively question military narratives, and exhibit higher levels of algorithmic literacy. Neutral observers (27%) engage minimally with security topics, passively consuming algorithmically filtered content without critical awareness of its origins. Digital activists (13%) are highly engaged in online security debates, are critically aware of algorithmic influence, and often challenge dominant security frameworks.

These four audience profiles are summarized in **Table 1**, which presents a typology of algorithmically mediated security engagement among young women. This typology offers a novel framework for understanding how platform logics shape feminist visibility and interpretative agency within military and security communication.

Table 1

Typology of female users in algorithmically mediated security discourses

User Segment	Engagement with Security Discourses	Trust in Mainstream Media	Awareness of Algorithmic Personalization	Feminist Security Engagement
Mainstream Security Consumers	High engagement with institutional security narratives	High	Low	Minimal
Critical Analysts	Moderate-to-high engagement, with a critical stance toward dominant security narratives	Low	High	Moderate
Neutral Observers	Low engagement and mostly passive information consumption	Medium	Low	Minimal
Digital Activists	High engagement, often focused on counter-narrative or feminist security perspectives	Low	High	High

Note: The table summarizes the interpretative typology derived from cluster analysis. Statistical cluster profiles and cluster sizes are reported in Appendix D.

Further analysis of responses on trust in media and perceptions of security threats reveals distinct patterns across the identified audience types. Institutional media trust was positively associated with alignment with dominant security narratives ($r = .51$, $p < .01$). This pattern was most visible among mainstream security consumers and, to a lesser extent, neutral observers. In contrast, critical analysts and digital activists were characterized by lower institutional trust and higher subjective algorithmic awareness. This pattern is consistent with the negative correlation between subjective algorithmic awareness and institutional media trust ($r = -.46$, $p < .01$). These patterns reflect broader dynamics of algorithmic mediation, suggesting that trust in dominant security narratives is closely associated with users' levels of algorithmic exposure and critical engagement. Responses regarding awareness of algorithmic personalization further highlight key divergences. Only 29% of respondents reported that they understood how algorithmic curation affects their exposure to security content, while 46% acknowledge uncertainty about whether their digital environments selectively shape security narratives. The remaining 25% report being unaware of algorithmic influence on security communication. This distribution suggests a significant gap in digital literacy concerning how security narratives are filtered and amplified within platformed media environments (Gombar, 2025).

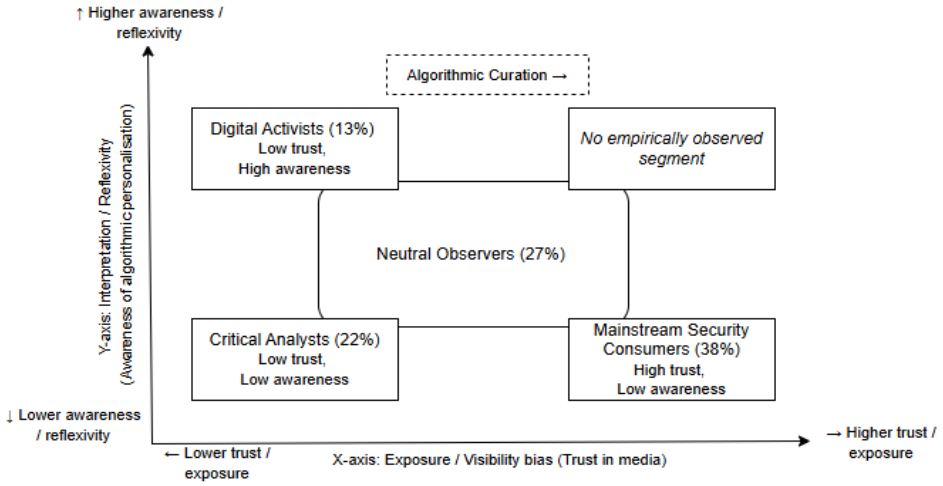
Open-ended responses provide additional qualitative insights into the limitations of feminist security perspectives in algorithmically mediated environments. Eskola (1988) similarly critiques how dominant epistemologies in social sciences often obstruct the development of alternative perspectives, limiting the possibility of integrating feminist critiques into mainstream security discourses. Several respondents noted that when they attempted to engage with feminist critiques of defense policies or alternative security discourses, they encountered reduced visibility of such content in their digital feeds. Others highlighted the prevalence of algorithmically amplified mainstream military narratives, reinforcing existing security paradigms while limiting exposure to critical perspectives. These qualitative findings align with prior research indicating that algorithmic bias in digital platforms prioritizes dominant geopolitical discourses while marginalizing alternative viewpoints (Noble, 2018).

These findings indicate that respondents perceive algorithmic personalization as substantially shaping their encounters with security-related discourses. The data do not verify platform-level algorithmic behavior directly; rather, they show how young women interpret, anticipate, and respond to algorithmically curated environments. The segmentation of respondents into distinct engagement profiles suggests that algorithmic mediation is not uniform but rather differentially structures access to security information based on prior engagement patterns,

trust in media, and critical awareness of algorithmic curation. These results provide a foundation for further discussion of the political and epistemic consequences of digital military communication, which will be explored in the following section. To illustrate these findings visually, **Figure 1** maps the differentiated impacts of algorithmic mediation across the four identified user segments, highlighting the intersection of media trust, algorithmic awareness, and feminist security engagement.

Figure 1

Algorithmic visibility model: user segments by trust, awareness, and interpretative reflexivity



Note: User segments are positioned by trust in mainstream media (X-axis; exposure/visibility bias) and awareness of algorithmic personalization (Y-axis; interpretative reflexivity). Algorithmic curation acts as a directional force increasing exposure along the X-axis. Percentages indicate indicative cluster proportions (N = 425).

As depicted in **Figure 1**, algorithmic mediation does not exert a uniform influence across the studied population. Instead, it reinforces pre-existing dispositions among mainstream security consumers and neutral observers, who tend to absorb content aligned with hegemonic defense narratives without questioning its algorithmic construction. In contrast, digital activists and critical analysts demonstrate resistant patterns of engagement, marked by heightened awareness of algorithmic influence and greater receptivity to feminist and counter-narrative perspectives. This differentiated structure of visibility and trust highlights the role of platform logic in shaping the epistemic architecture of digital security discourses. Rather than acting as neutral distributors, algorithms are perceived and theorized as infrastructures of power that may modulate what is seen, amplified, and left invisible. H1 is supported: a larger share of respondents encountered security narratives via algorithmic curation (72%) than through active seeking (24%). H2 is supported: trust in institutional media is negatively correlated with algorithmic awareness ($r = -0.46$, $p < .01$), consistent with the four-cluster segmentation.

As visualised in this model, the segmentation of user agency reveals how algorithmic environments selectively foster or suppress feminist perspectives based on media trust, digital literacy, and political engagement. These patterns support the theoretical interpretation that algorithmic personalization may operate as a political force determining the content and the contours of interpretative agency within militarized communication spaces (Bucher, 2018; Noble, 2018; D'Ignazio & Klein, 2020). Rather than offering a fixed typology, this model invites further thinking on how algorithmic infrastructures condition feminist agency in militarized digital spaces. The proposed model in **Figure 1** represents an original analytical contribution, developed from the empirical and theoretical architecture of this study. It offers a postdigital feminist lens for understanding stratified user positioning within algorithmically curated security discourses. It invites further interrogation of digital infrastructures as sites of epistemic violence and feminist resistance (Gupta, 2026). In viewing algorithmic personalization as a vector of epistemic power, this model demands that feminist theory reconceptualise visibility not as a given but as a digitally contested terrain.

DISCUSSION

Algorithmic visibility and the gendered curation of security discourses

The findings of this study align with previous research on algorithmic personalization by showing that respondents primarily interpret their encounters with security-related content as shaped by algorithmic recommendation systems rather than by active information seeking. Gergen (2015) argues that research should not merely reflect the world but actively participate in its transformation, an idea that resonates with feminist interventions in algorithmic governance and security discourses. Evans and Riley (2023) emphasize the emotional

and affective dimensions of digital environments, suggesting that the experience of algorithmic curation is not only cognitive but deeply intertwined with affective responses to security narratives. Seventy-two percent of respondents reported encountering security narratives primarily through social media feeds they perceived as algorithmically curated, underscoring the importance of perceived and anticipated visibility in digital security communication (Zuboff, 2019; Crawford, 2021). This pattern reinforces concerns about the epistemic exclusion of critical and feminist security perspectives, which struggle to gain traction within algorithmic systems designed to amplify dominant geopolitical and military narratives (Sjoberg & Gentry, 2007; Shepherd, 2008). Previous research has demonstrated that algorithmic curation can create ideological silos, limiting users' exposure to diverse perspectives in security debates (Macgilchrist et al., 2024). Crawford (2021) highlights how automated moderation systems disproportionately filter feminist and critical security perspectives, reinforcing dominant geopolitical narratives. Zuboff's (2019) work on surveillance capitalism further underscores how data-driven infrastructures prioritize engagement-maximizing content over epistemic diversity, exacerbating the invisibility of marginalized voices in security discourse.

One participant reflected on how security-related content appears in her feed:

"I usually see security-related content through recommendations rather than actively searching for it. The algorithm constantly suggests military reports and analyses, even when I am not interested" (Female student, 23)

This observation aligns with existing research on algorithmic personalization, which indicates that security discourse is shaped more by platform curation than user intent (Bucher, 2018; Noble, 2018). As a result, feminist and critical security perspectives struggle to gain algorithmic visibility, reinforcing dominant geopolitical narratives (Sjoberg & Gentry, 2007; Shepherd, 2008).

Another respondent expressed frustration with the reach of feminist security perspectives on social media:

"Whenever I try to share a feminist view on the military or security, my posts get significantly less engagement. It seems like the algorithm prioritizes mainstream military narratives" (Female student, 22)

These finding echoes Banet-Weiser's notion of platform feminism, in which digital spaces offer visibility while also constraining feminist discourse within patriarchal platform structures. In this study, respondents identifying with more activist and critical profiles reported lower perceived visibility of alternative security perspectives, suggesting a perceived asymmetry of visibility rather than directly verified algorithmic suppression.

Moreover, participants showed varying levels of trust in algorithmically curated security content. One student, for instance, admitted:

"I have no idea why I keep seeing military and security news all the time, but I assume it is because my friends engage with it" (Female student, 19)

This statement reflects broader concerns about algorithmic transparency and digital literacy, as only 29% of respondents were aware of how security-related content is filtered on digital platforms (D'Ignazio & Klein, 2020; Bucher, 2018).

Finally, one participant articulated the difficulty of finding feminist security analyses in algorithmically dominated spaces:

"I would love to see more critical security analyses on social media, but algorithms do not seem to support that kind of content" (Female student, 21)

These reflections highlight the structural barriers that feminist security perspectives face within military-affiliated digital ecosystems.

This calls for further research into how digital infrastructures can be reconfigured to promote epistemic diversity in security discourses. Specifically, future studies could employ algorithmic audits (Sandvig et al., 2014) to examine the extent to which feminist narratives are deprioritized within digital security ecosystems. Moreover, interdisciplinary collaborations between feminist scholars, data scientists, and policymakers are essential to developing more transparent and equitable content moderation strategies (D'Ignazio & Klein, 2020). This research also underscores the need for regulatory frameworks that enforce algorithmic accountability, ensuring that marginalized perspectives in security discourse receive adequate visibility (Noble, 2018). These dynamics further highlight how algorithmic infrastructures entrench epistemic asymmetries within digital security ecosystems.

Similar studies on gendered algorithmic bias suggest that digital platforms prioritize authoritative, state-backed security narratives while deprioritizing dissenting or critical voices (D'Ignazio & Klein, 2020; Gillespie, 2018). These results indicate that mainstream security consumers place greater trust in military institutions and are more likely to engage with algorithmically promoted content ($r = 0.51$, $p < 0.01$). At the same time, critical analysts and digital activists experience algorithmic barriers to accessing alternative perspectives ($r = -0.46$, $p < 0.01$). These findings align with previous studies indicating that feminist critiques of security policy remain marginalized within digital security ecosystems due to algorithmic gatekeeping mechanisms (Noble, 2018; Enloe,

2000). This raises concerns about the broader implications of algorithmic visibility on security perceptions, as digital platforms function as passive mediators and active security actors that govern access to information (Zuboff, 2019). Benjamin (2019) examines how digital infrastructures encode racial and gendered exclusions, reinforcing structural inequalities in knowledge production and digital visibility. The logic of data colonialism embedded in algorithmic governance reinforces hegemonic defense discourses, shaping what is perceived as a legitimate security concern and what remains excluded from mainstream debates. Bloch (1986) introduces the concept of the 'principle of hope,' emphasizing the potential for alternative imaginaries to emerge despite structural constraints, which aligns with feminist security activism seeking to challenge dominant narratives.

Structural constraints on feminist digital activism in military communication

Beyond algorithmic curation, the structural limitations of feminist engagement with security discourses highlight deeper issues of platform governance, digital surveillance, and content moderation policies (Broussard, 2018). The segmentation analysis suggests that respondents in the digital activist profile report lower perceived visibility of feminist and alternative security perspectives, alongside lower institutional trust and higher subjective algorithmic awareness. This should be interpreted as a pattern of perceived visibility asymmetry rather than as direct evidence of verified algorithmic suppression. This echoes findings from research on platformed resistance movements, in which alternative viewpoints are often categorized as "low-engagement" content and deprioritized in algorithmic ranking systems (Zuboff, 2019; Crawford, 2021). Studies on gendered censorship in digital activism suggest that feminist critiques of militarization and national security frameworks are often algorithmically sidelined (Sjoberg, 2010; Shepherd, 2008).

Feminist resistance within digital security narratives requires strategies beyond institutional engagement and the embrace of direct action. Graeber (2009) conceptualizes direct action as a means of bypassing institutional barriers and challenging dominant power structures, offering an alternative framework for feminist resistance in digital security spaces. Within algorithmically mediated security discourses, feminist activists often employ direct-action tactics, such as disruptive online interventions, decentralized information sharing, and counter-hegemonic storytelling, to resist the marginalization of gendered perspectives in defense communication. Participants' accounts suggest that such actions may be experienced as being met with reduced algorithmic visibility or limited circulation. This pattern underscores the need to critically examine how digital infrastructures condition the visibility and effectiveness of feminist interventions in security discourses.

These findings support this argument, as multiple respondents noted that attempts to engage with feminist security perspectives resulted in reduced visibility or algorithmically driven counter-narratives that reinforced dominant security discourses. These patterns exemplify what Banet-Weiser (2018) describes as the paradox of platform feminism, where digital spaces simultaneously offer new opportunities for visibility while embedding feminist discourse within structures that sustain platform patriarchy. Hunt and Rygiel (2006) analyze how war and security policies are constructed through gendered narratives, reinforcing hierarchical power structures in military communication. As a result, the infrastructures that enable feminist security engagement also to function as regulatory mechanisms that condition their reach, positioning feminist interventions as algorithmically peripheral within digital security debates. This aligns with digital militarization, where platformed security narratives operate within hegemonic geopolitical frameworks that reinforce masculinized, state-centered interpretations of defense and security (Duncanson, 2013; Whitworth, 2004).

To visually illustrate these dynamics, **Figure 2** presents a conceptual model of the perceived and theorized pathways through which feminist security narratives may become less visible within platform infrastructures.

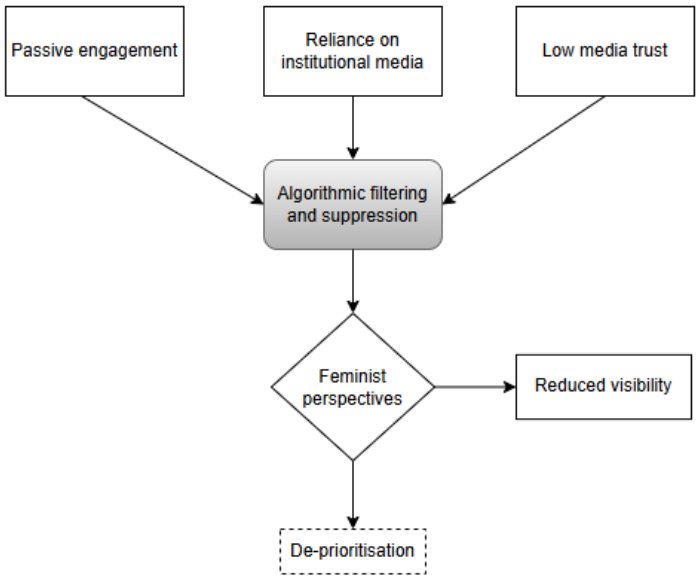
While statistical analysis reveals the segmented patterns of trust, awareness, and feminist engagement across user types, the structural mechanics behind such asymmetries remain primarily invisible within traditional metrics. To address this gap, **Figure 2** offers a conceptual flowchart that maps the pathways through which algorithmic infrastructures filter, suppress, or amplify feminist security narratives in digital environments. These mechanisms are rarely neutral. As shown in the model, initial user behaviors—such as passive engagement or reliance on institutional media—are algorithmically recorded, weighted, and recursively fed into content curation systems. Feminist perspectives, particularly those critical of military institutions or national security policies, may be perceived by users as receiving lower visibility within ranking systems designed to maximize engagement and user retention (Zuboff, 2019; Gillespie, 2018). Platform partnerships with state or defense actors may further exacerbate this filtering effect, embedding content moderation within geopolitical and ideological interests (Crawford, 2021).

This diagram also includes feedback loops that illustrate how perceived or theorized algorithmic suppression of feminist perspectives may limit their visibility and recalibrate the platform's perception of what is relevant, thus recursively marginalising critical voices. Suzor (2019) argues that platform governance must be rethought through participatory design that centres accountability and equity in algorithmic infrastructures. In visualising

these pathways, the figure contributes to the ongoing effort to expose algorithmic opacity and advocate for epistemic justice in digital security communication.

Figure 2

Pathways of algorithmic filtering of feminist security narratives



Source: Elaborated by the authors from empirical patterns and platform critique literature

The politics of digital trust: Navigating algorithmic bias in security perceptions

One of the most striking findings of this study is the significant variation in trust in security-related information across algorithmic exposure patterns. These results indicate that participants with high institutional trust exhibited greater algorithmic exposure to traditional security narratives, while those with low institutional trust engaged more with critical and feminist perspectives. This supports previous research on the reinforcement of ideological silos within algorithmically mediated environments (Macgilchrist et al., 2024).

The low awareness among respondents of algorithmic influence on security discourses (only 29% demonstrated a clear understanding of how security content is filtered) suggests a broader crisis in algorithmic transparency and digital literacy (D'Ignazio & Klein, 2020). These findings highlight the need for critical algorithmic literacy initiatives that equip users—particularly those engaging with military and security topics—with the skills to navigate algorithmic curation biases and actively seek diverse security perspectives.

Limitations

Several limitations should be acknowledged. First, the study is based on a convenience sample of female university students in Croatia, which limits the generalisability of the findings to broader populations, age groups, or national contexts. Second, the survey captures self-reported perceptions of algorithmic curation rather than verified platform-level algorithmic behavior. The findings therefore support claims about perceived and anticipated algorithmic influence, not direct causal claims about algorithmic suppression. Third, the cross-sectional design captures associations between subjective algorithmic awareness, institutional media trust, and feminist engagement, but it cannot establish temporal or causal relationships. Finally, although the open-ended responses provide interpretive depth, they should be understood as illustrative accounts rather than exhaustive qualitative evidence of platform governance mechanisms.

Implications for future research and policy recommendations

The findings of this study contribute to ongoing debates on the politics of digital visibility, feminist security studies, and algorithmic governance. By showing that respondents perceive algorithmic personalization as structuring their encounters with military and security communication, this research underscores the urgent need for digital policy interventions that promote epistemic diversity in security discourses (Costello et al., 2025).

Future research should explore the intersection of digital security infrastructures and feminist engagement, particularly in platform regulation and algorithmic auditing (Lindberg & Johansson, 2023; Ross, 2023). Future interdisciplinary studies should prioritize empirical testing of algorithmic biases to ensure that security

communication platforms foster multiple perspectives rather than reinforce dominant geopolitical narratives (Macgilchrist et al., 2024). Additionally, examining perceived and platform-level forms of algorithmic suppression in security-related digital activism through in-depth qualitative methodologies could provide deeper insights into the lived experiences of feminist security analysts and activists. From a policy perspective, platform transparency measures and algorithmic accountability frameworks must be implemented to counteract the exclusion of critical perspectives from security communication ecosystems (Noble, 2018; D'Ignazio & Klein, 2020). Initiatives that integrate feminist security critiques into mainstream military communication channels could help challenge the structural biases embedded in algorithmically governed security narratives (Shepherd, 2008; Sjoberg, 2010).

These findings support the theoretical argument that algorithmic infrastructures are experienced and interpreted not as neutral filters but as active epistemic agents—shaping what is seen, amplified, or excluded in digital security discourses. Within such architectures of power, postdigital feminist research must continue to interrogate the unseen protocols that govern visibility and legitimacy. Therefore, this study lays the groundwork for emancipatory engagements that challenge algorithmic marginalization and reposition interpretative agency within militarized communication environments—inviting policy reconfiguration and scholarly reimagination.

CONCLUSION

This study explored how female university students perceive the algorithmic shaping of women's visibility in military and security communication through the lens of postdigital feminism. Drawing on survey data from 425 female university students in Croatia, the findings show that respondents understand their exposure to security narratives as being shaped by algorithmic personalization, while feminist critiques are perceived as less visible within their digital feeds. The segmentation of users into four distinct profiles—from mainstream security consumers to digital activists—reveals a stratified field of algorithmic engagement. While some respondents absorbed militarized narratives passively, others challenged them with critical feminist perspectives, often reporting reduced visibility or limited circulation of feminist security perspectives. This differentiated landscape underscores how algorithms are perceived and anticipated as technical systems and epistemic actors.

By situating algorithmic infrastructures as political actors, this study contributes to ongoing debates on digital governance, feminist security, and the politics of visibility. It calls for critical algorithmic literacy, platform accountability, and policy frameworks safeguarding epistemic diversity in militarized communication. Future research should employ methodologies such as algorithmic ethnography to trace how feminist security discourses are curated—or erased—by platform logics.[1] Longitudinal studies may reveal how algorithmic architectures evolve, offering insight into possible sites of resistance and intervention. An interdisciplinary approach, integrating feminist theory, critical algorithm studies, and security research, is essential to reimagine digital infrastructures that include rather than exclude. For feminist media scholarship, this means treating algorithmic visibility itself as a contested site of security politics, where struggles over representation, affect, and credibility is inseparable from struggles over militarism.

Finally, this work affirms the role of postdigital feminist scholarship in interrogating the infrastructures that regulate interpretative agency in digital security environments. As Hurley (2023) notes, postdigital feminists must learn to navigate the contradictions of visibility: seizing digital presence while resisting its algorithmic containment. In doing so, they not only challenge platformed militarism but also open pathways toward more democratic, inclusive, and epistemically just security futures.

Acknowledgement

The authors have no acknowledgments to declare.

Funding

This research received no external funding.

Ethical statement

Participation in the study was voluntary and anonymous. All participants were adults and provided informed consent before taking part. No directly identifiable or sensitive personal data was collected. As the study was non-interventional and involved an anonymous survey of adult participants, formal ethical approval was not required under the applicable national requirements.

[1] Particular attention should be given to post-socialist and NATO-aligned countries in Southeastern Europe, where the entanglement of transitional governance, digital platform logic, and security communication remains underexplored.

Competing interests

The authors declare that they have no competing interests.

Author contributions

Both authors contributed to the conceptualization and design of the study, interpretation of the findings, and preparation of the manuscript. Marija Gombar conducted the formal analysis and prepared the original draft. Maja Križanec Cvitković contributed to the interpretation of the results and critical review of the manuscript. Both authors read and approved the final version of the manuscript.

Data availability

The data supporting the findings of this study are available from the corresponding author upon reasonable request.

AI disclosure

The authors used Grammarly solely for proofreading, grammar correction, and language refinement during the final preparation of the manuscript. No generative AI tools were used to conduct the research, analyse the data, interpret the findings, or generate the substantive scientific content. The authors reviewed and approved the final manuscript and take full responsibility for its content.

Biographical sketch

Marija Gombar is a Ph.D. candidate in Media and Communication at University North and a Lieutenant Colonel serving in the Armed Forces of the Republic of Croatia. She is the author of three scientific monographs and numerous research papers. Her research interests include digital resilience, digital citizenship, algorithmic governance, digital trust, cybersecurity communication, strategic communication, and security-related digital behaviour. Her work examines digital responsibility, algorithmic awareness, and communication processes in contemporary security environments.

Maja Križanec Cvitković is a Ph.D. candidate in Media and Communication at University North and a religious education teacher at a secondary school in Croatia. Her professional and research interests focus on artificial intelligence and the social dimension of information and communication sciences. She is particularly interested in the intersections of education, digital technologies, communication processes, and the social implications of emerging technological developments. Her work explores how contemporary digital environments shape understanding, values, and human interaction in educational and social contexts.

Disclaimer/Publisher's Note

REFERENCES

Acar, E. (2025). From welcome to surveillance: Intersecting experiences of visibility and vulnerability among international students in the United States. *European Journal of Education & Language Review, 1*(1), Article 3. https://doi.org/10.20897/ejelr/17571

Appadurai, A. (2000). Grassroots globalization and the research imagination. *Public Culture, 12*(1), 1–19. https://doi.org/10.1215/08992363-12-1-1

Atkins, L. C., & Grant, S. B. (2022). Diverse applications of sociological imagination: A qualitative study of service-learning mentoring. *Journal of Applied Social Science, 16*(1), 328–345. https://doi.org/10.1177/19367244211021390

Back, L., & Puwar, N. (Eds.). (2012). *Live methods*. Wiley-Blackwell.

Banet-Weiser, S. (2018). *Empowered: Popular feminism and popular misogyny*. Duke University Press. https://doi.org/10.1215/9781478002772

Barnetz, Z. (2015). The role of radical imagination in social work education, practice, and research. *Journal of Teaching in Social Work, 35*(3), 251–261. https://doi.org/10.1080/08841233.2015.1028607

Bassett, C. (2015). Not now? Feminism, technology, postdigital. In D. M. Berry & M. Dieter (Eds.), *Postdigital aesthetics: Art, computation and design* (pp. 136–150). Palgrave Macmillan. https://doi.org/10.1057/9781137437204_11

Benjamin, R. (2019). *Race after technology: Abolitionist tools for the New Jim Code.* Polity Press.

Bloch, E. (1986). *The principle of hope* (N. Plaice, S. Plaice, & P. Knight, Trans.; Vol. 1). MIT Press. (Original work published 1959)

Broussard, M. (2018). *Artificial unintelligence: How computers misunderstand the world.* MIT Press.

Buch, A., Lindberg, Y., & Cerratto Pargman, T. (Eds.). (2024). *Framing futures in postdigital education: Critical concepts for data-driven practices.* Springer. https://doi.org/10.1007/978-3-031-58622-4

Bucher, T. (2018). *If...then: Algorithmic power and politics.* Oxford University Press. https://doi.org/10.1093/oso/9780190493028.001.0001

Castoriadis, C. (1987). *The imaginary institution of society* (K. Blamey, Trans.). Polity Press. (Original work published 1975)

Chowdhury, R., & Lakshmi, D. (2023). *"Your opinion doesn't matter, anyway": Exposing technology-facilitated gender-based violence in an era of generative AI.* UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000387483

Cohn, C. (1987). Sex and death in the rational world of defense intellectuals. *Signs: Journal of Women in Culture and Society, 12*(4), 687–718. https://doi.org/10.1086/494362

Costello, E., McDonald, J., Macgilchrist, F., Jandrić, P., Carbonel, H., Crighton, S., Buch, A., & Peters, M. A. (2025). Speculative practicescapes of learning design and dreaming. *Postdigital Science and Education, 7*(2), 560–588. https://doi.org/10.1007/s42438-024-00465-5

Crawford, K. (2021). *Atlas of AI: Power, politics, and the planetary costs of artificial intelligence.* Yale University Press.

D'Ignazio, C., & Klein, L. F. (2020). *Data feminism.* MIT Press. https://doi.org/10.7551/mitpress/11805.001.0001

Duncanson, C. (2013). *Forces for good? Military masculinities and peacebuilding in Afghanistan and Iraq.* Palgrave Macmillan.

Eichler, M. (2012). *Militarizing men: Gender, conscription, and war in post-Soviet Russia.* Stanford University Press.

Enloe, C. (2000). *Maneuvers: The international politics of militarizing women's lives.* University of California Press.

Eskola, A. (1988). *Blind alleys in social psychology.* North-Holland.

Evans, A., & Riley, S. (2023). *Digital feeling.* Palgrave Macmillan. https://doi.org/10.1007/978-3-031-23562-7

Gergen, K. J. (2015). From mirroring to world-making: Research as future forming. *Journal for the Theory of Social Behaviour, 45*(3), 287–310. https://doi.org/10.1111/jtsb.12075

Gillespie, T. (2018). *Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media.* Yale University Press.

Gombar, M. (2025). The paradox of trust in digital platforms: Algorithmic awareness in digital interactions. Revija za sociologiju, 55(2), 121–144. https://doi.org/10.5613/rzs.55.2.2

Gombar, M., & Boban, M. (2026). Algorithmic awareness and digital responsibility: The role of platform trust and digital literacy. Business Systems Research, 17(1), 179–203. https://doi.org/10.2478/bsrj-2026-0009

Graeber, D. (2009). *Direct action.* AK Press.

Gupta, A. (2026). Bodies under scanner: AI, surveillance, and gendered resistance in Manjula Padmanabhan's Harvest. *Journal of Interdisciplinary Research in Artificial Intelligence and Society, 2*(1), Article 2. https://doi.org/10.20897/jirais/18487

Haiven, M., & Khasnabish, A. (2014). *The radical imagination: Social movement research in the age of austerity.* Zed Books.

Haraway, D. (1988). Situated knowledges: The science question in feminism and the privilege of partial perspective. *Feminist Studies, 14*(3), 575–599. https://doi.org/10.2307/3178066

Hesse-Biber, S. N. (Ed.). (2014). *Feminist research practice: A primer* (2nd ed.). SAGE Publications. https://doi.org/10.4135/9781071909911

Hrastinski, S., & Jandrić, P. (2023). Imagining education futures: Researchers as fiction authors. *Postdigital Science and Education, 5*(3), 509–515. https://doi.org/10.1007/s42438-023-00403-x

Hunt, K., & Rygiel, K. (Eds.). (2006). *(En)gendering the War on Terror: War stories and camouflaged politics.* Ashgate.

Hurley, Z. (2023). Postdigital feminism(s). In P. Jandrić (Ed.), *Encyclopedia of postdigital science and education.* Springer. https://doi.org/10.1007/978-3-031-35469-4_42-1

Jacobsen, M., Drake, M., & Petersen, A. (Eds.). (2016). *Imaginative methodologies in the social sciences: Creativity, poetics, and rhetoric in social research.* Routledge.

Jandrić, P., Knox, J., Besley, T., Ryberg, T., Suoranta, J., & Hayes, S. (2018). Postdigital science and education. *Educational Philosophy and Theory, 50*(10), 893–899. https://doi.org/10.1080/00131857.2018.1454000

Jandrić, P., Luke, T. W., Sturm, S., McLaren, P., Jackson, L., MacKenzie, A., Tesar, M., Stewart, G. T., Roberts, P., Abegglen, S., Burns, T., Sinfield, S., Jaldemark, J., Peters, M. A., Sinclair, C., & Gibbons, A. (2023).

Collective writing: The continuous struggle for meaning-making. *Postdigital Science and Education, 5*(3), 851–893. https://doi.org/10.1007/s42438-022-00320-5

Jandrić, P., Tolbert, S., Hayes, S., & Jopling, M. (2025). Postdigital citizen science: Mapping the field. *Postdigital Science and Education, 7*(1), 9–30. https://doi.org/10.1007/s42438-023-00443-3

Kara, H. (2015). *Creative research methods in the social sciences: A practical guide.* Policy Press. https://doi.org/10.51952/9781447320258

Kind, A. (Ed.). (2016). *The Routledge handbook of philosophy of imagination.* Routledge.

Koro-Ljungberg, M. (2016). *Reconceptualizing qualitative research: Methodologies without methodology.* SAGE. https://doi.org/10.4135/9781071802793

Levy, A., & Godfrey-Smith, P. (Eds.). (2020). *The scientific imagination: Philosophical and psychological perspectives.* Oxford University Press. https://doi.org/10.1093/oso/9780190212308.001.0001

Lindberg, Y., & Johansson, S. (2023). Postdigital educational futures. In P. Jandrić (Ed.), *Encyclopedia of postdigital science and education.* Springer. https://doi.org/10.1007/978-3-031-35469-4_39-1

Macgilchrist, F., Jarke, J., Allert, H., & Cerratto Pargman, T. (2024). Design beyond design thinking: Designing postdigital futures when weaving worlds with others. *Postdigital Science and Education, 6*(1), 1–12. https://doi.org/10.1007/s42438-023-00447-z

Mills, C. W. (2000). *The sociological imagination.* Oxford University Press. (Original work published 1959)

Newman, N., Fletcher, R., Eddy, K., Robertson, C. T., & Nielsen, R. K. (2023). *Digital news report 2023.* Reuters Institute for the Study of Journalism. https://doi.org/10.60625/risj-p6es-hb13

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism.* NYU Press.

Oyewole, O. (2026). Media literacy and peer collaboration as predictors of civic engagement among pre-service teachers in Oyo State. *Asia Pacific Journal of Education and Society, 14*(1), Article 8. https://doi.org/10.20897/apjes/18502

Palmer, N. (2023). The sociological imagination within teaching sociology: 1973–2020. *Teaching Sociology, 51*(1), 1–12. https://doi.org/10.1177/0092055X221098452

Parashar, S. (2014). *Women and militant wars: The politics of injury.* Routledge.

Raza, F. A., Singh, A. D., Anwar, R., Kovilpillai, J. J. S., Hamdan, A. B., Konno, F., Rajaratnam, V., Raman, M., & Razami, H. H. (2026). Gender and functional differentiation in generative AI usage among Malaysian higher education student. *European Journal of STEM Education, 11*(1), Article 17. https://doi.org/10.20897/ejsteme/18267

Rohrer, I., & Thompson, M. (2023). Imagination theory: Anthropological perspectives. *Anthropological Theory, 23*(2), 186–208. https://doi.org/10.1177/14634996221129117

Ross, J. (2022). *Digital futures for learning: Speculative methods and pedagogies.* Routledge.

Ross, J. (2023). Postdigital speculation. In P. Jandrić (Ed.), *Encyclopedia of postdigital science and education.* Springer. https://doi.org/10.1007/978-3-031-35469-4_19-1

Sandvig, C., Hamilton, K., Karahalios, K., & Langbort, C. (2014, May 22). *Auditing algorithms: Research methods for detecting discrimination on internet platforms* [Paper presentation]. Data and Discrimination: Converting Critical Concerns into Productive Inquiry, Seattle, WA, United States.

Shepherd, L. J. (2008). *Gender, violence, and security: Discourse as practice.* Zed Books.

Sjoberg, L. (2010). Women fighters and the "beautiful soul" narrative. *International Review of the Red Cross, 92*(877), 53–68. https://doi.org/10.1017/S1816383110000027

Sjoberg, L., & Gentry, C. E. (2007). *Mothers, monsters, whores: Women's violence in global politics.* Zed Books.

Suoranta, J., Teräs, M., Teräs, H., Jandrić, P., Ledger, S., Macgilchrist, F., & Prinsloo, P. (2022). Speculative social science fiction of digitalization in higher education: From what is to what could be. *Postdigital Science and Education, 4*(2), 224–236. https://doi.org/10.1007/s42438-021-00260-6

Suzor, N. (2019). *Lawless: The secret rules that govern our digital lives.* Cambridge University Press. https://doi.org/10.1017/9781108612068

wessalowski, N., Lange, G. M., & Kannengießer, S. (2025). A feminist critique of cybersecurity: Technofeminist imaginaries of vulnerability and care. *Feminist Encounters: A Journal of Critical Studies in Culture and Politics, 9*(2), Article 25. https://doi.org/10.20897/femenc/16783

Whitworth, S. (2004). *Men, militarism, and UN peacekeeping: A gendered analysis.* Lynne Rienner Publishers.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* PublicAffairs.

APPENDICES

Appendix A

Survey Instrument

All closed-ended items were measured on a five-point Likert scale, where 1 = strongly disagree and 5 = strongly agree. The instrument included 21 closed-ended items and 3 open-ended questions. The closed-ended items measured three constructs: subjective algorithmic awareness, institutional media trust, and feminist engagement. The open-ended questions explored participants' interpretations of algorithmically mediated security communication.

Code	Item	Source	Scale	Notes
AA1	Algoritmi društvenih mreža određuju koji sigurnosni sadržaj vidim.	Bucher (2018)	1–5 Likert	
AA2	Moje preporuke za teme rata/obrane temelje se na mojoj prošloj interakciji, primjerice klikovima, zadržavanju na objavama ili dijeljenjima.	Bucher (2018)	1–5 Likert	
AA3	Mogu prepoznati kada je sadržaj o sigurnosti došao putem algoritamskih preporuka.	Bucher (2018)	1–5 Likert	
AA4	Platforme favoriziraju mainstream, državne ili institucionalne izvore u sigurnosnim vijestima.	AUT	1–5 Likert	
AA5	Kritičke ili feminističke perspektive imaju manju vidljivost zbog algoritamskog rangiranja.	D'Ignazio & Klein (2020)	1–5 Likert	
AA6	Ako ne interagiram aktivno, algoritam mi i dalje servira sigurnosne narative.	Bucher (2018)	1–5 Likert	
AA7	Preporučeni sadržaj često sužava raspon perspektiva koje vidim o sigurnosti.	Bucher (2018)	1–5 Likert	
AA8	Znam gdje na platformi mogu podesiti personalizaciju sadržaja.	Bucher (2018)	1–5 Likert	Procedural awareness
IMT1	Vjerujem nacionalnim televizijskim i portalnim vijestima pri izvještavanju o sigurnosti/obrani.	Newman et al. (2023)	1–5 Likert	
IMT2	Vjerujem međunarodnim mainstream medijima, primjerice BBC-u ili Reutersu, o sigurnosnim temama.	Newman et al. (2023)	1–5 Likert	
IMT3	Vjerujem informacijama koje dijele službene institucije, primjerice vlada, vojska ili policija, na društvenim mrežama.	Newman et al. (2023)	1–5 Likert	
IMT4	Smjernice i priopćenja ministarstava ili vojske smatram pouzdanim izvorom.	Newman et al. (2023)	1–5 Likert	
IMT5	Vijesti s nezavisnih ili fact-checking portala smatram pouzdanijima od društvenih mreža.	Newman et al. (2023)	1–5 Likert	
IMT6	Ne vjerujem informacijama o sigurnosti koje se šire preko influencera.	Newman et al. (2023)	1–5 Likert	Reverse-coded
IMT7	Općenito, moje je povjerenje u medije visoko kada prate vojne ili sigurnosne teme.	Newman et al. (2023)	1–5 Likert	
FE1	Aktivno pretražujem feminističke ili kritičke analize sigurnosnih tema.	D'Ignazio & Klein (2020)	1–5 Likert	
FE2	Spremna sam javno komentirati ili dijeliti feminističke perspektive o ratu/obrani.	D'Ignazio & Klein (2020)	1–5 Likert	
FE3	Smatram važnim da se rodna dimenzija uključi u vojne/sigurnosne rasprave.	D'Ignazio & Klein (2020)	1–5 Likert	
FE4	Algoritamska pristranost umanjuje vidljivost feminističkih glasova u sigurnosti.	D'Ignazio & Klein (2020)	1–5 Likert	
FE5	Sudjelujem u online akcijama, primjerice peticijama ili kampanjama, koje traže rodnu pravednost u sigurnosnim politikama.	AUT	1–5 Likert	
FE6	Kada su feminističke objave slabije vidljive, pokušavam ih pojačati putem likea, dijeljenja ili komentara.	AUT	1–5 Likert	
O1	Opišite nedavni primjer kada ste primile sigurnosni ili militarizirani sadržaj koji niste tražile. Kako ste ga interpretirale?	Bucher (2018) / AUT	Open-ended	

Code	Item	Source	Scale	Notes
O2	Imate li iskustvo da je feministička perspektiva bila slabije vidljiva ili uklonjena? Što mislite zašto?	D'Ignazio & Klein (2020) / AUT	Open-ended	
O3	Što po vama platforme trebaju promijeniti kako bi osigurale pravedniju vidljivost različitih perspektiva o sigurnosti?	AUT	Open-ended	

Note: Items are presented in the original Croatian-language version administered to participants. AA = subjective algorithmic awareness; IMT = institutional media trust; FE = feminist engagement. IMT6 was reverse-coded so that higher composite IMT scores consistently indicate higher institutional media trust. AUT indicates author-developed items based on the conceptual framework of the study.
Source: Authors' instrument based on the cited sources and the conceptual framework.

Appendix B

Hierarchical Cluster Analysis Diagnostics

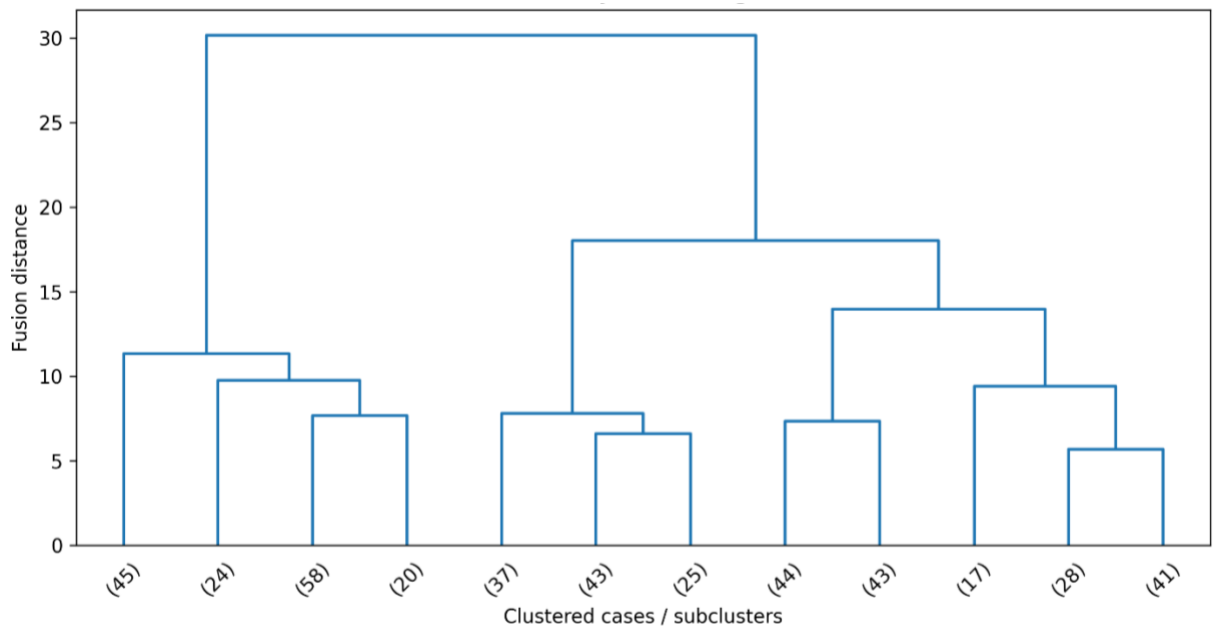
The four-cluster solution was selected after inspection of the dendrogram and the final steps of the agglomeration schedule. The solution was retained because the transition from four to three clusters produced a noticeable increase in fusion distance, indicating that further merging would reduce the substantive differentiation between user profiles.

Final Agglomeration Steps

Step	Number of clusters after fusion	Fusion distance	Interpretation
420	5	9.75	Competing five-cluster solution
421	4	11.32	Retained four-cluster solution
422	3	13.98	Marked increase; loss of substantive differentiation
423	2	18.02	Over-aggregation of distinct user profiles
424	1	30.16	Complete aggregation of all cases

Note: Hierarchical cluster analysis was conducted using Ward's method and squared Euclidean distance on standardized scores for subjective algorithmic awareness, institutional media trust, and feminist engagement. Inspection of the final agglomeration steps supported a four-cluster solution because subsequent fusion steps produced substantially larger increases in fusion distance.
Source: Authors' analysis.

Dendrogram of the Hierarchical Cluster Analysis



Note: The dendrogram illustrates the hierarchical clustering structure based on standardized scores for subjective algorithmic awareness, institutional media trust, and feminist engagement. The four-cluster solution was retained because it provided the most interpretable segmentation before larger increases in fusion distance occurred.
Source: Authors' analysis.

Appendix C

Descriptive Statistics and Correlations

Variable	Mean	SD	α	1	2	3
1. Subjective Algorithmic Awareness (AA)	3.71	0.64	.82	—		
2. Institutional Media Trust (IMT)	3.54	0.58	.79	−.46**	—	
3. Feminist Engagement (FE)	3.12	0.77	.84	.36**	−.29**	—

Note: N = 425. **p < .01. Cronbach's α values indicate acceptable internal consistency for all three composite scales. Higher scores indicate higher subjective algorithmic awareness, higher institutional media trust, and higher feminist engagement, respectively.
Source: Authors' analysis.

Appendix D

Cluster Analysis Profiles

Cluster	Label	n	%	Profile characteristics
C1	Mainstream security consumers	162	38.1%	High institutional media trust, lower subjective algorithmic awareness, and low feminist engagement
C2	Neutral observers	115	27.1%	Average-to-low scores across all three dimensions, with limited active engagement
C3	Critical analysts	93	21.9%	High subjective algorithmic awareness, moderate feminist engagement, and lower institutional media trust
C4	Digital activists	55	12.9%	High subjective algorithmic awareness and feminist engagement, low institutional media trust

Note: Cluster labels were assigned based on standardized profiles of subjective algorithmic awareness, institutional media trust, and feminist engagement. Percentages are calculated from the full sample of 425 respondents.
Source: Authors' analysis.