



Katarzyna Grabowska
NASK



CyberTalk, czyli cyberbezpieczeństwo oczami kobiet

dr hab. Aleksandra Gasztold
NASK, ACIG



Rozmowa z dr hab. Aleksandrą Gasztold, redaktorką naczelną Applied Cybersecurity & Internet Governance.

KG: Udział kobiet w obszarze cyberbezpieczeństwa i badań nad bezpieczeństwem – jak wygląda dziś?

Czy coś się zmienia?

AG: Liczba kobiet wchodzących zarówno do branży IT, jak i do badań nad cyberbezpieczeństwem systematycznie rośnie, choć różnice w reprezentacji wciąż pozostają znaczące. Wpływ mają czynniki rozwojowe, strukturalne i kulturowe, które kształtują ścieżki kariery kobiet oraz ich widoczność w środowisku eksperckim. Dlatego tak ważne są dalsze badania i działania wspierające równość płci oraz pełniejsze wykorzystanie potencjału kobiet w tej dziedzinie, na co zwracaliśmy uwagę

wspólnie z prof. Dorotą Domalewską i prof. Rubénem Arcosem w artykule Mapping the Role of Social Sciences in Cybersecurity Research (Studia Politologiczne 2025). Niezwykle ważna jest także i praktyka. Kierując czasopismem Applied Cybersecurity & Internet Governance przykładamy szczególną wagę do równościowej polityki publikacyjnej, nie wyobrażamy sobie, że można inaczej ale też chcemy dać przykład innym wydawcom, że patriarchat odszedł do lamusa. Warto podkreślić, że cyberbezpieczeństwo jest pojęciem niezwykle szerokim. Często praca edukacyjna, która jest związana ze wzmacnianiem kompetencji cyfrowych, budowaniem świadomości, prowadzeniem działań społecznych i kulturowych, pozostaje niezauważana lub nienależycie doceniana. To właśnie w tych obszarach są aktywne edukatorki.





CyberTalk, czyli cyberbezpieczeństwo oczami kobiet

Także w nauce to kobiety coraz częściej prowadzą badania nad polityką cyberbezpieczeństwa, cyberkulturą, dezinformacją, edukacją cyfrową czy społecznymi skutkami technologii. Wnoszą nowe perspektywy, interdyscyplinarność i prospołeczną wrażliwość, a przede wszystkim konsekwentnie umieszczają człowieka w centrum technologicznej debaty. Gdy spojrzymy na dynamikę ostatnich lat, to ta zmiana jest zauważalna. Rośnie odsetek publikacji tworzonych przez kobiety oraz zwiększa się ich udział w pracach zespołów SOC, w analizie incydentów i zagrożeń, a także w obszarach strategicznych i regulacyjnych. Mimo tego ich widoczność w świecie wciąż naznaczonym androcentrycznym myśleniem o bezpieczeństwie bywa ograniczana.

Można to wyraźnie zauważyć na panelach i wydarzeniach dotyczących obszaru cyber, techniki i technologii, na których dominują mężczyźni. A kiedy organizator twierdzi, że „w tym obszarze nie ma kobiet”, to oznacza jedynie, że nie poruszył nawet palcem po klawiaturze, by ich poszukać. Istnieje rozbudowana lista znakomitych ekspertek, która jasno pokazuje, że w tej dziedzinie nie brakuje kompetentnych kobiet.

KG: Jakie według Ciebie znaczenie ma mentoring w rozwoju kobiet w świecie cyber i nowych technologii?

AG: Mentoring ma w tej branży znaczenie absolutnie kluczowe. Cyberbezpieczeństwo jest środowiskiem szybko się zmieniającym, pełnym nowych narzędzi, nowych kompetencji i nierzadko wysokich barier wejścia. Mentorki i mentorzy pomagają te bariery obniżyć. W mojej





CyberTalk, czyli cyberbezpieczeństwo oczami kobiet

pracy w programie Mentoring Aktywnych Kobiet widzę trzy najważniejsze funkcje wsparcia rozwojowego. Po pierwsze: odwaga i widoczność. Kobiety, szczególnie rozpoczynające karierę, często mają kompetencje, ale nie mają pewności siebie. Mentoring pomaga „wejść do pokoju”, zabrać głos, budować pozycję. Po drugie: świadome planowanie kariery. Możliwość konsultacji 1:1 pomaga zobaczyć dłuższą perspektywę, staje się impulsem zmiany czy rozwoju, a także kształtuje cechy przywódcze. I ostatni filar: usieciowienie.

W cyberbezpieczeństwie relacje i wymiana wiedzy są bezcenne. Programy mentoringowe tworzą społeczności, które trwają długo po zakończeniu programu. Dodam tylko, że MAK skierowany jest do kobiet w różnym wieku, co wyróżnia go na tle wielu programów nastawionych na start

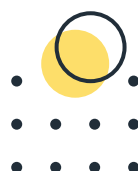
w branży.

Wierzymy, że wszelkie różnice nie stanowią barier a otwierają nowe perspektywy. Impulsem do tego otwarcia były działania podejmowane przez zespół NASK w ramach Europejskiego Miesiąca Cyberbezpieczeństwa.

KG: Jakie są wyzwania w badaniach i praktyce cyberbezpieczeństwa z perspektywy nauk społecznych?

AG: Cyberbezpieczeństwo stało się dziś jednym z kluczowych filarów bezpieczeństwa państwa, a dla nauk społecznych oznacza to pojawienie się nowych, wyjątkowo złożonych wyzwań zarówno badawczych, jak i praktycznych.

Dynamiczny rozwój rozwiązań cyfrowych zmienia rzeczywistość znacznie szybciej, niż potrafią nadążyć za nim język, prawo czy systemy edukacyjne. Dlatego badaczki i badacze muszą nie tylko rozumieć technologię, lecz przede wszystkim umieć tłumaczyć jej





CyberTalk, czyli cyberbezpieczeństwo oczami kobiet

konsekwencje społeczne, polityczne i kulturowe w tym precyzyjnie analizować nowe formy zagrożeń.

Jednym z najbardziej palących problemów, pozostaje narastająca skala dezinformacji, która eroduje zaufanie publiczne i podważa fundamenty instytucji demokratycznych.

To właśnie na styku technologii, komunikacji i procesów społecznych ujawnia się rola nauk społecznych jako kluczowego elementu budowania odporności państwa i społeczeństwa.

Drugim istotnym wyzwaniem jest konieczność ścisłej współpracy interdyscyplinarnej. Badania nad cyberbezpieczeństwem wymagają dziś wspólnej pracy socjologów i socjolożek, politologów i politolożek, specjalistów i specjalistek od bezpieczeństwa, inżynierów

i inżynierek, analityków i analityczek danych i ekspertów oraz ekspertek od sztucznej inteligencji. Takie podejście pozwala zrozumieć zarówno techniczne mechanizmy zagrożeń, jak i ich skutki dla zachowań społecznych, procesów decyzyjnych czy struktur władzy. Różnorodność nie jest tu dodatkiem, jest warunkiem skuteczności.

Równie ważnym obszarem pozostaje etyka i odpowiedzialność w obliczu rozwoju sztucznej inteligencji, automatyzacji oraz nowych sposobów pozyskiwania i przetwarzania danych.

Pytania o to, kto odpowiada za decyzje systemów algorytmicznych, jak zapewnić ochronę prywatności oraz jak równoważyć bezpieczeństwo z prawami jednostki, stają się centralnym wyzwaniem dla badaczek i praktyków.

Wszystkie te elementy łączy wspólna myśl –

EUROPEJSKI
MIESIĄC
CYBER
BEZPIECZEŃSTWA





CyberTalk, czyli cyberbezpieczeństwo oczami kobiet

cyberbezpieczeństwo to nie tylko domena technologii, ale przede wszystkim ludzi i struktur społecznych. Dlatego nauki społeczne są dziś niezbędnym komponentem zrozumienia, co kryje się pod tym pojęciem i kształtowania tego obszaru wiedzy współtworząc fundamenty bezpiecznego, odpornego i świadomego cyfrowo społeczeństwa. Zachęcam do korzystania z perspektywy skoncentrowanej na człowieku w ekosystemie cyfrowym, którą – jako trzy autorki – współtworzymy w książce *Humans in the Cyber Loop: Perspectives on Social Cybersecurity* (Domalewska, Gasztold, Wrońska, Brill 2025).

KG: Jak instytucje akademickie mogą skuteczniej wspierać rozwój kobiet w obszarach bezpieczeństwa i cyberprzestrzeni?

AG: Najlepsze rezultaty przynoszą działania, które w spójny sposób łączą infrastrukturę, wsparcie merytoryczne i świadomie kształtowaną kulturę organizacyjną. Niezwykle ważną rolę odgrywają tu programy mentoringowe i tutoring – regularne, systemowe, dostępne nie tylko dla najlepszych studentek, lecz także dla tych kobiet, które poszukują swojej ścieżki rozwoju. Równie istotna jest widoczność ekspertek. Panele, konferencje i publikacje muszą opierać się na zasadzie różnorodności, bo kobiety powinny być widoczne jako liderki i ekspertki. I nie jest to zadanie działów promocji, lecz element polityki równościowej uczelni oraz instytutów badawczych. Dopełnieniem tego ekosystemu jest wsparcie badań i grantów, w tym rozwiązania ułatwiające powrót po przerwach, na przykład związanych z macierzyństwem. Ważne są także międzynarodowe sieci i staże,





CyberTalk, czyli cyberbezpieczeństwo oczami kobiet

bo cyberbezpieczeństwo ma charakter globalny, a doświadczenie zagraniczne poszerza horyzonty i wzmacnia kompetencje. Wreszcie, konieczne jest budowanie silnych relacji z branżą. Ośrodki naukowe powinny aktywnie współpracować z instytucjami państwowymi, NASK oraz firmami analitycznymi i technologicznymi, tworząc środowisko, które realnie wspiera rozwój kobiet w cyberbezpieczeństwie.

KG: Czym dla Ciebie jest budowanie świadomości cyberbezpieczeństwa i jak prowadzić skuteczną edukację?

AG: Budowanie świadomości cyberbezpieczeństwa to przede wszystkim kształtowanie postawy odpowiedzialności cyfrowej, zarówno indywidualnej, jak i społecznej. Aby edukacja w tym obszarze była naprawdę skuteczna, potrzebujemy kilku

kluczowych elementów. Jednym z nich jest prostota przekazu. Cyberbezpieczeństwo nie jest hermetyczną dziedziną, a każdy powinien rozumieć, jak poruszać się w rzeczywistości cyfrowej. W dalszej kolejności ważna jest praktyka zamiast teorii – realne studia przypadków, symulacje incydentów. Ćwiczenia uczą więcej niż najobszerniejsze podręczniki. Kolejnym elementem jest promowanie rzetelnych liderów i liderek opinii.

Edukacja działa wtedy, gdy mówią o niej osoby cieszące się zaufaniem – ekspertki i eksperci, nauczyciele i nauczycielki, ale także rzetelni influencerzy i influencerki itd. Świadomość cyberbezpieczeństwa to proces kulturowy, a nie jednorazowa kampania, wymaga konsekwencji, powtarzalności i włączania różnych środowisk.

KG: Jakie kompetencje są kluczowe dla kobiet rozwijających się w obszarze bezpieczeństwa?





CyberTalk, czyli cyberbezpieczeństwo oczami kobiet

AG: Kluczowe kompetencje dla kobiet rozwijających się w obszarze bezpieczeństwa obejmują zarówno solidne fundamenty techniczne, jak i umiejętności analityczne pozwalające czytać dane, rozumieć trendy i precyzyjnie diagnozować problemy. Równie ważne są świetne zdolności komunikacyjne, gdyż w tej branży często trzeba przekładać złożone zagadnienia na język zrozumiały dla decydentów i decydek, zespołów czy społeczności. Niezbędne pozostają także odwaga i odporność psychiczna, które pomagają funkcjonować w dynamicznym, wymagającym i nierzadko stresującym środowisku, a także naturalna ciekawość technologiczna. Gotowość do uczenia się, testowania nowych rozwiązań i zmieniania kierunków. Kluczowym elementem jest sieć relacji i wsparcia, dzięki której zawodowa

droga w cyberbezpieczeństwie staje się nie tylko możliwa, ale i znacznie bogatsza. Odrobina dystansu do całego cyfrowego zamieszkania plus szczerzy zachwyt rzeczywistością offline, gdzie nikt nie prosi o aktualizację, również bardzo pomagają.

KG: Dziękuję za podzielenie się swoimi doświadczeniami i przemyśleniami.

Bezpieczeństwo zaczyna się od zrozumienia – a nauka łączy technologię z człowiekiem. To właśnie dzięki takim rozmowom widzimy, jak różnorodność perspektyw kształtuje przyszłość cyfrowego świata.

AG: Dziękuję!

