ISSN: 2450-6869
eISSN:2719-6763
No. 22, 2025

DEFENCE SCIENCE REVIEW
http://www.journalssystem.com/pno/

DOI: 10.37055/pno/ 230920

The impact of new technologies on women's military service: cybersecurity, gender integration and the redesign of service rules

Original article

Received: 2026-08-04

Revised:

Accepted: 2026-08-07

Final review: 2026-08-07

Peer review:

Double blind

Keywords: cybersecurity, women in the military, artificial intelligence, gender integration, military service.

Magdalena Kowalska[1, A-B, D]
ORCID 0009-0008-8324-4321

A - Research concept and design, B - Collection and/or assembly of data, C - Data analysis and interpretation,
D - Writing the article, E - Critical revision of the article,
F - Final approval of the article

[1] Faculty of Security, Logistics and Management, Military University of Technology, Poland

Abstract

Objectives: The article examines how emerging technologies - particularly cyber capabilities, artificial intelligence (AI), data analytics, autonomous systems and digitally mediated work - alter women's access to, performance in and experience of military service. It asks which service rules must change if technological modernisation is to strengthen operational effectiveness without reproducing gendered organisational inequalities.

Results: Technology widens the range of militarily decisive roles in which cognitive, analytical and socio-technical competence is more important than body-size proxies. Cybersecurity also turns every service member into a security actor. These opportunities are conditional: biased data, masculine professional stereotypes, unequal access to technical training, poorly fitted equipment, intrusive monitoring and online gender-based abuse can transfer older inequalities into digital systems. The article develops a gender-responsive cyber-service model based on task-related standards, skills-based career architecture, universal cyber competence, auditable AI, privacy-by-design, flexible but secure service arrangements, inclusive equipment and accountable command.

Conclusions: New technology does not automatically equalise military service. Its positive effect depends on institutional design. Gender-responsive cybersecurity is therefore not a welfare supplement but a readiness requirement: it expands the talent pool, improves risk recognition and helps maintain trust in data-driven command.

Corresponding author Magdalena Kowalska Faculty of Security, Logistics and Management, Military University of Technology, Poland; email: magdalena.kowalska@wat.edu.pl

Introduction

Armed forces are being reorganised around data, software, networks and increasingly autonomous systems. Cyber operations, artificial intelligence (AI), cloud computing, unmanned platforms, extended-reality training, biometrics and human-machine teaming now influence command, logistics, intelligence, force protection and personnel management. NATO's technology agenda treats data, AI, autonomy, quantum technologies, biotechnology and human enhancement, hypersonics and space as mutually reinforcing areas rather than isolated inventions (NATO, 2023a; NATO, 2026). This transformation changes the meaning of military capability. It also changes who can contribute, how competence is measured, where service is performed and which risks a service member must manage.

The implications for women are substantial but ambiguous. On one hand, digitally intensive forces depend less exclusively on the physical archetype historically associated with the infantryman. Cyber defence, intelligence analysis, electronic warfare, remotely operated systems and software-enabled logistics can broaden occupational access. On the other hand, technology is introduced into organisations whose recruitment practices, promotion systems and professional identities have long been gendered. Digital tools may therefore widen opportunity while encoding old assumptions into data, automated assessments and everyday work. A technically neutral system can produce unequal outcomes when its training data, performance indicators, interfaces or security procedures reflect a historically male workforce (Chandler, 2021; Blanchard and Bruun, 2024).

This is not a marginal personnel question. NATO data show that women represented, on average, 13.9 per cent of personnel in Allied armed forces in 2024, an increase of 3.5 percentage points over ten years, but progress remained slow and uneven. Women were also concentrated differently across branches and ranks, and they represented 13.4 per cent of reported reserve forces (NATO Committee on Gender Perspectives, 2025). The organisational challenge is thus not only to admit women but to ensure that they participate in capability-generating roles, acquire authority, and remain in service. Perceived gender equality affects the armed forces' attractiveness to women, while exclusion and narrow images of the 'real soldier' weaken recruitment and retention (Graf and Kuemmel, 2022; Kintzle et al., 2023; Reis and Menezes, 2020).

Cybersecurity sharpens this problem because it is simultaneously a specialist function and a service-wide discipline. A cyber operator may defend networks, conduct threat hunting or support effects in a multi-domain operation, but a pilot, logistician, commander or conscript can also expose an operational pattern through an unsecured device, location data, credential compromise or social-engineering attack. Consequently, digital security changes general duties of care, obedience, confidentiality and readiness. It creates requirements for continuous learning, secure use of personal and service devices, reporting of anomalies, protection of identities and responsible interaction with AI. These obligations apply to all personnel, yet their design can have differentiated consequences for women when threats involve sexualised disinformation, doxing, intimate-image abuse, online harassment or biased identity technologies (Millar, 2021; NATO, 2024a).

The main research question is: how do emerging technologies, especially cybersecurity and AI, alter the institutional rules and lived conditions of women's military service? Two subsidiary questions are addressed. First, through which mechanisms do new technologies expand or restrict women's participation and career progression? Second, what governance principles can convert technological change into both operational advantage and substantive gender integration? The working proposition is that technology improves women's military participation only where forces replace historical proxies with task-related standards, distribute cyber competence across the force, audit data-driven decisions, design secure flexibility and hold commanders accountable for inclusion and digital safety.

The article contributes in three ways. It connects scholarship on gendered military organisations with research on cyber expertise and military AI; it distinguishes access to technology-enabled jobs from authority within those jobs; and it proposes a practical model for service regulation. Denmark and the wider Nordic experience are used as an illustrative case because they combine long-standing formal access to military occupations, current reform of conscription and documented persistence of gendered professional norms. Polish military-academic materials are used to relate the argument to contemporary service conditions, technological modernisation and the human factor in protecting critical military infrastructure.

In Poland, the legal order does not reserve service in the civilian intelligence and security agencies for either sex. The Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency establishes eligibility criteria that are formally gender-neutral, while constitutional equality and anti-discrimination rules provide the wider normative framework (Republic of Poland, 2002). Nevertheless, the public cannot evaluate actual patterns of entry, assignment, retention and promotion because detailed sex-disaggregated staffing data are not routinely disclosed. The resulting knowledge gap should not be filled by assumptions. It instead requires a cautious analytical approach that separates verified institutional rules, historical evidence, international comparisons and the limited findings of exploratory research.

2. Materials and methods

The study uses a structured qualitative literature review and comparative document analysis. It is not a statistical meta-analysis and does not claim causal effects for a single technology. The unit of analysis is the service rule: a formal regulation, personnel practice or recurrent organisational expectation governing entry, training, task allocation, conduct, deployment, evaluation, promotion, welfare or separation. This approach is appropriate because the impact of technology appears not only in technical performance but also in decisions about who is considered suitable, who receives training and responsibility, and whose risk is recognised.

The evidence base was assembled purposively around four source groups. The first comprises peer-reviewed studies of women in military organisations, including Danish and Nordic research on gendered professional narratives, combat service, conscription and organisational integration (Muhr and Sløk-Andersen, 2017; Knudsen and Teisen, 2018; Ahlbäck, Sundevall and Hjertquist, 2024; Nielsen, 2026). The second covers cybersecurity work, cyber-military expertise, recruitment and human factors (Dawson and Thomson, 2018; Orye and Brantly, 2020; Fisher,

2022; Guidetti et al., 2023). The third consists of policy and governance documents on NATO cyber defence, responsible AI, Women, Peace and Security (WPS), standards and threat landscapes (NATO, 2024a; NATO, 2024b; ENISA, 2024; NIST, 2023). The fourth includes three Polish theses supplied by the user: on technology-driven force development, cybersecurity at military airfields and the contemporary determinants of military service (Andrzejczuk, 2026; Filipek, 2026; Świątek, 2026).

Sources were selected mainly from 2016-2026, with older works retained only where they provide a necessary conceptual baseline. Each text was coded against eight categories: recruitment and conscription; occupational standards; education and cyber competence; professional identity and authority; deployment and work organisation; personnel data and AI; equipment and infrastructure; and protection, reporting and accountability. A second coding pass identified opportunity-risk pairs. For example, remote access may improve continuity and work-life balance, yet it also expands the attack surface and can isolate personnel from informal networks. AI-supported selection may increase consistency, yet historical data can convert past exclusion into predictive scores.

The method has three limitations. Published evidence on gender in operational cyber units remains limited, many national datasets do not disaggregate cyber occupations by sex and rank, and policy documents describe intended practice rather than implementation. Security classification also prevents observation of many military systems and incidents. The findings are therefore analytical propositions grounded in converging evidence, not universal estimates. They are designed to guide policy evaluation and future empirical research, including interviews with servicewomen in cyber, intelligence, communications and unmanned-systems roles.

3. Technological transformation of military service

Technological change affects military service through convergence. AI depends on data, cloud or edge computing and secure connectivity; unmanned systems depend on communications, navigation, software and electronic protection; and decision-support systems depend on sensors, interfaces and trained users. Świątek (2026) identifies AI, autonomous systems, quantum technologies, space capabilities, mobile technologies and extended reality as cross-cutting drivers of force development. The crucial organisational consequence is that technology cannot be confined to a technical corps. It creates new specialist occupations while adding digital responsibilities to conventional ones.

In the industrial model, personnel systems often treated combat exposure and command of physically demanding units as the principal route to military legitimacy. The software-defined force complicates that hierarchy. Mission success may depend on a threat analyst who identifies anomalous network behaviour, a data steward who preserves integrity, a drone team that interprets sensor feeds, or a commander who understands the limits of an AI recommendation. These functions are not physically risk-free and are not detached from combat. They are parts of the kill chain, protection system and command architecture. Service rules should therefore connect status and promotion to mission effects and demonstrated competence rather than to inherited prestige rankings between branches.

Cyber operations have a distinctive personnel logic. Expertise changes quickly; some skills are scarce in the regular force but available among reservists or civilians; operational tasks may be performed from fixed sites; and teams combine engineering, intelligence, legal, linguistic and communication competence. Comparative research on military cyber reserves shows that armed forces use different models to gain access to civilian talent, but women remain underrepresented in both regular and reserve cyber communities (Orye and Brantly, 2020). The appropriate response is not simply a campaign depicting women at computer screens. It requires alternative entry pathways, recognition of civilian credentials, modular reserve obligations, transparent security-clearance processes, funded conversion training and promotion routes that do not penalise technical specialisation.

At the same time, cyber readiness is universal. ENISA's analysis of social engineering demonstrates how attackers exploit trust, urgency, identity and human behaviour rather than only software weaknesses (ENISA, 2024). Andrzejczuk's study of military airfield infrastructure similarly stresses regular training, incident procedures and awareness because personnel are a first line of defence (Andrzejczuk, 2026). The implication is a two-tier competence model: every service member needs validated baseline skills, while specialists need advanced role certification and recurring exercises. Treating cyber hygiene as an optional annual briefing creates a gap between the formal duty to protect information and the practical ability to do so.

AI adds a further layer because it can operate both as a military capability and as an administrative decision tool. It can support intelligence fusion, logistics, predictive maintenance, cyber defence, training and human-resource management. NATO's revised AI strategy retains six principles for responsible use: lawfulness; responsibility and accountability; explainability and traceability; reliability; governability; and bias mitigation (NATO, 2024b). Applied to personnel, these principles mean that an individual must be able to contest a consequential automated recommendation, commanders must know when a system is being used, performance must be tested across relevant groups, and responsibility cannot be displaced onto an algorithm.

The technical and human layers are inseparable. Cyber engineers interviewed in the Norwegian military worried not only about solving technical problems but about explaining them to non-specialists. Women also anticipated that gendered expectations about what a cyber expert looks and sounds like could reduce the credibility attributed to their advice (Fisher, 2022). This is operationally significant: a correct warning that is ignored because the speaker does not fit a stereotype has the same practical effect as a detection failure. Training must therefore include communication across professional communities, challenge and escalation procedures, and command norms that evaluate evidence rather than identity.

4. Women in armed forces: formal access, occupational distribution and authority

Women's military participation has expanded through legal equality, personnel demand and changing social expectations, but formal access is only the first stage of integration (Moore, 2017; Ben-Shalom, Lewin and Engel, 2019; Dahl, Kotsadam and Rooth, 2021). A systematic review by Reis and Menezes (2020) finds persistent inequalities in role distribution, career opportunities, privacy, harassment and organisational culture. The issue is not that all women experience the military in the same way. Rank, age, family status, branch, ethnicity, disability and technical background intersect. The analytical point is that policies designed around an unmarked male norm can impose additional costs on those who do not match it.

Danish research illustrates this distinction. Women gained broad access to military occupations relatively early, yet the organisational story of the capable soldier remained linked to masculinity. Muhr and Sløk-Andersen (2017) show how narratives of women's insufficiency survived formal inclusion. Interviews with Danish female combat soldiers similarly revealed a continuous negotiation between military competence and expectations of femininity (Knudsen and Teisen, 2018). Nielsen (2026) argues that apparently gender-neutral professionalism can reproduce exclusion when daily arrangements and social practices reward assimilation into male-coded norms. Technology enters this existing environment; it does not reset it.

The Nordic trajectory also demonstrates the role of labour demand. Ahlbäck, Sundevall and Hjertquist (2024) show that women's integration in Denmark, Finland, Norway and Sweden emerged from the interaction of personnel requirements and equality politics. Denmark's current model places women who turned eighteen after 1 July 2025 under the same obligation to attend an assessment for military service as men (Life in Denmark, 2026). NATO reporting recorded women at 10.9 per cent of the Danish Defence in 2024 and noted the decision to implement gender-equal conscription, alongside continuing challenges in embedding gender perspectives in defence culture (NATO Committee on Gender Perspectives, 2025). This produces a practical test: a larger and more diverse intake must be connected to the skills demanded by a digital force rather than channelled through old occupational expectations.

Gender-neutral conscription does not automatically create gender-neutral outcomes. Assessment instruments, recruitment messages, accommodation, uniforms, equipment, medical protocols, instructor behaviour and career information shape who completes training and what work they subsequently perform. A task-based standard should be identical for everyone performing the same task, but it must also be demonstrably related to that task. Removing unjustified height rules is different from lowering a safety-critical standard. The correct principle is validity: the armed force should be able to explain why a requirement predicts mission performance and should revalidate it when technology changes the task (Sørlie et al., 2020).

Authority is as important as representation. Women may enter cyber, intelligence or communications roles but remain positioned as support personnel whose advice is filtered through traditional combat arms. This creates a digital version of occupational segregation. Promotion boards should therefore value technical command, incident leadership, secure capability delivery, education of non-specialists and contributions to multi-domain operations. Otherwise, forces may recruit women into shortage occupations while preserving senior authority

for those following legacy career paths. The result would be numerical diversity without redistribution of professional power.

Retention is also shaped by the relationship between service and family life. Military mobility, sudden deployment, repeated relocation and prolonged separation can impose cumulative strain (Filipek, 2026; Diacone et al., 2025). NATO's 2023-2024 reporting shows that many Allies have work-life and childcare policies, but availability remains uneven (NATO Committee on Gender Perspectives, 2025). Digital work can reduce some travel and permit continuity during pregnancy, recovery, caregiving or reserve service. Yet flexible service should be available on transparent, gender-neutral terms; otherwise, women may be concentrated in remote posts and lose operational exposure, informal networks or promotion opportunities.

5. Cybersecurity as a driver of new service rules for women

The interaction between gender and cybersecurity is best understood as a redesign problem. Security rules determine access to information, devices, spaces, networks and authority. Personnel rules determine entry, training, assignment, evaluation and support. When these systems are designed separately, a formally inclusive personnel policy can be undermined by a security architecture that assumes uninterrupted presence, uniform bodies, linear careers or trust buildthrough male-dominated informal networks. Conversely, flexible work introduced without security engineering can create unacceptable operational risk.The objective is secure inclusion: arrangements that enlarge the effective talent pool while maintaining mission assurance.

5.1 Recruitment, selection and role assignment

Technology enables skills-based recruitment. Cyber ranges, practical challenges and portfolio assessment can reveal problem-solving ability more directly than generic educational pedigree or physical proxies. This may benefit candidates whose competence developed through civilian work, self-study or non-linear careers. It can also support reserve models that combine military discipline with scarce civilian expertise. However, digital selection tools must be accessible, validated and monitored. If success profiles are trained on past high performers from a male-dominated organisation, an algorithm may learn proxies for historical similarity rather than future capability.

The same concern applies to automated screening of applications, psychological assessment, voice analysis, facial recognition and predictive attrition models. Chandler (2021) shows that gender norms can enter military AI throughout the lifecycle, including data collection, model training, evaluation and use. NIST distinguishes systemic, computational/statistical and human-cognitive bias, which is useful for military personnel governance (NIST, 2023). A fair model requires representative and relevant data, but balanced data alone are insufficient. The target variable may itself be biased - for example, historical promotion, commander ratings or retention in a hostile climate. Human review must therefore examine the institutional meaning of the label, not only model accuracy.

Recruitment messaging also matters. Cyber occupations are often portrayed through a masculine 'hacker' or elite-warrior identity. Fisher's findings on the stereotype of the male cyber engineer and Graf and Kuemmel's evidence that perceived equality influences employer

attractiveness suggest a straightforward policy implication: forces should present varied technical roles and credible women practitioners, while also publishing role standards, training pathways and safeguards. Representation in advertising is useful only if it matches the service environment candidates will encounter

5.2 Education, competence and professional credibility

All personnel should receive recurring training in authentication, data handling, phishing, operational security, incident reporting and safe use of AI-enabled tools. Such training must be evaluated through behaviour and exercises rather than attendance. Phishing is an adaptive socio-technical attack rather than a static technical trick (Alkhalil et al., 2021); gamified simulations can improve engagement and reporting, although results should not become opaque disciplinary scores (Canham, Posey and Constantino, 2022). A command climate in which personnel fear humiliation for reporting a mistake is incompatible with rapid incident response. This has a gender dimension where women already experience heightened scrutiny or token status.

Specialist development requires deeper change. Technical career fields need instructors, mentors, laboratory access, protected learning time and command opportunities. Soft skills are not secondary: successful cyber performance includes communication, teamwork and the ability to translate uncertainty for decision-makers (Dawson and Thomson, 2018). If women are stereotyped as less technical, they may perform additional credibility work before their advice is accepted. Formal escalation routes, paired briefings, red-team protocols and evidence-based decision logs reduce dependence on informal status.

AI-supported military education can personalise learning and identify gaps, but data-driven assessment can also reproduce bias or punish different interaction styles. Kuloğlu and Koçanli (2025) argue that AI adoption in professional military education should be aligned with gender-sensitive governance. Service rules should require instructors to disclose consequential use of automated analytics, validate measures across groups, permit review and correction of records, and prohibit reliance on a single score for career decisions. Training data should be retained only for defined purposes and protected as sensitive personnel information.

5.3 Deployment, remote work and the military family

Cyber and intelligence functions can sometimes be performed from distributed sites, creating options for reserve participation, continuity during temporary medical restrictions and reduced relocation. These possibilities may improve retention, especially where caregiving responsibilities are unequally distributed. They can also allow personnel with valuable civilian skills to contribute without adopting a fully conventional service pattern. This does not mean that cyber service is comfortable office work. Shift work, classified facilities, continuous operations and cognitive overload can produce significant strain, and many tasks cannot be performed from home (Guidetti et al., 2023).

Secure flexibility therefore requires role-by-role analysis. Commanders should identify which outputs require presence in a classified environment, which can be produced through accredited remote infrastructure and which can be scheduled flexibly. Eligibility should be based on mission and security conditions rather than assumptions about motherhood.

Participation in flexible arrangements must not remove personnel from promotion-relevant assignments, exercises or leadership. The same principle applies to pregnancy, parental leave and return-to-duty pathways: competence should be maintained through secure training and planned reintegration, not through career isolation.

Digital connectivity can also extend command demands into private life. Always-on messaging, location tracking and expectations of immediate response may intensify the traditional military requirement of availability. Filipek (2026) describes how sudden travel, separation and relocation affect family organisation; digital command can add a layer of permanent reachability without removing physical absence. Service regulations should define duty windows, emergency contact channels, device expectations and data collection, while preserving the commander's ability to act in genuine crises. Clear rules protect readiness by reducing chronic overload and ambiguous availability.

5.4 Personnel data, biometrics and AI-enabled management

Military organisations collect unusually sensitive data: health, fitness, location, performance, family circumstances, security vetting, communications and sometimes biometrics. Wearables and connected equipment can improve safety, training and health monitoring, but they also create a detailed record of bodies and behaviour. Because devices and baseline models have often been developed around male populations, error rates or thresholds may not transfer equally. Data on menstruation, pregnancy or reproductive health can be clinically useful yet especially vulnerable to misuse, inference or unauthorised disclosure.

Privacy and cybersecurity should therefore be built into capability acquisition. Data minimisation, purpose limitation, access control, retention schedules, audit logs, encryption and independent review are operational controls, not civilian luxuries. The EU AI Act excludes systems used exclusively for military, defence or national-security purposes, so armed forces cannot assume that civilian compliance automatically governs military personnel analytics (European Union, 2024). NATO's responsible-use principles and national law must be translated into enforceable internal rules. High-consequence personnel systems should undergo algorithmic impact assessment, subgroup testing, adversarial testing and periodic review after deployment.

Human oversight must be substantive. A commander who merely confirms an automated recommendation without understanding its basis does not provide a meaningful safeguard. Decision-makers need training on model limitations and the authority to depart from outputs. Personnel need notice when automated analysis materially affects selection, assignment, discipline or promotion, subject to legitimate security constraints. A protected appeal route should permit correction of inaccurate data and examination of whether the system produced unjustifiably different outcomes. Blanchard and Bruun (2024) emphasise that bias can arise from society, data processing, algorithm development and use; governance must cover all four points rather than focus only on code.

5.5 Technology-enabled gender threats and digital protection

Women in uniform can be targeted through cyber means in ways that combine operational and gendered harm. Doxing can expose home addresses or family relationships; account compromise can support blackmail; deepfakes and intimate-image abuse can damage trust; sexualised disinformation can be used to undermine authority; and coordinated harassment can impose psychological costs. These acts may be conducted by adversaries, extremist communities or insiders. NATO's revised AI strategy explicitly identifies AI-enabled disinformation, information operations and gender-based violence as concerns (NATO, 2024b). This connects personnel protection directly to alliance security.

Existing reporting systems often separate cybersecurity incidents, harassment and counter-intelligence. A victim may therefore be sent between technical, disciplinary and welfare channels while evidence disappears. Forces should establish a joint protocol that preserves digital evidence, secures accounts and devices, assesses operational compromise, protects privacy, offers psychological and legal support and prevents retaliation. Commanders must understand that sexualised abuse can be an influence operation or coercive security threat, not merely an interpersonal dispute.

Protective measures should avoid transferring the burden to women by restricting their visibility or access. Advising women to disappear from professional networks may reduce career opportunities and public representation while leaving the aggressor's advantage intact. Risk-based training, identity protection, rapid takedown procedures, secure communication channels and family awareness are preferable. Digital safety should also cover partners and dependants when adversaries use family information to pressure personnel.

6. Results: a gender-responsive cyber-service model

The review identifies six mechanisms through which technology changes women's service. First, occupational substitution changes the weight of physical, cognitive and digital tasks. Second, competence visibility changes when practical digital assessment can reveal skills but algorithmic systems can obscure judgement. Third, spatial reconfiguration creates distributed and reserve service possibilities while expanding the attack surface. Fourth, datafication makes personnel decisions more measurable but also more intrusive and path-dependent. Fifth, professional re-ranking can raise the strategic value of cyber expertise while leaving traditional hierarchies intact. Sixth, threat personalisation allows adversaries to combine operational targeting with gendered abuse. These mechanisms show why neither technological determinism nor a purely cultural explanation is sufficient.

Table 1. Technology-service mechanisms: opportunities, gender-related risks and rule implications

Technology or practice	Operational and inclusion opportunity	Gender-related or security risk	Required service rule
AI-supported recruitment and HR	Skills-based screening; consistency; identification of non-traditional talent	Historical labels, proxy discrimination, opaque ranking	Impact assessment; task-valid criteria; subgroup testing; human review and appeal
Cyber operations and digital intelligence	High-value roles based on analytical and socio-technical competence	Technical stereotyping; support-role segregation; ignored expertise	Transparent competencies; specialist command; evidence-based escalation; mentoring

Technology or practice	Operational and inclusion opportunity	Gender-related or security risk	Required service rule
Remote and distributed service	Reserve access; continuity; reduced relocation; flexible learning	Isolation; unequal visibility; home-network risk; permanent reachability	Role-based eligibility; accredited access; duty windows; equal promotion credit
AI-enabled education and simulation	Adaptive learning; scalable exercises; safe rehearsal	Biased scoring; surveillance; inaccessible interfaces	Disclosure; multi-source assessment; accessibility tests; limited retention of learning data
Wearables, biometrics and connected equipment	Safety, health insight and performance feedback	Male baselines; privacy intrusion; reproductive-health exposure	Representative validation; data minimisation; medical confidentiality; secure lifecycle
Unmanned and autonomous systems	Reduced physical exposure; new operator, analyst and commander roles	Deskilling; automation bias; gendered recognition errors	Human-machine training; bias testing; meaningful control; accountable decisions
Social media and digital identity	Recruitment, professional networks and strategic communication	Doxing, deepfakes, sexualised disinformation and harassment	Joint cyber/harassment response; evidence preservation; identity and family protection

Source: Author's analysis based on Chandler (2021), Fisher (2022), NATO (2024a; 2024b) and Blanchard and Bruun (2024).

6.1 From equality of access to capability assurance

Table 1 demonstrates that every technology creates both an opportunity and a governance risk. This symmetry is important. An armed force should not reject a useful system merely because bias is possible, nor deploy it on the assumption that technical performance guarantees fairness. The correct response is assurance across the lifecycle: define the mission need, examine affected personnel, validate data and interfaces, test in realistic conditions, train users, monitor outcomes and provide correction. Gender analysis becomes one form of operational red-teaming because it tests whether a system performs outside the population and assumptions that dominated its development.

The model also rejects occupational essentialism. Women are not inherently better communicators, more ethical cyber operators or naturally suited to remote work. Such claims simply replace negative stereotypes with flattering ones. The case for participation is equal access to the full talent pool and the operational value of teams capable of recognising varied risks. Diversity can improve analysis only where different perspectives are heard, expertise is distributed and dissent is safe. Representation without authority cannot deliver this effect

Table 2 translates the review into eight principles. Together they link personnel policy with cybersecurity governance. Mission-valid standards protect effectiveness; universal cyber duty treats security as part of military professionalism; a skills-based career system prevents technical roles from becoming dead ends; auditable AI protects both fairness and command responsibility; secure flexibility supports retention without creating uncontrolled access; inclusive equipment prevents readiness losses; integrated digital protection addresses compound threats; and command accountability makes implementation measurable.

Table 2. Eight principles of gender-responsive cyber service

Principle	Operational requirement
1. Mission-valid standards	Every entry, fitness and technical requirement must be demonstrably related to the task and revalidated when technology changes it.
2. Universal cyber duty	All personnel require recurrent, tested cyber competence; specialists require role certification and continuous development.
3. Skills-based career architecture	Civilian credentials, reserve expertise, technical leadership and incident command must count in assignment and promotion.
4. Auditable AI and data	Consequential personnel systems require traceability, subgroup testing, human responsibility, correction and appeal.
5. Secure flexibility	Remote, distributed and part-time service must be role-based, security-engineered and career-neutral.
6. Inclusive equipment and interfaces	Uniforms, protective equipment, workstations, wearables and software must be validated for the service population.
7. Integrated digital protection	Cyber incident, counter-intelligence, harassment and welfare procedures must converge for doxing, deepfakes and coercion.
8. Command accountability	Leaders must monitor access, training, task allocation, credibility, promotion and retention outcomes, not only headcount.

Source: Author's own elaboration.

7. Discussion

The central finding is that new technology changes the structure of opportunity but not automatically the distribution of power. Cybersecurity can weaken the historical link between military legitimacy and a narrow physical archetype because decisive effects increasingly depend on cognitive, analytical, linguistic and socio-technical skill. Yet cyber communities can produce their own masculine stereotypes, while AI can scale past inequalities (Millar and Shires, 2024). The outcome is determined by institutional choices concerning standards, data, career value and command practice.

This finding supports scholarship that treats the military as a gendered organisation rather than a neutral container into which women are added. Danish studies show that formal equality can coexist with narratives of women's insufficiency and demands for assimilation (Muhr and Sløk-Andersen, 2017; Nielsen, 2026). Cyber research adds a new layer: even technically competent women may anticipate reduced credibility as experts (Fisher, 2022). Thus, the key transition is from access to epistemic authority - the recognised right to define a technical problem, warn a commander and shape a decision.

Operational effectiveness and equality are sometimes presented as competing goals. The evidence suggests a more precise relationship. Invalid standards, ignored expertise, poor equipment fit, unreported incidents and biased personnel systems reduce readiness. Conversely, standards cannot be relaxed merely to improve representation. The task is to measure the right capability. RAND's work on occupation-specific physical standards illustrates the principle that requirements should be linked to actual job demands (Hardison, Hosek and Bird, 2018). The same logic should govern cyber testing, command prerequisites and automated assessment.

The Danish case is useful for NATO and Poland because it links gender-neutral service obligations with a changing security environment. Universal assessment can broaden the recruitment base, but only a deliberately designed pathway will connect women to cyber, AI, electronic warfare and unmanned-systems careers. Poland's development of Cyber Defence Forces and its investment in AI and unmanned capabilities create a similar need to align personnel and technology strategies (National Security Bureau, 2020; Świątek, 2026). Recruitment targets should be accompanied by data on training access, occupational assignment, certification, command, promotion and retention.

For NATO, interoperability should include the human layer. Allies share networks, data, exercises and command structures, but national service rules differ. A common baseline could require gender-responsive testing of AI-enabled personnel tools, minimum digital-protection procedures, recognition of cyber reserve qualifications and reporting of women by cyber occupation and rank. NATO's WPS Policy already calls for gender perspectives in standards and responsible use of AI (NATO, 2024a); implementation also depends on the institutional work of bodies such as the NATO Committee on Gender Perspectives (Hurley, 2024). Gender Advisors, cyber commands, personnel directorates, medical services, legal advisers and acquisition authorities should be connected rather than leaving responsibility in a single specialist office.

Commanders require usable indicators. Headcount is necessary but insufficient. A unit-level dashboard might compare application, selection, course access, certification, operational task allocation, incident-reporting outcomes, promotion, flexible-service use and exit reasons by sex and rank, subject to privacy and sample-size safeguards. Disparity is a prompt for investigation, not proof of discrimination. The aim is to identify friction points: for example, whether women enter a cyber programme but are assigned fewer operational tasks, or whether flexible work correlates with slower promotion.

Acquisition rules also need personnel evidence. A wearable, biometric gate, voice interface or decision tool should not be accepted on aggregate accuracy alone. Test populations must reflect intended users and operating conditions. Procurement contracts should require documentation, audit access, security patching, data portability, incident notification and the ability to suspend or override a system. Where vendors claim that a model is proprietary, the state still retains responsibility for military decisions. Explainability may be constrained by classification, but accountability cannot be outsourced.

Work-life policy is a readiness investment rather than a concession. Digital service options can mitigate some effects of relocation and family separation described in contemporary military experience (Filipek, 2026), yet they must be designed without creating a secondary career track. NATO data indicate that work-life and childcare measures are common but not universal (NATO Committee on Gender Perspectives, 2025). Secure flexibility should be accompanied by equal access to exercises, command roles, professional education and networks. Men must be encouraged to use parental and flexible provisions so that such arrangements do not become coded as women's exceptions.

Protection from technology-enabled gender harm should be exercised like other readiness procedures. Units can rehearse a scenario in which a servicewoman is doxed, a deepfake is circulated and credentials are targeted through family members. The response should connect incident containment, counter-intelligence, strategic communication, evidence preservation, welfare and legal action. This approach recognises that the same event can affect an individual, a unit's trust and an operation's information environment. It also avoids blaming the target for maintaining a professional digital presence.

There are risks of overcorrection. Excessive monitoring in the name of security can chill reporting and disproportionately expose intimate data. Assigning all women to engagement or gender-adviser duties can narrow their careers. Treating cyber roles as a route around all physical requirements can create status divisions and misunderstand operational demands. The proposed model therefore rests on role validity, individual competence and universal safeguards, not assumptions about women as a group.

Future research should test the model empirically. Comparative studies could follow cohorts entering gender-neutral conscription and examine assignment to digital occupations. Interviews and network analysis could explore whose cyber advice reaches command decisions. Audits could compare AI-based personnel recommendations with human outcomes, while preserving classified information and personal privacy. Longitudinal research should examine whether remote and reserve pathways improve retention without slowing promotion. Finally, incident studies should evaluate integrated responses to doxing, deepfakes and online harassment.

8. Conclusions

New technologies are transforming women's military service in three connected senses. They create new operational roles and routes into service; they impose new universal duties of digital security and responsible technology use; and they alter the administrative systems through which personnel are selected, monitored and promoted. These changes can weaken old barriers, but they can also digitise them.

The answer to the main research question is therefore conditional. Cybersecurity and AI broaden women's effective participation when armed forces use mission-valid standards, recognise technical leadership, provide universal and specialist cyber education, secure flexible service, validate equipment and interfaces across the population, and govern personnel data through auditable human responsibility. Without these measures, technology may place women in new roles while preserving unequal credibility, career value and exposure to harm.

The most important policy shift is from representation to capability assurance. Gender analysis should be embedded in cyber doctrine, acquisition, personnel management, training and command review. It should ask not only how many women serve, but whether they receive access to scarce skills, lead operational work, influence decisions, use safe equipment, retain control over sensitive data and obtain effective protection from technology-enabled abuse. These are measurable features of readiness.

For NATO members, including Poland and Denmark, the practical agenda is clear: align technology and personnel strategies; collect occupationally specific data; create technical career and reserve pathways; audit AI-enabled decisions; and connect WPS structures with cyber commands. A digitally capable force cannot be built from technology alone. It depends on whether institutions can recognise, develop and trust competence across the whole population they are expected to defend.

References

Ahlbäck, A., Sundevall, F. and Hjertquist, J. (2024) 'A Nordic model of gender and military work? Labour demand, gender equality and women's integration in the armed forces of Denmark, Finland, Norway and Sweden', Scandinavian Economic History Review, 72(1), pp. 49-66. doi: 10.1080/03585522.2022.2142661.

Alkhalil, Z., Hewage, C., Nawaf, L. and Khan, I. (2021) 'Phishing attacks: A recent comprehensive study and a new anatomy', Frontiers in Computer Science, 3, 563060. doi: 10.3389/fcomp.2021.563060.

Ben-Shalom, U., Lewin, E. and Engel, S. (2019) 'Organizational processes and gender integration in operational military units: An Israel Defense Forces case study', Gender, Work & Organization, 26(9), pp. 1289-1303. doi: 10.1111/gwao.12348.

Canham, M., Posey, C. and Constantino, M. (2022) 'Phish Derby: Shoring the human shield through gamified phishing attacks', Frontiers in Education, 6, 807277. doi: 10.3389/feduc.2021.807277.

Dahl, G.B., Kotsadam, A. and Rooth, D.-O. (2021) 'Does integration change gender attitudes? The effect of randomly assigning women to traditionally male teams', Quarterly Journal of Economics, 136(2), pp. 987-1030. doi: 10.1093/qje/qjaa047.

Dawson, J. and Thomson, R. (2018) 'The future cybersecurity workforce: Going beyond technical skills for successful cyber performance', Frontiers in Psychology, 9, 744. doi: 10.3389/fpsyg.2018.00744.

Diacone, N., van Baarle, E., Bosch, J. and Moe... [Incomplete entry – please verify and complete before submission]

Moore, B.L. (2017) 'Introduction to Armed Forces & Society: Special issue on women in the military', Armed Forces & Society, 43(2), pp. 191-201. doi: 10.1177/0095327X17694909.

Muhr, S.L. and Sløk-Andersen, B. (2017) 'Exclusion and inclusion in the Danish military: A historical analysis of the construction and consequences of a gendered organizational narrative', Journal of Organizational Change Management, 30(3), pp. 367-379. doi: 10.1108/JOCM-10-2016-0195.

Nielsen, H.P. (2026) 'Fighting to become one of the boys: Inattentive (re)gendering of military professionalism among Danish soldiers', Armed Forces & Society, 52(1). doi: 10.1177/0095327X241298609.

Reis, J. and Menezes, S. (2020) 'Gender inequalities in the military service: A systematic literature review', Sexuality & Culture, 24, pp. 1004-1018. doi: 10.1007/s12119-019-09662-y.

Sørlie, H.O., Hetland, J., Dysvik, A., Fosse, T.H. and Martinsen, Ø.L. (2020) 'Person-organization fit in a military selection context', Military Psychology, 32(3), pp. 237-246.

Other sources

Andrzejczuk, N. (2026) Cybersecurity at military airfields - challenges and methods of critical infrastructure protection (in Polish). Unpublished master's thesis. Warsaw: Military University of Technology.

Blanchard, A. and Bruun, L. (2024) Bias in Military Artificial Intelligence. Stockholm: Stockholm International Peace Research Institute.

Chandler, K. (2021) Does Military AI Have Gender? Geneva: United Nations Institute for Disarmament Research.

National Security Bureau (2020) National Security Strategy of the Republic of Poland 2020. Warsaw: National Security Bureau.

NATO (2023a) Science and Technology Trends 2023-2043. Brussels: NATO Science and Technology Organization.

NATO (2024a) NATO Policy on Women, Peace and Security. Brussels: North Atlantic Treaty Organization.

NATO (2024b) Summary of NATO's Revised Artificial Intelligence Strategy. Brussels: North Atlantic Treaty Organization.

NATO (2026) Innovation and technology adoption. Updated: 8 July 2026. Available at: nato.int (Accessed: 31 July 2026).

NATO Committee on Gender Perspectives (2025) Summary of the National Reports of NATO Member and Partner Nations 2023-2024. Brussels: NATO.

NIST (2023) Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. Gaithersburg, MD: National Institute of Standards and Technology. doi: 10.6028/NIST.AI.100-1.

Orye, E. and Brantly, A.F. (2020) Cyber Workforce Recruitment and Retention: An Awareness Study. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Świątek, J. (2026) Modern technologies shaping the development of armed forces (in Polish). Unpublished master's thesis. Warsaw: Military University of Technology.