

Studia Bezpieczeństwa Narodowego
Zeszyt 39 (2026)
ISSN 2028-2677, s. 81-100
DOI: 10.37055/sbn/223975

Instytut Bezpieczeństwa
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna
w Warszawie

National Security Studies
Volume 39 (2026)
ISSN 2028-2677, pp. 81-100
DOI: 10.37055/sbn/223975

Institute of Security
Faculty of Security, Logistics and Management
Military University of Technology
in Warsaw

ROLA KOBIET W CYBERBEZPIECZEŃSTWIE WYBRANYCH SŁUŻB MUNDUROWYCH

THE ROLE OF WOMEN IN CYBERSECURITY WITHIN SELECTED UNIFORMED SERVICES

Magdalena KOWALSKA

Wojskowa Akademia Techniczna im. J. Dąbrowskiego w Warszawie
ORCID: 0009-0008-8324-4321

Abstrakt. Przedmiotem badań, których wyniki przedstawiono w artykule, jest rola kobiet w zapewnianiu cyberbezpieczeństwa służb mundurowych, ze szczególnym uwzględnieniem Sił Zbrojnych RP, Policji oraz Straży Granicznej. Celem badań jest określenie obszarów kompetencji kobiet w systemie cyberbezpieczeństwa państwa oraz identyfikacja czynników ograniczających pełne wykorzystanie ich potencjału zawodowego, eksperckiego i organizacyjnego. Problem badawczy sformułowano w postaci pytania: w jaki sposób udział kobiet wpływa na rozwój zdolności cyberbezpieczeństwa w formacjach mundurowych? Weryfikacji poddano hipotezę, że obecność kobiet w zespołach cyberbezpieczeństwa nie ma wyłącznie znaczenia równościowego, lecz stanowi istotny czynnik zwiększający odporność organizacyjną, jakość analizy zagrożeń, interdyscyplinarność procesu decyzyjnego oraz skuteczność reagowania na incydenty bezpieczeństwa komputerowego. W badaniach zastosowano jakościową analizę dokumentów, przegląd literatury przedmiotu oraz analizę porównawczą zadań realizowanych przez trzy wybrane formacje mundurowe. Uwzględniono akty prawne, dokumenty strategiczne, raporty instytucji międzynarodowych, publikacje naukowe oraz informacje udostępniane przez właściwe instytucje publiczne. Wyniki badań wskazują, że kobiety mogą pełnić kluczowe funkcje w analizie cyberzagrożeń, informatyce śledczej, ochronie systemów teleinformatycznych, zarządzaniu ryzykiem, edukacji cyberbezpieczeństwa, komunikacji kryzysowej oraz współpracy międzynarodowej. Ich kompetencje są szczególnie istotne w środowisku wymagającym precyzyjnej analizy danych, pracy zespołowej, umiejętności komunikacyjnych i zdolności łączenia perspektywy technicznej, prawnej oraz organizacyjnej. Jednocześnie stwierdzono występowanie barier edukacyjnych, stereotypów zawodowych, ograniczonej widoczności ekspertek, niedostatecznie rozwiniętych ścieżek mentoringowych oraz niewystarczającego monitorowania udziału kobiet w specjalistycznych stanowiskach cyberbezpieczeństwa. Wnioski prowadzą do sformułowania rekomendacji obejmujących systemową rekrutację, specjalistyczne szkolenia, programy retencji, mentoring ekspercki oraz jawne monitorowanie karier kobiet w cyberobronie, cyberdochodzeniach, ochronie infrastruktury granicznej i bezpieczeństwie danych. Artykuł wskazuje także na konieczność pogłębionych badań empirycznych, obejmujących przebieg karier, motywacje, doświadczenia służbowe oraz potrzeby szkoleniowe kobiet pełniących funkcje techniczne,

analityczne i kierownicze w strukturach odpowiedzialnych za bezpieczeństwo cyfrowe państwa oraz ochronę obywateli i cudzoziemców w warunkach narastającej złożoności współczesnych zagrożeń hybrydowych.

Abstract. The subject of the research presented in this article is the role of women in ensuring the cybersecurity of uniformed services, with particular emphasis on the Armed Forces of the Republic of Poland, the Police, and the Border Guard. The aim of the research is to determine the areas of women's competencies in the field of state cybersecurity and to identify the factors limiting the use of this potential. The research problem was formulated as the following question: how does women's participation influence the development of cybersecurity capabilities in uniformed formations? The study sought to verify the research hypothesis that the presence of women in cybersecurity teams is not merely a matter of equality, but constitutes a factor that increases organisational resilience, improves the quality of threat analysis, and enhances the effectiveness of responding to computer security incidents. The research employed qualitative document analysis, a literature review, and a comparative analysis of the tasks performed by the three formations. Strategic documents, legal acts, reports by international institutions, and information published by relevant public institutions were considered. The findings indicate that women can perform key functions in cyber threat analysis, digital forensics, protection of ICT systems, risk management, cybersecurity education, and international cooperation. At the same time, educational barriers, professional stereotypes, limited visibility of female experts, and insufficiently developed mentoring pathways persist. The conclusions lead to recommendations including systematic recruitment, specialist training, retention programmes, and transparent monitoring of women's participation in cybersecurity areas. The article also highlights the need for more detailed empirical research on the career paths of women in structures responsible for cyber defence, cyber investigations, the protection of digital border infrastructure, and the security of citizens' and foreigners' data.

Słowa kluczowe: cyberbezpieczeństwo, służby mundurowe, kobiety, różnorodność, kompetencje cyfrowe.
Keywords: cybersecurity, uniformed services, women, diversity, digital competences.

Wprowadzenie

Bezpieczeństwo państwa coraz silniej zależy od odporności systemów teleinformatycznych, jakości zarządzania informacją oraz zdolności do rozpoznawania zagrożeń w cyberprzestrzeni. Współczesne operacje wojskowe, działania policyjne i ochrona granic państwowych są realizowane w środowisku, w którym dane, infrastruktura cyfrowa i systemy łączności stanowią zasób strategiczny. Cyberataki, operacje wpływu, wyłudzenia, przejęcia kont, złośliwe oprogramowanie, ataki na łańcuchy dostaw oraz naruszenia poufności danych mogą powodować skutki porównywalne z tradycyjnymi zagrożeniami bezpieczeństwa. ENISA wskazuje, że na podstawie raportów możliwe jest identyfikowanie trendów, aktorów, technik oraz środków ograniczania ryzyka, co potwierdza trwałe znaczenie systematycznej analizy środowiska cyberzagrożeń (ENISA 2024).

Cyberprzestrzeń ma również wymiar militarny. NATO uznaje cyberprzestrzeń za domenę operacyjną, a więc przestrzeń, w której państwa muszą posiadać zdolności obronne, rozpoznawcze i dowódcze (NATO 2021). W polskim porządku prawnym szczególne znaczenie ma Ustawa o obronie Ojczyzny, zgodnie z którą Wojska Obrony Cyberprzestrzeni są specjalistycznym komponentem Sił Zbrojnych właściwym do realizacji pełnego spektrum działań w cyberprzestrzeni, w tym proaktywnej ochrony i aktywnej obrony zasobów kluczowych

dla Sił Zbrojnych RP (Rzeczpospolita Polska 2022). W tym kontekście cyberbezpieczeństwo nie jest wyłącznie obszarem technicznym, lecz częścią jedną z kluczowych domen zapewniania bezpieczeństwa narodowego (NATO 2021; Rzeczpospolita Polska 2022; Rada Ministrów 2019).

Równolegle zachodzi zmiana społeczna i organizacyjna związana z udziałem kobiet w służbach mundurowych. Formacje historycznie postrzegane jako męskie coraz częściej wymagają kompetencji analitycznych, komunikacyjnych, językowych, prawnych, technicznych i menedżerskich. Cyberbezpieczeństwo jest dobrym przykładem tej przemiany, ponieważ skuteczność działań zależy przede wszystkim od wiedzy specjalistycznej, umiejętności współpracy, odporności psychicznej, zdolności uczenia się oraz poprawnego wnioskowania na podstawie danych. Nie oznacza to, że znikają bariery organizacyjne i kulturowe; oznacza natomiast, że kryteria skuteczności w cyberbezpieczeństwie tworzą przestrzeń do szerszego włączenia kobiet w zadania operacyjne, analityczne i kierownicze (Wojsko Polskie b.d.; Policja 2024; Straż Graniczna 2024; OECD 2024).

Celem artykułu jest pogłębiona analiza roli kobiet w cyberbezpieczeństwie trzech typów formacji: wojska, policji i straży granicznej. Problem badawczy przyjmuje postać pytania: w jaki sposób udział kobiet wpływa na rozwój zdolności cyberbezpieczeństwa w służbach mundurowych? Hipoteza brzmi: wzrost udziału kobiet w zespołach cyberbezpieczeństwa zwiększa potencjał analityczny i organizacyjny formacji mundurowych, jednak wymaga wsparcia systemowego w zakresie rekrutacji, kształcenia, awansu i retencji. Tak sformułowany cel i hipoteza wymagają ujęcia interdyscyplinarnego, łączącego perspektywę nauk o bezpieczeństwie, zarządzania zasobami ludzkimi, studiów nad technologią oraz praktyki cyberobrony i zwalczania cyberprzestępczości (van Knippenberg i Schippers 2007; Woolley et al. 2010; OECD 2024).

Aktualny stan wiedzy

Z analizy literatury przedmiotu wynika, że cyberbezpieczeństwo jest kategorią szerszą niż klasycznie rozumiane bezpieczeństwo informacji. Obejmuje ono ochronę danych, systemów i sieci, ale także odporność organizacji, bezpieczeństwo użytkowników, ciągłość usług publicznych, zarządzanie ryzykiem oraz zdolność państwa do reagowania na zagrożenia powstające w środowisku cyfrowym. Von Solms i van Niekerk wskazują, że cyberbezpieczeństwo wykracza poza ochronę zasobów informacyjnych i obejmuje również ochronę osób oraz procesów społecznych zależnych od technologii cyfrowych. Podobnie Craigen, Diakun-Thibault i Purse definiują cyberbezpieczeństwo jako zespół działań, zasobów i praktyk służących ochronie cyberprzestrzeni, użytkowników i organizacji przed szkodliwymi zdarzeniami. Dla służb mundurowych oznacza to konieczność odejścia od wąskiego rozumienia

cyberbezpieczeństwa jako zadania informatycznego i traktowania go jako elementu bezpieczeństwa narodowego, organizacyjnego i operacyjnego (von Solms i van Niekerk 2013; Craigen et al. 2014; Singer i Friedman 2014).

W literaturze naukowej podkreśla się również, że cyberzagrożenia nie mają jedynie technicznego charakteru. Hansen i Nissenbaum pokazują, że cyberbezpieczeństwo stało się odrębnym sektorem bezpieczeństwa, w którym zagrożenia są konstruowane przez połączenie technicznych podatności, praktyk politycznych i społecznych wyobrażeń o katastrofie cyfrowej. Dunn Cavelti analizuje natomiast proces politycznego konstruowania cyberzagrożeń i wskazuje, że bezpieczeństwo cybernetyczne jest powiązane z ochroną infrastruktury krytycznej, zdolnością państwa do działania i zaufaniem społecznym. W konsekwencji zespoły odpowiedzialne za cyberbezpieczeństwo w formacjach mundurowych muszą łączyć wiedzę techniczną z analizą strategiczną, prawną, społeczną i komunikacyjną (Dunn Cavelti 2008; Hansen i Nissenbaum 2009).

W odniesieniu do wojskowego wymiaru cyberbezpieczeństwa kluczowe jest pojęcie cyberprzestrzeni jako domeny operacyjnej. Jeżeli cyberprzestrzeń jest przestrzenią prowadzenia działań, to zespół cyberbezpieczeństwa nie może być traktowany wyłącznie jako zaplecze administracyjne. Staje się elementem zdolności operacyjnych, wpływa na ciągłość dowodzenia, ochronę informacji, bezpieczeństwo systemów łączności i odporność infrastruktury używanej przez wojsko. W literaturze strategicznej zwraca się uwagę, że cyberoperacje mogą obejmować sabotaż, szpiegostwo, zakłócanie procesów decyzyjnych i działania informacyjne, a ich skutki zależą od kontekstu politycznego i organizacyjnego. Rid przestrzega przed automatycznym utożsamianiem wszystkich cyberoperacji z wojną, natomiast Libicki akcentuje specyfikę odstraszenia i reagowania w cyberprzestrzeni. Polskie regulacje prawne wskazują na zadania Wojsk Obrony Cyberprzestrzeni w zakresie pełnego spektrum działań w cyberprzestrzeni oraz ochrony zasobów kluczowych z punktu widzenia Sił Zbrojnych RP. Z punktu widzenia zasobów kadrowych oznacza to potrzebę pozyskiwania talentów niezależnie od płci, wieku czy tradycyjnych wyobrażeń o profilu żołnierza (Libicki 2009; Rid 2013; NATO 2021; Rzeczpospolita Polska 2022).

Zagrożenia cyfrowe istotne dla wojska, Policji i Straży Granicznej mają charakter wielowymiarowy. Nie ograniczają się do ataków na serwery lub sieci, lecz obejmują manipulację informacyjną, socjotechnikę, oszustwa finansowe, wycieki danych, cyberprzestępczość transgraniczną, naruszenia ciągłości działania oraz działania sponsorowane przez państwa. Dla służb mundurowych oznacza to konieczność tworzenia zespołów łączących kompetencje techniczne z rozumieniem prawa, psychologii sprawcy, międzynarodowej wymiany informacji, języków obcych, analizy danych i zarządzania kryzysowego. Badania nad czynnikiem ludzkim w bezpieczeństwie wskazują, że użytkownicy i personel organizacji nie powinni być postrzegani wyłącznie jako „najsłabsze ogniwo”, lecz jako część systemu

bezpieczeństwa, który wymaga właściwego projektowania procedur, edukacji i kultury organizacyjnej (Adams i Sasse 1999; ENISA 2024; Parlament Europejski i Rada UE 2022).

W Policji najważniejszą instytucjonalną zmianą było utworzenie Centralnego Biura Zwalczania Cyberprzestępczości. Do jego zadań należy rozpoznawanie i zwalczanie przestępstw popełnionych przy użyciu systemów informatycznych, systemów teleinformatycznych lub sieci teleinformatycznych, zapobieganie takim przestępstwom oraz wykrywanie i ściganie ich sprawców. Badania nad cyberprzestępczością wskazują, że technologia przekształca zarówno formy popełniania czynów zabronionych, jak i sposoby ich wykrywania. Wall podkreśla transformacyjny wpływ technologii informacyjnych na przestępczość, natomiast Yar i Steinmetz opisują cyberprzestępczość jako zjawisko obejmujące zarówno przestępstwa przeciwko systemom, jak i przestępstwa wykorzystujące technologie do oszustw, przemocy, eksploatacji danych i naruszania prywatności. Ten zakres zadań wymaga kompetencji śledczych i technicznych: analizy śladów cyfrowych, zabezpieczania dowodów elektronicznych, pracy z danymi, rozpoznawania schematów oszustw i współpracy z podmiotami prywatnymi (Wall 2007; Casey 2011; Yar i Steinmetz 2019; CBZC b.d.).

Informatyka śledcza jest szczególnie istotnym obszarem, w którym role kobiet mogą być rozwijane w służbach mundurowych na równi z rolami mężczyzn. Casey wskazuje, że dowody cyfrowe wymagają zachowania integralności, właściwego dokumentowania czynności, rozumienia ograniczeń technologii oraz ścisłego związku między procedurą techniczną i procesową. Oznacza to, że kompetencje potrzebne w cyberdochodzeniach nie ograniczają się do obsługi narzędzi informatycznych. Obejmują także precyzję analityczną, znajomość procedur, odporność na presję, umiejętność współpracy z prokuraturą i biegłymi oraz zdolność przedstawiania ustaleń w sposób zrozumiały dla decydentów i sądu (Casey 2011; CBZC b.d.).

W Straży Granicznej cyberbezpieczeństwo wiąże się nie tylko z ochroną własnych systemów informatycznych, lecz także z cyfryzacją kontroli granicznej. Rozwój systemów takich jak Entry/Exit System i ETIAS zmienia sposób zarządzania ruchem granicznym oraz zwiększa znaczenie interoperacyjności, przetwarzania danych i bezpieczeństwa informacji. Polskie przepisy dotyczące udziału Rzeczypospolitej Polskiej w Systemie Wjazdu/Wyjazdu przewidują m.in. możliwość przetwarzania przez Straż Graniczną danych biometrycznych w zakresie niezbędnym do identyfikacji lub weryfikacji tożsamości osoby. W praktyce wzmacnia to zapotrzebowanie na funkcjonariuszki i funkcjonariuszy posiadających kompetencje z zakresu bezpieczeństwa danych, ochrony prywatności, analizy ryzyka, obsługi złożonych systemów informacyjnych i reagowania na incydenty naruszające ciągłość procesów granicznych (Frontex 2025; Rzeczpospolita Polska 2024).

Drugim nurtem badań istotnym dla tematu artykułu jest problem niedostatecznej reprezentacji kobiet w zawodach cyfrowych. Eurostat podaje, że w 2024 roku

kobiety stanowiły 19,5% specjalistów ICT w Unii Europejskiej. Komisja Europejska wskazuje szerzej, że kobiety stanowią około jednej trzeciej absolwentów STEM i jedną piątą specjalistów ICT, mimo że tworzą większość populacji UE. W sektorze cyberbezpieczeństwa dane również pokazują dysproporcję: ISC2 szacuje, że kobiety stanowią średnio 22% zespołów bezpieczeństwa. Oznacza to, że służby mundurowe konkurują o specjalistki na rynku, który sam w sobie charakteryzuje się deficytem kobiet i niedoborem kadr. Literatura naukowa wiąże tę sytuację z czynnikami edukacyjnymi, kulturowymi i organizacyjnymi, a nie z brakiem zdolności kobiet do wykonywania zadań technicznych (Cheryan et al. 2017; Eurostat 2025; European Commission 2025; ISC2 2025).

Badania dotyczące edukacji i rynku pracy pokazują, że nierówności pojawiają się już na etapie kształtowania aspiracji edukacyjnych i zawodowych. Cheryan i współautorzy wskazują, że większe luki płciowe w informatyce, inżynierii i fizyce są powiązane m.in. z męską kulturą danej dziedziny, ograniczonymi wczesnymi doświadczeniami dziewcząt oraz stereotypami dotyczącymi tego, kto „pasuje” do zawodu technicznego. Moss-Racusin i współautorzy wykazali z kolei, że nawet w środowiskach akademickich mogą występować subtelne uprzedzenia faworyzujące kandydatów płci męskiej przy ocenie kompetencji i potencjału. W cyberbezpieczeństwie te mechanizmy mogą zniechęcać kobiety do wyboru ścieżki zawodowej, ograniczać dostęp do mentoringu oraz utrwalać przekonanie, że jest to obszar zarezerwowany dla wąsko rozumianych specjalistów technicznych (Moss-Racusin et al. 2012; Cheryan et al. 2017).

Nowsze badania dotyczące kobiet w cyberbezpieczeństwie potwierdzają, że luka płciowa ma charakter strukturalny. Peacock i Irons analizują bariery wejścia i awansu kobiet w branży cyberbezpieczeństwa, zwracając uwagę na znaczenie stereotypów, niedostatecznej widoczności ekspertek, braku wzorców ról oraz ograniczonego dostępu do sieci zawodowych. Kshetri i Chhetri wskazują, że asymetria płci w cyberbezpieczeństwie ma konsekwencje społeczno-ekonomiczne, ponieważ zmniejsza pulę dostępnych talentów i ogranicza różnorodność perspektyw w sektorze odpowiedzialnym za ochronę cyfrowych zasobów. Francis i współautorzy, analizując edukację cyberbezpieczeństwa, podkreślają znaczenie poczucia sprawczości, motywacji, wsparcia oraz doświadczeń praktycznych dla rozwijania kompetencji i trwałego zainteresowania tą dziedziną (Peacock i Irons 2017; Kshetri i Chhetri 2022; Francis et al. 2024).

Istotne znaczenie ma także sposób społecznego przedstawiania zawodów cyberbezpieczeństwa. Da Silva, analizując praktyki cyberbezpieczeństwa, opisuje zjawisko „cybermęskości”, w którym prestiż zawodowy bywa wiązany z figurą eksperta dominującego technicznie, działającego poza zwykłymi regułami organizacji i legitymizującego swoją pozycję hermetycznym językiem specjalistycznym. Taki obraz może ograniczać udział kobiet, ale również zawężać rozumienie kompetencji potrzebnych w cyberbezpieczeństwie. W służbach mundurowych problem ten może

być wzmacniany przez hierarchiczność, kulturę dyspozycyjności oraz tradycyjne wyobrażenia o zawodach związanych z bezpieczeństwem (Da Silva 2023).

Trzeci nurt dotyczy kobiet w formacjach wojskowych i szerzej w sektorze bezpieczeństwa. Carreiras, analizując udział kobiet w siłach zbrojnych państw zachodnich, wskazuje, że ich integracja zależy nie tylko od formalnego dostępu do służby, lecz także od realnego dostępu do specjalizacji, awansu, prestiżowych zadań i struktur decyzyjnych. Sjöberg podkreśla, że płeć jest ważną kategorią analizy bezpieczeństwa i konfliktu, ponieważ wpływa na sposób definiowania zagrożeń, ról organizacyjnych oraz praktyk instytucjonalnych. W odniesieniu do cyberbezpieczeństwa służb mundurowych oznacza to, że nie wystarczy stwierdzić ogólny wzrost liczby kobiet w formacji. Konieczne jest pytanie, czy kobiety są obecne w zadaniach specjalistycznych, analitycznych i kierowniczych związanych z cyberobroną, cyberdochodzeniami oraz ochroną cyfrowej infrastruktury państwa (Carreiras 2006; Sjöberg 2013).

Czwarty nurt dotyczy wpływu różnorodności na jakość decyzji i funkcjonowanie zespołów. Badania nad zespołami wskazują, że różnorodność może zwiększać zasób perspektyw, pod warunkiem, że organizacja potrafi nią zarządzać i tworzy warunki rzeczywistego udziału w podejmowaniu decyzji. Woolley i współautorzy pokazali, że inteligencja zbiorowa grupy nie sprowadza się do średniej inteligencji indywidualnej jej członków, lecz jest związana między innymi ze społeczną wrażliwością i równomiernym udziałem w rozmowie. W cyberbezpieczeństwie ma to szczególne znaczenie, ponieważ analiza incydentu wymaga łączenia rozproszonych sygnałów, kwestionowania założeń, szybkiego formułowania hipotez i gotowości do uczenia się na podstawie niepełnych danych (van Knippenberg i Schippers 2007; Woolley et al. 2010).

W literaturze i dokumentach instytucjonalnych coraz częściej podkreśla się, że zwiększenie udziału kobiet w cyberbezpieczeństwie nie powinno być traktowane jako działanie wizerunkowe. ENISA w kampanii #CyberALL łączy różnorodność z lepszym podejmowaniem decyzji, innowacyjnością oraz atrakcyjnością ścieżek kariery w cyberbezpieczeństwie. Z kolei inicjatywy Komisji Europejskiej i Women4Cyber pokazują, że działania na rzecz większej obecności kobiet muszą obejmować edukację, sieciowanie, widoczność ról zawodowych, wsparcie początkujących specjalistek oraz współpracę z pracodawcami. W odniesieniu do służb mundurowych szczególnego znaczenia nabiera także kultura organizacyjna: hierarchia, dyspozycyjność, wymogi bezpieczeństwa, procedury dostępu do informacji i ścieżki awansu mogą zarówno wspierać, jak i ograniczać udział kobiet (ENISA b.d.; European Commission 2024; European Commission 2025).

Ocena dotychczasowego dorobku wskazuje na lukę badawczą. Dostępne opracowania opisują cyberbezpieczeństwo, cyberprzestępczość, kobiety w ICT albo kobiety w służbach mundurowych, lecz rzadziej analizują przecięcie tych obszarów. Brakuje zwłaszcza badań porównujących role kobiet w cyberbezpieczeństwie wojska, policji i straży granicznej oraz badań empirycznych pokazujących, w jakich zadaniach

specjalistycznych kobiety faktycznie uczestniczą. Niniejszy artykuł wypełnia tę lukę poprzez zestawienie mandatów instytucjonalnych, typów zadań cyberbezpieczeństwa, kompetencji oraz barier organizacyjnych charakterystycznych dla trzech formacji (Carreiras 2006; Peacock i Irons 2017; Kshetri i Chhetri 2022; Eurostat 2025; ISC2 2025; Policja 2024; Straż Graniczna 2024; Wojsko Polskie b.d.).

Metodyka badań

Badanie ma charakter jakościowy, eksploracyjno-porównawczy i problemowo ukierunkowany. Jego konstrukcja została podporządkowana problemowi badawczemu sformułowanemu we wstępie, tj. ustaleniu, w jaki sposób udział kobiet wpływa na rozwój zdolności cyberbezpieczeństwa w służbach mundurowych. Nie analizowano zatem wyłącznie ogólnej liczebności kobiet w formacjach, lecz przede wszystkim relację między zadaniami cyberbezpieczeństwa, wymaganymi kompetencjami, możliwymi rolami zawodowymi oraz barierami ograniczającymi wykorzystanie potencjału kadr kobiecych. Takie ujęcie pozwalało traktować udział kobiet nie jako kategorię statystyczną, lecz jako zmienną organizacyjną powiązaną z odpornością, jakością analizy zagrożeń i skutecznością reagowania na incydenty (van Knippenberg i Schippers 2007; Woolley et al. 2010; OECD 2024).

Problem główny został doprecyzowany przez cztery pytania szczegółowe. Po pierwsze, jakie obszary cyberbezpieczeństwa są szczególnie istotne dla wojska, Policji i Straży Granicznej? Po drugie, jakie kompetencje techniczne, analityczne, prawne, komunikacyjne i organizacyjne są wymagane w tych obszarach? Po trzecie, w jakich rolach kobiety mogą realnie wzmacniać zdolności cyberbezpieczeństwa poszczególnych formacji? Po czwarte, jakie bariery edukacyjne, kulturowe i instytucjonalne utrudniają przejście od formalnej obecności kobiet w służbach do ich rzeczywistego udziału w zadaniach specjalistycznych i decyzyjnych? Takie rozbieżności problemu badawczego umożliwiło powiązanie części empiryczno-analitycznej artykułu bezpośrednio z hipotezą, a nie jedynie z ogólną charakterystyką kobiet w formacjach mundurowych.

Hipotezę badawczą zoperacjonalizowano w czterech wymiarach analitycznych. Pierwszy wymiar dotyczył potencjału analitycznego, rozumianego jako zdolność zespołu do identyfikowania nietypowych wzorców, formułowania hipotez i pracy na rozproszonych danych. Drugi wymiar obejmował odporność organizacyjną, czyli zdolność formacji do utrzymania ciągłości działania, uczenia się po incydentach i ograniczania zależności od wąskiej grupy specjalistów. Trzeci wymiar odnosił się do skuteczności reagowania na incydenty, obejmującej koordynację techniczną, prawną, dowodową i komunikacyjną. Czwarty wymiar dotyczył warunków systemowych: rekrutacji, szkolenia, awansu, retencji oraz widoczności ekspertek. Przyjęto,

że hipoteza może zostać uznana za potwierdzoną warunkowo wtedy, gdy analiza wykaże zgodność między potrzebami operacyjnymi formacji a rolami, w których kobiety mogą wzmacniać zdolności cyberbezpieczeństwa, przy jednoczesnym wskazaniu barier ograniczających pełne wykorzystanie tego potencjału.

Zastosowano trzy powiązane metody: analizę dokumentów, przegląd literatury oraz analizę porównawczą. Analiza dokumentów objęła akty prawne, dokumenty strategiczne, informacje instytucjonalne i raporty międzynarodowe dotyczące cyberbezpieczeństwa, udziału kobiet w technologiach cyfrowych oraz zadań formacji mundurowych. Przegląd literatury służył identyfikacji ustaleń na temat różnorodności zespołów, deficytu kobiet w ICT, specyfiki pracy w cyberbezpieczeństwie, cyberprzestępczości, informatyki śledczej i wojskowego wymiaru cyberprzestrzeni. Analiza porównawcza pozwoliła zestawić trzy formacje według jednolitych kryteriów, przy zachowaniu odmienności ich mandatów ustawowych i praktyk operacyjnych (Rzeczpospolita Polska 2018; ENISA 2024; OECD 2024).

Dobór źródeł miał charakter celowy i wynikał z potrzeby triangulacji perspektyw. Uwzględniono źródła normatywne i instytucjonalne, ponieważ określają one mandat działania wojska, Policji i Straży Granicznej. Wykorzystano również raporty ENISA, Eurostatu, ISC2, OECD i Komisji Europejskiej, ponieważ opisują aktualne trendy w zakresie cyberzagrożeń, kompetencji cyfrowych i udziału kobiet w sektorze ICT. W części dotyczącej Policji wykorzystano materiały Centralnego Biura Zwalczania Cyberprzestępczości, natomiast w części dotyczącej Straży Granicznej - dokumenty odnoszące się do cyfryzacji granic, danych biometrycznych oraz planu równości płci. Źródła te zestawiono z literaturą naukową dotyczącą cyberbezpieczeństwa, cyberprzestępczości, różnorodności zespołów oraz kobiet w sektorze bezpieczeństwa, aby uniknąć jednostronnego ujęcia problemu wyłącznie w kategoriach prawnych albo wyłącznie społecznych (ENISA 2024; Eurostat 2025; ISC2 2025; OECD 2024; European Commission 2025).

Materiał badawczy kodowano według kategorii odpowiadających treści hipotezy. W odniesieniu do każdej formacji identyfikowano: mandat instytucjonalny, dominujące typy zagrożeń, rodzaje czynności cyberbezpieczeństwa, wymagane kompetencje, możliwe role kobiet, bariery wejścia i awansu oraz mechanizmy wsparcia organizacyjnego. Szczególną uwagę zwracano na to, czy dana rola ma charakter techniczny, analityczny, śledczy, koordynacyjny, edukacyjny czy kierowniczy. Pozwoliło to odróżnić ogólną obecność kobiet w formacji od ich udziału w zadaniach bezpośrednio wpływających na rozwój zdolności cyberbezpieczeństwa.

Procedura badawcza składała się z pięciu etapów. W pierwszym etapie zidentyfikowano zadania cyberbezpieczeństwa właściwe dla każdej formacji. W drugim etapie przyporządkowano tym zadaniom potencjalne role zawodowe, takie jak analityk cyberzagrożeń, specjalista bezpieczeństwa systemów, informatyk śledczy, analityk danych, koordynator zarządzania ryzykiem, specjalista ochrony informacji

lub edukator cyberbezpieczeństwa. W trzecim etapie określono bariery udziału kobiet, korzystając z literatury dotyczącej rynku ICT, różnorodności i służb mundurowych. W czwartym etapie zestawiono role i bariery z wymiarami hipotezy, tj. potencjałem analitycznym, odpornością organizacyjną i skutecznością reagowania. W piątym etapie sformułowano wnioski i rekomendacje odnoszące się do rekrutacji, szkolenia, retencji i awansu (CBZC b.d.; Rzeczpospolita Polska 2022; Rzeczpospolita Polska 2024).

Kryteriami porównania były: mandat instytucjonalny, dominujący typ zagrożeń, charakter czynności cyberbezpieczeństwa, kluczowe kompetencje, możliwe role kobiet, bariery oraz rekomendowane mechanizmy wsparcia. Wojsko analizowano przede wszystkim z punktu widzenia cyberobrony, ochrony systemów dowodzenia i działań w domenie cyberprzestrzeni. Policję analizowano przez pryzmat zwalczania cyberprzestępczości, informatyki śledczej, zabezpieczania dowodów cyfrowych i prewencji. Straż Graniczną analizowano w odniesieniu do cyfrowej kontroli granicznej, ochrony danych, interoperacyjności systemów i ryzyka transgranicznego. Zastosowanie tych samych kryteriów pozwala uniknąć prostego porównywania liczebności kobiet w formacjach, które mają odmienne zadania, strukturę organizacyjną i poziom jawności danych (van Knippenberg i Schippers 2007; ENISA 2024; OECD 2024).

Weryfikacja hipotezy miała charakter jakościowy, a nie statystyczny. Oceniano, czy zebrany materiał pozwala wykazać logiczny związek między udziałem kobiet a rozwojem zdolności cyberbezpieczeństwa, a także czy związek ten ma charakter bezpośredni czy pośredni. Za bezpośredni uznano udział kobiet w zadaniach technicznych, analitycznych, śledczych i koordynacyjnych. Za pośredni uznano wpływ na kulturę organizacyjną, edukację cyberbezpieczeństwa, komunikację ryzyka, mentoring i retencję kompetencji. Tak rozumiana weryfikacja nie polegała na dowodzeniu przewagi jednej płci nad drugą, lecz na ocenie, czy usuwanie barier wobec kobiet może zwiększyć realny zasób kompetencji dostępnych dla formacji.

Ograniczeniem badania jest dostępność danych. Informacje dotyczące szczegółowej obsady stanowisk cyberbezpieczeństwa w służbach mundurowych, zwłaszcza w strukturach wojskowych, są z natury ograniczone ze względów bezpieczeństwa. Dlatego artykuł nie rekonstruuje pełnej statystyki personalnej, lecz analizuje role, kompetencje i mechanizmy organizacyjne możliwe do uchwycenia na podstawie jawnych dokumentów. Drugie ograniczenie dotyczy płci: kategoria ta jest analizowana jako czynnik organizacyjny i społeczny, nie zaś jako automatyczny wyznacznik kompetencji. W artykule przyjęto założenie, że kluczowym kryterium obsady stanowisk pozostają kwalifikacje, a celem polityk równościowych jest usuwanie barier ograniczających dostęp do rozwoju zawodowego. Trzecie ograniczenie wynika z eksploracyjnego charakteru badania: ustalenia należy traktować jako podstawę do dalszych badań empirycznych, obejmujących wywiady, analizę przebiegu karier

i ocenę programów szkoleniowych (Wojsko Polskie b.d.; Policja 2024; Straż Graniczna 2024).

Wyniki

Analiza potwierdza, że cyberbezpieczeństwo w służbach mundurowych ma charakter zróżnicowany instytucjonalnie. W wojsku dominuje logika ochrony zdolności operacyjnych i prowadzenia działań w cyberprzestrzeni. W Policji najważniejsze jest rozpoznawanie, zapobieganie i zwalczanie czynów zabronionych popełnianych z użyciem technologii teleinformatycznych. W Straży Granicznej cyberbezpieczeństwo łączy ochronę własnych systemów z cyfrową obsługą procesów granicznych i przetwarzaniem wrażliwych danych, w tym danych biometrycznych. W odniesieniu do problemu badawczego oznacza to, że wpływ udziału kobiet na rozwój zdolności cyberbezpieczeństwa należy rozpatrywać przez trzy mechanizmy: poszerzenie puli specjalistycznych kompetencji, zwiększenie różnorodności perspektyw w analizie zagrożeń oraz wzmocnienie ciągłości organizacyjnej przez lepszą rekrutację i retencję talentów (Rzeczpospolita Polska 2022; CBZC b.d.; Frontex 2025; Rzeczpospolita Polska 2024).

Tabela 1. Role kobiet w formacjach mundurowych w zakresie cyberbezpieczeństwa

Formacja	Dominujące zadania cyberbezpieczeństwa	Przykładowe role kobiet
Wojsko	Ochrona systemów dowodzenia i łączności, aktywna obrona zasobów cyberprzestrzeni, analiza kampanii APT, zarządzanie podatnościami, wsparcie operacji i ciągłości działania.	analityczka cyberzagrożeń, specjalistka SOC, kryptolożka, administratorka systemów, specjalistka zarządzania podatnościami, koordynatorka reagowania
Policja	Rozpoznawanie i zwalczanie cyberprzestępczości, informatyka śledcza, zabezpieczanie dowodów cyfrowych, analiza oszustw internetowych, OSINT i działania prewencyjne.	funkcjonariuszka CBZC, analityczka OSINT, specjalistka informatyki śledczej, analityczka oszustw internetowych, edukatorka cyberprewencji
Straż Graniczna	Ochrona systemów granicznych, analiza danych, obsługa systemów biometrycznych, bezpieczeństwo informacji, zarządzanie ryzykiem transgranicznym i współpraca międzynarodowa.	specjalistka ochrony danych, analityczka ryzyka, administratorka systemów granicznych, koordynatorka wymiany informacji, specjalistka ciągłości działania

Źródło: Opracowanie własne na podstawie: Libicki 2009; Singer i Friedman 2014; NATO 2021; Rzeczpospolita Polska 2022; Wall 2007; Casey 2011; Yar i Steinmetz 2019; CBZC b.d.; Frontex 2025; Rzeczpospolita Polska 2024; von Solms i van Niekerk 2013; ENISA 2024; Furnell 2021; Carreiras 2006; Peacock i Irons 2017; Kshetri i Chhetri 2022; Woolley et al. 2010; OECD 2024

Poniższe zestawienie ma charakter syntetyczny i nie stanowi statystyki personalnej. Jego celem jest pokazanie, w których obszarach zadaniowych udział kobiet może bezpośrednio przekładać się na zdolności operacyjne, analityczne i organizacyjne formacji. Takie ujęcie odpowiada hipotezie, zgodnie z którą znaczenie kobiet w cyberbezpieczeństwie nie ogranicza się do wymiaru równościowego, lecz obejmuje praktyczne wzmocnienie procesów rozpoznawania, ochrony, dochodzenia i reagowania.

Pierwszy wynik dotyczy bezpośredniej odpowiedzi na problem badawczy. Udział kobiet wpływa na rozwój zdolności cyberbezpieczeństwa wtedy, gdy kobiety są włączane w role specjalistyczne, a nie wyłącznie w zadania administracyjne lub pomocnicze. W analizowanych formacjach można wyróżnić co najmniej sześć grup ról: techniczne, analityczne, śledcze, prawno-proceduralne, koordynacyjne oraz edukacyjno-komunikacyjne. W każdej z nich kobiety mogą uczestniczyć w procesach istotnych dla wykrywania zagrożeń, ochrony systemów, dokumentowania incydentów, komunikowania ryzyka i budowania odporności użytkowników. Tym samym znaczenie kobiet nie wynika z przypisywania im stałych cech płciowych, lecz z faktu, że ich szerszy udział zwiększa pulę kompetencji dostępnych dla organizacji (Furnell 2021; OECD 2024; ISC2 2025).

Drugi wynik dotyczy Sił Zbrojnych RP. W wymiarze wojskowym udział kobiet może wzmacniać zdolności cyberbezpieczeństwa przede wszystkim przez zwiększenie zasobu specjalistów zdolnych do ochrony systemów dowodzenia, analizy kampanii cybernetycznych, monitorowania podatności, zarządzania incydentami i wsparcia procesów decyzyjnych. W tym obszarze szczególnie istotne są role analityczek cyberzagrożeń, specjalistek SOC, administratorów systemów, kryptologów, specjalistek zarządzania podatnościami oraz koordynatorek reagowania. Udział kobiet może więc oddziaływać na odporność organizacyjną wojska nie przez sam fakt zwiększenia reprezentacji, lecz przez włączenie do zadań, które mają znaczenie dla ciągłości działania, ochrony informacji i przewagi decyzyjnej w cyberprzestrzeni (Libicki 2009; NATO 2021; Rzeczpospolita Polska 2022).

Trzeci wynik odnosi się do Policji. W zwalczaniu cyberprzestępczości szczególne znaczenie ma połączenie kompetencji technicznych, śledczych i komunikacyjnych. Kobiety mogą wzmacniać ten obszar jako funkcjonariuszki prowadzące czynności w sprawach cyberprzestępstw, specjalistki informatyki śledczej, analityczki OSINT, analityczki oszustw internetowych oraz osoby projektujące działania prewencyjne. Z punktu widzenia hipotezy kluczowe jest to, że cyberdochodzenia wymagają nie tylko znajomości narzędzi informatycznych, ale również precyzyjnego dokumentowania czynności, rozumienia procedury karnej, pracy z ofiarami, współpracy z prokuraturą i zdolności przedstawiania ustaleń w sposób zrozumiały dla decydentów. Włączenie kobiet w te role może poszerzać zdolność Policji do reagowania na zjawiska, w których komponent techniczny łączy się z psychologią sprawcy, ekonomią oszustwa i ochroną pokrzywdzonych (Wall 2007; Casey 2011; Yar i Steinmetz 2019; CBZC b.d.).

Czwarty wynik dotyczy Straży Granicznej. W tej formacji cyberbezpieczeństwo jest ściśle powiązane z cyfryzacją kontroli granicznej, interoperacyjnością systemów, przetwarzaniem danych osobowych i biometrycznych oraz wymianą informacji z partnerami krajowymi i zagranicznymi. Role kobiet mogą koncentrować się na ochronie danych, analizie ryzyka, administrowaniu systemami granicznymi, zarządzaniu ciągłością działania, audycie bezpieczeństwa informacji i koordynacji współpracy transgranicznej. Udział kobiet może wzmacniać zdolności formacji szczególnie tam, gdzie incydent cyberbezpieczeństwa wpływa jednocześnie na ciągłość odpraw, ochronę prywatności, zaufanie do systemów państwa oraz bezpieczeństwo obywateli i cudzoziemców (Frontex 2025; Rzeczpospolita Polska 2024; Straż Graniczna 2024).

Piąty wynik dotyczy jakości analizy zagrożeń. W każdej z analizowanych formacji cyberbezpieczeństwo wymaga pracy na niepełnych, niejednoznacznych i dynamicznie zmieniających się danych. Zespoły muszą rozpoznawać anomalie, oceniać wiarygodność źródeł, łączyć ślady techniczne z kontekstem organizacyjnym oraz kwestionować własne założenia. Różnorodność zespołów, w tym większy udział kobiet, może ograniczać ryzyko myślenia grupowego i zwiększać zakres perspektyw używanych przy analizie incydentów. Ustalenie to potwierdza część hipotezy dotyczącą jakości analizy zagrożeń, ale z istotnym zastrzeżeniem: korzyści pojawiają się wtedy, gdy kobiety mają realny udział w diagnozie problemu i procesie decyzyjnym, a nie jedynie formalną obecność w strukturze organizacyjnej (van Knippenberg i Schippers 2007; Woolley et al. 2010).

Szósty wynik dotyczy skuteczności reagowania na incydenty. Reagowanie w cyberbezpieczeństwie obejmuje działania techniczne, prawne, komunikacyjne i organizacyjne. W praktyce oznacza to konieczność współpracy administratorów, analityków, dowódców lub przełożonych, prawników, rzeczników, funkcjonariuszy prowadzących czynności procesowe oraz partnerów zewnętrznych. Kobiety uczestniczące w takich zespołach mogą wzmacniać nie tylko samą warstwę techniczną reagowania, lecz także dokumentowanie incydentu, komunikację z użytkownikami, koordynację działań oraz analizę skutków organizacyjnych. Ten wynik rozwija hipotezę w kierunku bardziej precyzyjnego wniosku: skuteczność reagowania zależy od komplementarności kompetencji, a większy udział kobiet jest jednym ze sposobów poszerzenia tej komplementarności.

Siódmy wynik dotyczy barier ograniczających potwierdzenie hipotezy w praktyce. Najważniejsze bariery mają charakter systemowy: niski udział kobiet w edukacji technicznej, stereotypowe postrzeganie cyberbezpieczeństwa jako domeny męskiej, niewielka widoczność ekspertek, trudności w łączeniu wymogów służby z życiem prywatnym, brak formalnych programów mentoringowych i ograniczona transparentność ścieżek awansu. W służbach mundurowych dochodzą czynniki specyficzne: hierarchiczność organizacji, wymagania dyspozycyjności, procedury kwalifikacyjne, dostęp do informacji niejawnych oraz konieczność utrzymywania

gotowości do działania. Bariery te nie podważają hipotezy, lecz wskazują, że jej praktyczna realizacja wymaga wsparcia systemowego w rekrutacji, kształceniu, awansie i retencji (Ashcraft et al. 2016; European Commission 2025; OECD 2024; Straż Graniczna 2024).

Ósmy wynik stanowi syntetyczną ocenę hipotezy. Zebrany materiał pozwala uznać ją za potwierdzoną warunkowo. Potwierdzenie dotyczy tego, że udział kobiet może zwiększać potencjał analityczny i organizacyjny formacji mundurowych, wzmacniać interdyscyplinarność zespołów oraz poszerzać zasób kompetencji potrzebnych do reagowania na incydenty. Warunkowość wynika natomiast z faktu, że sam wzrost liczby kobiet nie gwarantuje poprawy zdolności cyberbezpieczeństwa. Decydujące znaczenie ma dopiero rzeczywiste włączenie kobiet w zadania techniczne, analityczne, śledcze i kierownicze, zapewnienie dostępu do specjalistycznych szkoleń, przejrzystych ścieżek awansu oraz mechanizmów retencyjnych. W tym sensie wyniki badań wzmacniają tezę, że polityka kadrowa w cyberbezpieczeństwie powinna być traktowana jako element budowania odporności państwa, a nie wyłącznie jako instrument realizacji zasady równego traktowania.

Dyskusja

Uzyskane wyniki potwierdzają hipotezę, że udział kobiet w cyberbezpieczeństwie służb mundurowych ma wymiar strategiczny. Cyberbezpieczeństwo jest obszarem, w którym deficyt kadr stanowi jedno z głównych ograniczeń rozwoju zdolności państwa. Jeżeli kobiety pozostają niedoreprezentowane w ICT i cyberbezpieczeństwie, państwo zawęży pulę talentów, z której mogą korzystać wojsko, Policja i Straż Graniczna. Z tego powodu działania na rzecz udziału kobiet nie powinny być opisywane wyłącznie językiem polityki równościowej. Są one również elementem zarządzania bezpieczeństwem i zasobami krytycznymi (Eurostat 2025; ISC2 2025; European Commission 2025).

W praktyce oznacza to konieczność zmiany sposobu rekrutacji. Służby mundurowe powinny komunikować, że cyberbezpieczeństwo obejmuje wiele ról, a nie tylko programowanie lub administrację sieciową. Dla części kandydatek atrakcyjne mogą być ścieżki związane z analizą danych, OSINT, informatyką śledczą, ochroną prywatności, audytem, zarządzaniem ryzykiem, edukacją i reagowaniem kryzysowym. Pokazanie tej różnorodności obniża barierę wejścia i pozwala dotrzeć do osób, które nie identyfikują się z wąsko rozumianym zawodem informatyka, mimo że posiadają kompetencje przydatne w cyberbezpieczeństwie (ENISA b.d.; European Commission 2024; OECD 2024).

Drugim obszarem jest kształcenie. WAT, uczelnie wojskowe, szkoły policyjne, ośrodki szkolenia Straży Granicznej i uczelnie cywilne mogą pełnić rolę pomostu między edukacją techniczną a praktyką służby. Szczególnie

wartościowe byłyby moduły łączące bezpieczeństwo systemów, prawo, analizę danych, psychologię sprawcy, bezpieczeństwo informacji i zarządzanie incydem. Włączenie kobiet w takie programy powinno zaczynać się wcześniej niż na etapie naboru do służby: poprzez konkursy, patronaty, koła naukowe, staże, programy stypendialne i współpracę z organizacjami promującymi kobiety w technologiach (Ashcraft et al. 2016; European Commission 2024; OECD 2024).

Trzecim obszarem jest retencja. Samo przyjęcie kobiet do służby lub zatrudnienie ich na stanowiskach związanych z cyberbezpieczeństwem nie wystarcza. Potrzebne są mechanizmy utrzymania specjalistek: mentoring, jasne kryteria awansu, dostęp do certyfikacji, możliwość pracy projektowej, ochrona przed marginalizacją i przeciwdziałanie stereotypom. W cyberbezpieczeństwie utrata doświadczonego specjalisty jest kosztowna, ponieważ wraz z odejściem znika wiedza o systemach, procedurach, incydentach i kulturze organizacyjnej. Retencja kobiet jest więc także działaniem na rzecz ciągłości instytucjonalnej (OECD 2024; ISC2 2025; Straż Graniczna 2024).

Czwartym obszarem jest pomiar. Publiczne dane o udziale kobiet w formacjach mundurowych są zwykle zagregowane i nie pozwalają ustalić, ile kobiet pracuje bezpośrednio przy cyberbezpieczeństwie, informatyce śledczej, ochronie systemów czy analizie danych. Zrozumiałe są ograniczenia wynikające z bezpieczeństwa informacji, jednak możliwe jest publikowanie danych zbiorczych bez ujawniania wrażliwych szczegółów. Monitorowanie udziału kobiet w szkoleniach, certyfikacjach, awansach i stanowiskach specjalistycznych umożliwiłoby ocenę czy polityka kadrowa rzeczywiście zwiększa dostęp do kluczowych ról. (Policja 2024; Wojsko Polskie b.d.; Straż Graniczna 2024).

Należy również wskazać ryzyko pozornych działań. Różnorodność nie poprawia efektywności automatycznie. Jeżeli kobiety są obecne w zespołach, ale nie mają wpływu na decyzje, nie otrzymują zadań rozwojowych albo są kierowane głównie do funkcji pomocniczych, potencjał różnorodności nie zostanie wykorzystany. Organizacja musi tworzyć warunki, w których kompetencje są rozpoznawane, a osoby z różnym doświadczeniem uczestniczą w diagnozie problemu, projektowaniu rozwiązań i ocenie ryzyka. Dotyczy to szczególnie sytuacji kryzysowych, gdy presja czasu może wzmacniać nieformalne hierarchie i stereotypy (van Knippenberg i Schippers 2007; Woolley et al. 2010).

Dyskusja prowadzi do wniosku, że kobiety w cyberbezpieczeństwie służb mundurowych należy postrzegać jako część szerszej transformacji formacji bezpieczeństwa. Wojsko, Policja i Straż Graniczna stają się organizacjami opartymi na danych, interoperacyjności i zdolności szybkiej adaptacji. W takich organizacjach przewagę osiąga nie ten podmiot, który utrzymuje tradycyjny obraz służby, lecz ten, który potrafi skutecznie pozyskać, wyszkolić i utrzymać ludzi o wysokich kompetencjach. Z tego punktu widzenia płeć nie powinna ograniczać dostępu do ról cyberbezpieczeństwa, a polityka kadrowa powinna aktywnie usuwać bariery wejścia i rozwoju (Rada Ministrów 2019; ENISA 2024; Parlament Europejski i Rada UE 2022).

Wnioski

Wyniki analizy stanowiły podstawę do sformułowania pięciu zasadniczych wniosków. Po pierwsze, cyberbezpieczeństwo jest integralną częścią bezpieczeństwa narodowego i obejmuje zadania realizowane przez różne formacje mundurowe. W wojsku dotyczy ochrony i prowadzenia działań w cyberprzestrzeni, w Policji - zwalczania cyberprzestępczości, a w Straży Granicznej - ochrony systemów i danych wspierających cyfrową kontrolę graniczną. Różnice te powodują, że udział kobiet należy analizować w odniesieniu do konkretnych kompetencji i zadań, a nie przez pryzmat jednolitego modelu służby (Rzeczpospolita Polska 2022; CBZC b.d.; Rzeczpospolita Polska 2024).

Po drugie, kobiety mogą pełnić pełne spektrum ról w cyberbezpieczeństwie służb mundurowych: od stanowisk technicznych, przez analityczne i śledcze, po koordynacyjne i kierownicze. Ich znaczenie wynika nie z przypisywania określonych cech płci, lecz z poszerzenia puli talentów i zwiększenia różnorodności doświadczeń dostępnych dla organizacji. W warunkach niedoboru specjalistów cyberbezpieczeństwa każda bariera ograniczająca udział kobiet działa na niekorzyść państwa (Eurostat 2025; ISC2 2025; OECD 2024).

Po trzecie, największe ograniczenia mają charakter systemowy. Dotyczą edukacji technicznej, stereotypów, niewystarczającej widoczności ekspertek, nieformalnych mechanizmów awansu oraz braku spójnych programów mentoringowych. Usunięcie tych barier wymaga działań długofalowych: współpracy z uczelniami, czytelnych ścieżek kariery, finansowania certyfikacji, wsparcia przełożonych i monitorowania danych kadrowych (Ashcraft et al. 2016; European Commission 2025; Straż Graniczna 2024).

Po czwarte, udział kobiet w cyberbezpieczeństwie powinien być elementem strategii odporności organizacyjnej. Zespoły zajmujące się cyberzagrożeniami muszą szybko uczyć się nowych technik ataku, kwestionować własne założenia i łączyć kompetencje techniczne z prawnymi, analitycznymi oraz komunikacyjnymi. Różnorodność może wspierać te procesy, o ile jest połączona z kulturą współpracy i realnym wpływem na decyzje (ENISA 2024; van Knippenberg i Schippers 2007; Woolley et al. 2010).

Po piąte, dalsze badania powinny obejmować dane empiryczne z formacji mundurowych: wywiady ze specjalistkami, analizę ścieżek kariery, ocenę programów szkoleniowych oraz porównanie praktyk rekrutacyjnych. Szczególnie potrzebne są badania pokazujące, jakie mechanizmy faktycznie zwiększają trwały udział kobiet w zadaniach specjalistycznych, a nie tylko w ogólnej strukturze zatrudnienia. Najważniejszym praktycznym przesłaniem artykułu jest to, że włączenie kobiet w cyberbezpieczeństwo nie jest dodatkiem do polityki kadrowej, lecz warunkiem pełniejszego wykorzystania zasobów niezbędnych do ochrony państwa w środowisku cyfrowym (OECD 2024; ENISA b.d.; European Commission 2024).

BIBLIOGRAFIA

1. Adams A., Sasse M.A., 1999. Users Are Not the Enemy. *Communications of the ACM*, 42(12), s. 40-46, DOI: 10.1145/322796.322806.
2. Ashcraft C., McLain B., Eger E., 2016. Women in Tech: The Facts. National Center for Women & Information Technology, <https://ncwit.org/resource/thefacts/>, [dostęp: 24 czerwca 2026].
3. Carreiras H., 2006. Gender and the Military: Women in the Armed Forces of Western Democracies. Routledge, London-New York.
4. Casey E., 2011. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd ed. Academic Press, Waltham.
5. CBZC, b.d. Zadania Centralnego Biura Zwalczenia Cyberprzestępczości, <https://cbzc.policja.gov.pl/bzc/o-cbzc/podstawowe-zadania/5,Zadania-Centralnego-Biura-Zwalczenia-Cyberprzestepczosci.html>, [dostęp: 24 kwietnia 2026].
6. Cheryan S., Ziegler S.A., Montoya A.K., Jiang L., 2017. Why Are Some STEM Fields More Gender Balanced Than Others? *Psychological Bulletin*, 143(1), s. 1-35, DOI: 10.1037/bul0000052.
7. Craigen D., Diakun-Thibault N., Purse R., 2014. Defining Cybersecurity. *Technology Innovation Management Review*, 4(10), s. 13-21, DOI: 10.22215/timreview/835.
8. Da Silva J., 2023. Protection, Expertise and Domination: Cyber Masculinity in Practice. *Computers & Security*, 133, 103408, DOI: 10.1016/j.cose.2023.103408.
9. Dunn Cavelty M., 2008. Cyber-Security and Threat Politics: US Efforts to Secure the Information Age. Routledge, London-New York.
10. ENISA, 2024. ENISA Threat Landscape 2024, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>, [dostęp: 24.04.2026].
11. ENISA, b.d. #CyberALL, <https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/raising-awareness-campaigns/cyberall>, [dostęp: 24 kwietnia 2026].
12. European Commission, 2024. EU Must Reinforce Cybersecurity Skills, <https://digital-strategy.ec.europa.eu/en/news/eu-must-reinforce-cybersecurity-skills>, [dostęp: 24.04.2026].
13. European Commission, 2025. Women in Digital, <https://digital-strategy.ec.europa.eu/en/policies/women-digital>, [dostęp: 24 kwietnia 2026].
14. Eurostat, 2025. Rising Share of ICT Specialists Among Employed People, <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20250708-2>, [dostęp: 24 kwietnia 2026].
15. Francis S.P., Kolil V.K., Pavithran V., Ray I., Achuthan K., 2024. Exploring Gender Dynamics in Cybersecurity Education: A Self-Determination Theory and Social Cognitive Theory Perspective. *Computers & Security*, 144, 103968, DOI: 10.1016/j.cose.2024.103968.
16. Frontex, 2025. Frontex Gears Up for Digital Transformation of Europe's Border Management, <https://www.frontex.europa.eu/media-centre/news/news-release/frontex-gears-up-for-digital-transformation-of-europe-s-border-management-ZdfPCW>, [dostęp: 24 kwietnia 2026].

17. Furnell S., 2021. The Cybersecurity Workforce and Skills. *Computers & Security*, 100, 102080, DOI: 10.1016/j.cose.2020.102080.
18. Hansen L., Nissenbaum H., 2009. Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, 53(4), s. 1155-1175, DOI: 10.1111/j.1468-2478.2009.00572.x.
19. ISC2, 2025. Women Comprise 22% of the Cybersecurity Workforce, <https://www.isc2.org/Insights/2025/03/Women-Comprise-22-percent-of-the-Cybersecurity-Workforce>, [dostęp: 24 kwietnia 2026].
20. Kshetri N., Chhetri M., 2022. Gender Asymmetry in Cybersecurity: Socioeconomic Causes and Consequences. *Computer*, 55(2), s. 72-77, DOI: 10.1109/MC.2021.3127992.
21. Libicki M.C., 2009. Cyberdeterrence and Cyberwar. RAND Corporation, Santa Monica.
22. Moss-Racusin C.A., Dovidio J.F., Brescoll V.L., Graham M.J., Handelsman J., 2012. Science Faculty's Subtle Gender Biases Favor Male Students. *Proceedings of the National Academy of Sciences*, 109(41), s. 16474-16479, DOI: 10.1073/pnas.1211286109.
23. NATO, 2021. Remarks by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference, <https://www.nato.int/en/news-and-events/events/transcripts/2021/06/07/remarks>, [dostęp: 24 kwietnia 2026].
24. OECD, 2024. The Potential of Women for Digital Innovation. OECD Digital Economy Outlook 2024, https://www.oecd.org/en/publications/oecd-digital-economy-outlook-2024-volume-2_3adf705b-en/full-report/the-potential-of-women-for-digital-innovation_83bc2ba5.html, [dostęp: 24 kwietnia 2026].
25. Parlament Europejski i Rada UE, 2022. Dyrektywa (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/pol>, [dostęp: 24 kwietnia 2026].
26. Peacock D., Irons A., 2017. Gender Inequality in Cybersecurity: Exploring the Gender Gap in Opportunities and Progression. *International Journal of Gender, Science and Technology*, 9(1), s. 25-44.
27. Policja, 2024. W polskiej Policji służy prawie 20 000 kobiet, <https://policja.pl/pol/aktualnosci/242648,W-polskiej-Policji-sluzy-prawie-20-000-kobiet.html>, [dostęp: 24 kwietnia 2026].
28. Rada Ministrów, 2019. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WMP20190001037>, [dostęp: 24 kwietnia 2026].
29. Rid T., 2013. *Cyber War Will Not Take Place*. Oxford University Press, Oxford.
30. Rzeczpospolita Polska, 2018. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2024 poz. 1077, <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20240001077>, [dostęp: 24 kwietnia 2026].
31. Rzeczpospolita Polska, 2022. Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny, Dz.U. 2022 poz. 655, <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20220000655/U/D20220655Lj.pdf>, [dostęp: 24 kwietnia 2026].

32. Rzeczpospolita Polska, 2024. Ustawa z dnia 18 października 2024 r. o udziale Rzeczypospolitej Polskiej w Systemie Wjazdu/Wyjazdu, Dz.U. 2024 poz. 1688, <https://www.bip.kgsg.strazgraniczna.pl/download/381/44227/Ustawazdnia18paздziernika2024roudzialeRzeczypospolitejPolskiejwSystemieWjazduWyj.pdf>, [dostęp: 24 kwietnia 2026].
33. Singer P.W., Friedman A., 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, New York.
34. Sjoberg L., 2013. *Gendering Global Conflict: Toward a Feminist Theory of War*. Columbia University Press, New York.
35. Straż Graniczna, 2024. Plan Równości Płci, https://www.strazgraniczna.pl/download/1/37474/Plan_Rownosci_Plci__wersja_elektroniczna_.pdf, [dostęp: 24 kwietnia 2026].
36. van Knippenberg D., Schippers M.C., 2007. Work Group Diversity. *Annual Review of Psychology*, 58, s. 515-541, DOI: 10.1146/annurev.psych.58.110405.085546.
37. von Solms R., van Niekerk J., 2013. From Information Security to Cyber Security. *Computers & Security*, 38, s. 97-102, DOI: 10.1016/j.cose.2013.04.004.
38. Wall D.S., 2007. *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press, Cambridge.
39. Wojsko Polskie, b.d. Kobiety w armii. To już prawie 21 tys. żołnierzy zawodowych, <https://www.wojsko-polskie.pl/sgwp/articles/aktualnosci-w/kobiety-w-armii-to-juz-prawie-21-tys-zolnierzy-zawodowych/>, [dostęp: 24 kwietnia 2026].
40. Woolley A.W., Chabris C.F., Pentland A., Hashmi N., Malone T.W., 2010. Evidence for a Collective Intelligence Factor in the Performance of Human Groups. *Science*, 330(6004), s. 686-688, DOI: 10.1126/science.1193147.
41. Yar M., Steinmetz K.F., 2019. *Cybercrime and Society*, 3rd ed. SAGE Publications, London.