Anna Kwaśnik
NASK

CyberTalk, czyli cyberbezpieczeństwo oczami kobiet

Magdalena Wilczyńska
NASK

Rozmowa z Magdaleną Wilczyńską, Dyrektor Pionu Ochrony Informacyjnej Cyberprzestrzeni, NASK.

AK: Patrząc na Twoją drogę zawodową, jakie kompetencje okazały się kluczowe w pracy z bezpieczeństwem informacyjnym i dezinformacją – a których znaczenie doceniłaś dopiero z czasem?

MW: Moja ścieżka jest trochę nieoczywista – ale to typowe dla wielu analityków dezinformacji i ekspertów od cyberbezpieczeństwa. Zaczynałam od prawa i praw człowieka, szczególnie wolności słowa, by później przerzucić się z analiz prawnych na analizy danych. I okazało się, że dzięki dość szerokiemu oglądowi świata oraz dobremu rozumieniu procesów politycznych i demokratycznych analiza trendów i treści nie była dla mnie dużym wyzwaniem. To „łączenie kropek" bardzo przydało mi się później, również przy rozwijaniu kompetencji w analizie danych czy OSINT-cie. Twarde kompetencje analityczne przyszły z czasem – wcześniej znacznie ważniejsza była zdolność łączenia różnych perspektyw - prawnej, społecznej i technologicznej.

AK: Cyberbezpieczeństwo i bezpieczeństwo informacyjne łączy dziś wiele. Jakie umiejętności warto rozwijać na początku drogi – zwłaszcza jeśli ktoś nie ma technicznego wykształcenia, ale chce pracować w obszarze cyber?

MW: Rozwijać należy przede wszystkim ciekawość. Uważam, że w momencie, gdy do analiz – czy to w cyberbezpieczeństwie, czy w dezinformacji – podchodzimy rutynowo, tracimy cały fun z tej pracy. A także gubimy z pola widzenia potencjalnie istotne zagrożenia.

Oczywiście część tej pracy musi opierać się na wykrywaniu wzorców i zabezpieczaniu się przed nimi, ale dużo ważniejsze jest rozpoznawanie nowych ryzyk. Do tego potrzebna jest umiejętność zmiany perspektywy, wejścia w „nowe buty" i spojrzenia na te same dane z innej strony. W tej branży, zwłaszcza w przeciwdziałaniu dezinformacji, wciąż mamy wiele nierozwiązanych problemów. Dlatego warto uczyć się analizy treści, mechanizmów działania platform społecznościowych i podstaw algorytmów, ale także prawa, etyki oraz ochrony praw człowieka w sieci. Koniec końców to kompetencje w łączeniu różnych perspektyw mogą okazać się kluczowe.

W analizach dezinformacji często ważniejsze od twardych danych jest rozumienie państwa trzeciego, na przykład działań Rosji czy Chin, sytuacji geopolitycznej albo procesów unijnych. Można też specjalizować się obszarowo – wciąż brakuje ekspertów zajmujących się dezinformacją zdrowotną, klimatyczną, energetyczną czy migracyjną.

AK: Dezinformacja szybko się zmienia – dziś coraz częściej napędzają ją algorytmy i AI. Jak uczyć się i nadążać za tym światem, nie tracąc jednocześnie krytycznego myślenia i etycznej wrażliwości?

MW: Choć technologia się zmienia, same mechanizmy stojące za dezinformacją pozostają w dużej mierze niezmienne. Wciąż bazują na naszych błędach poznawczych, bezrefleksyjności w konsumpcji mediów i treści oraz na strachu przed innymi. Trzeba oczywiście śledzić nowe narzędzia i sposoby ich wykorzystywania, ale jednocześnie pamiętać, że fundamenty dezinformacji są stałe, jak gra na emocjach,

polaryzacja i podważanie zaufania.

Dla mnie kluczowe jest zachowanie równowagi między nadążaniem za technologią a nieuleganiem fascynacji nią.

AK: Dużą część swojej pracy poświęciłaś edukacji i wzmacnianiu odporności społecznej. Jakie kompetencje cyfrowe i informacyjne Twoim zdaniem warto rozwijać u młodych ludzi – ale też u dorosłych – by czuli się pewniej i bezpieczniej w sieci?

MW: Nie chcę powtarzać oklepanych stwierdzeń o konieczności edukacji medialnej czy o tym, że tzw. cyfrowi nomadzi wcale nie wiedzą, jak technologia działa. To oczywiście ważne – wiedza o tym, jak funkcjonują urządzenia, algorytmy i internet, powinna iść w parze z umiejętnością korzystania z tych technologii. Bardzo chciałabym jednak, aby równolegle z rozwijaniem kompetencji technologicznych kłaść silniejszy nacisk na uniezależnianie się od technologii. Na pielęgnowanie poczucia sprawczości - że możemy kształtować polityki dotyczące nowych technologii, reagować na scam, inicjować postępowania, ograniczać czas spędzany przy urządzeniach, ustalać zasady korzystania z mediów społecznościowych i oczekiwać etycznych rozwiązań.

AK: Jako kobieta-liderka w obszarze cyberbezpieczeństwa, jakie rady dałabyś kobietom, które myślą o pracy w tym obszarze, ale nie zawsze wierzą, że „to jest dla nich”?

MW: Kobietom myślącym o pracy w cyberbezpieczeństwie powiedziałabym przede wszystkim, że ten obszar naprawdę potrzebuje różnorodnych perspektyw. To nie jest świat

wyłącznie dla inżynierów. Choć w niektórych rolach kompetencje techniczne są kluczowe, cyberbezpieczeństwo daje też ogromne możliwości rozwoju obok tego nurtu. Dodałabym również, żeby nie bać się wchodzenia w obszary techniczne – nie zawsze są tak trudne i straszne, jak się wydaje. Wiele kobiet podchodzi do cyber z poczuciem, że muszą być perfekcyjnie przygotowane, zanim zrobią pierwszy krok, podczas gdy ten sektor w dużej mierze uczy się w praktyce. Warto szukać swojego miejsca i nie zniechęcać się stereotypami. Cyberbezpieczeństwo to nie tylko ochrona systemów, ale także ochrona ludzi, komunikacji, relacji społecznych i demokracji – a w tym kobiety od lat odgrywają kluczową rolę, nawet jeśli nie zawsze są wystarczająco widoczne.

AK: Dziękuję za inspirującą rozmowę!

MW: Dziękuję.