

Cybersecurity and Law

2025 Nr 2 (14)

DOI: 10.34567/cal/215573



The role of digital skills in the changing cybersecurity environment

Rola kompetencji cyfrowych w zmiennym środowisku cyberbezpieczeństwa

Paweł Rafał OSTOLSKI

Akademia Sztuki Wojennej

ORCID: 0000-0002-0728-6596

E-mail: p.ostolski@akademia.mil.pl

Abstract

The purpose of this article is to identify the key digital competencies that are essential for military and non-military entities to operate in a changing cybersecurity environment and to describe the role of this area of competence. Identifying the area of knowledge and skills in this field is the basis for systematically building resilience to cyber threats, which in today's digital world pose increasingly serious challenges to various organizations, governments, and even society as a whole.

Identifying digital competencies required a comparative analysis of selected literature and knowledge from online sources, as well as synthesis and the adoption of certain generalizations. An analogy with forecasting was also used to determine the development trends of digital competences in the perspective of 2030. The conclusions made it possible to include generalizing final statements in the summary.

The need to conduct research on the subject of scientific knowledge, which is digital competence, was justified using specific types of threats for this purpose. An analysis of the content of literature and online sources in the field of digital competence identification was carried out, and the results were presented for comparison and synthesis. Development trends were identified in accordance with the conditions observed in today's cyberspace. The growing role of digital competence in the changing cybersecurity environment was highlighted.

The role of digital competence is growing in proportion to technological development and social, economic, and political changes. Specialist knowledge and skills are essential for functioning effectively in the digital world. The use of computer technology permeates almost all spheres of human activity. A critical approach to the sources from which information is transmitted and to verifying its reliability is a priority. Cyber threats, information warfare, and disinformation require digital competence. Scientific achievements and government actions set trends in the development of digital competence.

Keywords

digital skills, cybersecurity, cyberspace

Streszczenie

Celem artykułu jest zidentyfikowanie kluczowych kompetencji cyfrowych, które są niezbędne do funkcjonowania podmiotów militarnych i niemilitarnych w zmiennym środowisku cyberbezpieczeństwa oraz deskrypcja roli tego obszaru kompetencyjnego. Wskazanie obszaru wiedzy i umiejętności w tym zakresie jest podstawą do systematycznego budowania odporności na zagrożenia cybernetyczne, które w dzisiejszym cyfrowym świecie stanowią coraz poważniejsze wyzwania dla różnych organizacji, rządów, a nawet całego społeczeństwa.

Identyfikacja kompetencji cyfrowych wymagała zastosowania analizy komparatystycznej wybranych treści literatury oraz wiedzy ze źródeł internetowych, a także dokonania syntezy i przyjęcia pewnych uogólnień. Posłużono się również analogią prognozowaniem, aby określić trendy rozwojowe kompetencji cyfrowych w perspektywie 2030 roku. Wnioskowanie umożliwiło zamieszczenie generalizujących konstatacji końcowych w podsumowaniu.

Uzasadniono potrzebę prowadzenia badań nad przedmiotem poznania naukowego, jaki stanowią kompetencje cyfrowe wykorzystując do tego celu określone rodzaje zagrożeń. Przeprowadzono analizę treści literatury i źródeł internetowych w zakresie identyfikacji kompetencji cyfrowych oraz przedstawiono je do porównania i syntezy. Wskazano trendy rozwojowe stosownie do uwarunkowań, które dostrzegane są w dzisiejszej cyberprzestrzeni. Wskazano wzrost roli kompetencji cyfrowych w zmiennym środowisku cyberbezpieczeństwa.

Rola kompetencji cyfrowych wzrasta proporcjonalnie do rozwoju technologicznego oraz przemian społecznych, gospodarczych i politycznych. Specjalistyczna wiedza i umiejętności są niezbędne do sprawnego funkcjonowania w świecie cyfrowym. Zastosowanie technologii komputerowych przenika niemal wszystkie sfery ludzkiej aktywności. Priorytetowym jest krytyczne podejście do źródeł z jakich przekazywane są informacje oraz do weryfikowania ich wiarygodności. Cyberzagrożenia oraz walka i wojna informacyjna wraz z dezinformacją wymagają kompetencji cyfrowych. Osiągnięcia naukowe i działania rządowe, wyznaczają trendy rozwoju kompetencji cyfrowych.

Słowa kluczowe

kompetencje cyfrowe, cyberbezpieczeństwo, cyberprzestrzeń

Wprowadzenie

Inspiracją do podjęcia badań w zakresie identyfikacji i roli kluczowych kompetencji cyfrowych, które mają szczególne znaczenie dla prawidłowego funkcjonowania poszczególnych podmiotów w systemie bezpieczeństwa państwa, było doświadczenie wielu zjawisk i faktów w zmiennym środowisku cyberbezpieczeństwa, jakie miały miejsce w przestrzeni uczelnianej Akademii Sztuki Wojennej, a także nasilających się działań dezinformacyjnych w polskiej sferze medialnej i nie tylko.

Tematyka ta nie była zbyt chętnie poruszana przez badaczy w mojej opinii, ze względu na pewną wrażliwość i delikatność podchodzenia, do niezbyt wygodnych kwestii braków kompetencyjnych, a nawet nieświadomości zachowań w trudnych sytuacjach, niosących ze sobą zagrożenia w sferze cyberbezpieczeństwa.

Zagrożenia te identyfikowali w swoich publikacjach ludzie nauki, którzy jednoznacznie wskazują na zwiększający się poziom ryzyka funkcjonowania

podmiotów w cyberprzestrzeni¹. Związane jest to z rozwojem stosowanych technik cyberprzestępczości oraz niskim poziomem świadomości zagrożeń pojawiających się w bardzo dynamicznie zmieniającym się środowisku cyberbezpieczeństwa przez osoby wykorzystujące w swojej działalności służbowej i prywatnej dostępne zasoby internetowe.

Znaczenie uświadomienia sobie na co jesteśmy narażeni, wchodząc w cyberprzestrzeń z naszą działalnością i funkcjonowaniem w świecie cyfrowym, akcentował G. Pilarski pisząc „(...) współcześnie bardzo istotnym zadaniem w zakresie cyberbezpieczeństwa, a może inaczej w zakresie przeciwdziałania cyberprzestępczości, jest podnoszenie świadomości nas wszystkich korzystających na co dzień z cyberprzestrzeni”². Przedstawia on również 15 najważniejszych rodzajów zagrożeń, które zostały zidentyfikowane przez specjalistów w raporcie Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa (ang. European Union Agency for Cybersecurity - ENISA), do których należą³:

1. Złośliwe oprogramowanie;
2. Ataki przez strony internetowe;
3. Phishing;
4. Ataki oparte na aplikacjach sieciowych;
5. Spam;
6. Atak typu DoS (ang. Denial of Service);
7. Kradzież tożsamości;
8. Naruszenie bezpieczeństwa danych;
9. Zagrożenie wewnętrzne;
10. Botnety;
11. Ingerencja fizyczna, uszkodzenie, kradzież i utrata;
12. Zagrożenie wycieku informacji;
13. Oprogramowanie typu ransomware;
14. Szpiegostwo w sieci;
15. Złośliwe wydobywanie kryptowalut (cryptojacking).

Oprócz tego zbioru zagrożeń, Autor zwraca uwagę czytelnika na różnorodność metod i technik ataków oraz wskazuje prognozowane tendencje rozwojowe i konieczność podejmowania działań prewencyjnych. Aby one były możliwe niewątpliwie wszystkim podmiotom militarnym i niemilitarnym, indywidualnym oraz instytucjonalnym, zapewnić musimy pożądany poziom kompetencji cyfrowych.

Potrzebę posiadania odpowiednich kwalifikacji personelu realizującego zadania w cyberprzestrzeni dostrzega G. Pilarski, który wymienia je, jako jeden z kluczowych elementów sukcesu: „(...) osiągnięcie sukcesu wymaga wielu działań uwzględniających kluczowe elementy, takie jak: infrastruktura technologiczna, wykwalifikowany personel, strategie i doktryny cyber wojenne, współpraca międzynarodowa i międzysektorowa, zastosowanie sztucznej

¹ Zob. P. Zaborowski, M. Kozłowski, Zastosowanie sztucznej inteligencji w rozwiązaniach cyberbezpieczeństwa, „Cybersecurity and Law” 2025, t. 1, nr 13, s. 126 oraz B. Farrand, H. Carrapico, A. Turobov, The new geopolitics of EU cybersecurity: security, economy and sovereignty, „International Affairs” 2024, t. 100, nr 6, s. 2380, a także Artificial Intelligence (AI) in Cybersecurity: The Future of Threat Defense, Fortinet, <https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity>, [dostęp: 24.11.2025].

² G. Pilarski, Przegląd współczesnych zagrożeń w cyberprzestrzeni, „Problemy techniki uzbrojenia” 2023, t. 167, nr 5, s. 98.

³ Ibidem, s. 98-100.

inteligencji i uczenia maszynowego, zdolności defensywne i ofensywne, środki prawne i regulacyjne, wywiad i analizy zagrożeń, ćwiczenia i symulacje”⁴.

Problematyka zwiększania zdolności defensywnych i ofensywnych poprzez budowanie pożądaných kompetencji dostrzegana jest również przez A. Bogdańskiego, który wskazuje zakres zagadnień cyberbezpieczeństwa w ćwiczeniach wojskowych, a szczególnie obrony przed cyberatakami i bezpiecznej wymiany informacji. Dodatkowo na podstawie badań własnych stwierdza, że tematyka ta nie jest realizowana systemowo i ogranicza się tylko do szkolenia doskonalącego⁵.

Zasadnym wydaje się podjęcie próby zdefiniowania kluczowych kompetencji cyfrowych, jakie powinny posiadać wszystkie podmioty realizujące zadania w podlegającym ciągłym dynamicznym zmianom środowisku cyberbezpieczeństwa. Taki cel badawczy generuje pytanie: Jakie kompetencje są kluczowe do właściwego funkcjonowania podmiotów militarnych i niemilitarnych w zmiennym środowisku cyberbezpieczeństwa?

Rozwiązanie tego problemu badawczego umożliwi przyjęcie następującej hipotezy: Właściwe funkcjonowanie podmiotów militarnych i niemilitarnych w zmiennym środowisku cyberbezpieczeństwa umożliwiają następujące kompetencje kluczowe „kompetencje informatyczne”, „kompetencje informacyjno-komunikacyjne” i „kompetencje funkcjonalne”.

Przeprowadzenie badań nad przedmiotem poznania naukowego, jakim są kompetencje cyfrowe wymagało zastosowania analizy komparatystycznej wybranych treści literatury i wiedzy ze źródeł internetowych, a następnie dokonania syntezy i przyjęcia pewnych uogólnień. Posłużono się również analogią i prognozowaniem⁶ w celu określenia trendów rozwojowych kompetencji cyfrowych w perspektywie czasowej pięciu lat.

Artykuł składa się z wprowadzenia oraz dwóch paragrafów. Pierwszy umiejscawia kompetencje cyfrowe wśród innych określonych w „Zaleceniu Rady z dnia 22 maja 2018 r. w sprawie kompetencji kluczowych w procesie uczenia się przez całe życie”⁷ oraz wskazuje zmiany w ich postrzeganiu po upływie 12 lat od 2006 roku. Drugi wskazuje zidentyfikowane kompetencje cyfrowe w różnych źródłach i podkreśla ich wzrastające znaczenie w dynamicznie zmieniającym się środowisku cyberbezpieczeństwa w perspektywie 2030 roku. Ostatnim elementem artykułu jest podsumowanie, w którym przedstawiono wnioski generalizujące i rekomendacje oraz sugestie w zakresie kierunków dalszych badań.

Kompetencje kluczowe w procesie uczenia się przez całe życie

Zrozumienie roli kompetencji cyfrowych, jaką odgrywają one w bezpiecznym funkcjonowaniu w cyberprzestrzeni, wymaga krótkiego wprowadzenia polegającego

⁴ G. Pilarski, Zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni, „Wiedza obronna” 2025, t. 292, nr 3, s. 130.

⁵ Zob. A. Bogdański, Good practices in military cybersecurity training, „Edukacyjna analiza transakcyjna” 2024, nr 13, s. 459.

⁶ Zob. M. Wrzosek, Zarządzanie wiedzą oficerów rozpoznania wojskowego, [w:] A. Szczygielska (red.), Organizacja systemu rozpoznania zagrożeń państwa. Zarządzanie wiedzą w podsystemie militarnym państwa, Warszawa 2022, s. 21.

⁷ Zalecenie Rady z dnia 22 maja 2018 r. w sprawie kluczowych kompetencji w zakresie uczenia się przez całe życie (Tekst mający znaczenie dla EOG), [https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32018H0604\(01\)](https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32018H0604(01)), [dostęp: 25.11.2025].

na przybliżeniu samego pojęcia „kompetencja”. Posłużę się w tym miejscu wynikami badań własnych, na podstawie których stwierdziłem, że może być ono rozumiane i definiowane w następujący sposób⁸:

- składnikiem kompetencji w starożytności było posiadanie cnót niezbędnych do właściwego wypełniania ról społecznych, politycznych, rodzinnych i zawodowych;
- według starożytnych Greków wiedza, jako cnota, stanowiła podstawę doświadczenia i nabywania umiejętności;
- Rzymianie przypisywali marginalne znaczenie wiedzy, ponieważ określali minimalne umiejętności niezbędne do wykonywania poszczególnych zawodów;
- średniowieczne myślenie o kompetencji charakteryzowało się zwiększeniem znaczenia wiedzy zawodowej, ale także wynikającej z rozwoju nauki i techniki;
- zgodnie z nurtem humanistycznym wiedza ogólna stanowiła podstawę budowania wszelkich kompetencji;
- kompetencje rozumiane są jako uprawnienia do określonych działań;
- dynamiczny rozwój nauki i techniki jest determinantem, który stymuluje wzrost liczby różnorodnych specjalizacji, w których podmiot podejmujący działania powinien posiadać preferowane właściwości;
- posiadanie pożądanых cech związanych z kompetencjami zawodowymi uważa się za główne źródło sukcesu;
- wiedza, umiejętności i postawy to składniki kompetencji w teorii zarządzania;
- umiejętność wykorzystania posiadanej wiedzy jest niezbędnym warunkiem realizacji zadań zawodowych;
- kompetencje są efektem właściwej realizacji procesu uczenia się;
- zdolność do realizacji różnorodnych zadań uzależniona jest od potencjału podmiotu, który jest podstawą kompetencji;
- behawiorystyczny instrumentalizm działania opiera się na kompetencjach, których składnikami są: wiedza, umiejętności, motywacja i samoocena;
- kompetencja jako struktura poznawcza integrująca celowo dobrane elementy i pozostająca w ciągłej interakcji z otoczeniem, jest koniecznym warunkiem zapewniającym ustawiczne jej doskonalenie.

Różnorodność stanowisk badawczych do tej kategorii uzależniona była na przestrzeni dziejów od kontekstów filozoficznych oraz rozwoju nauki i techniki, a także ewolucji dziedzin i dyscyplin naukowych.

Proces ten jest nieustannie kontynuowany oraz inspirowany ciągłymi zmianami otaczającej nas rzeczywistości, którą sami przekształcamy⁹. Każdy jest stymulowany do ciągłego adoptowania się w nowych uwarunkowaniach świata cyfrowego. Dlatego też wymagania kompetencyjne nigdy nie będą takie same, a z dużym prawdopodobieństwem można przyjąć założenie, że poziom kompetencji cyfrowych będzie się zwiększał proporcjonalnie do rozwoju nauki i techniki oraz technologii internetowych.

⁸ P. Ostolski, Dylematy przygotowania metodycznego nauczycieli akademickich, Warszawa 2020, s. 39-40.

⁹ Por. J. Ropski, Bezpieczeństwo edukacji w świecie VUCA, [w:] D. Kaźmierczak, J. Ropski, O. Wasiuta, W. Zakrzewski (red.), Edukacja w świecie VUCA, Szanse, Wyzwania, Zagrozenia, Kraków 2021, s. 56.

Potrzebna jest nam motywacja do zdobywania nowych zdolności poprzez wiedzę i umiejętności. Nie można beczynnie czekać, aż ktoś się nami zajmie, ponieważ działania w tym kierunku trzeba podejmować samodzielnie. Potwierdzeniem tego mogą być słowa G. Filipowicza, który pisze: „Jednym z podstawowych błędów, które możemy popełnić jako pracownicy, jest założenie, że to nasz pracodawca jest odpowiedzialny za rozwój naszych kompetencji, gdyż to on ma odpowiednie ku temu zasoby organizacyjne i finansowe”¹⁰. Potrzeba nam tylko trochę chęci do przełamania pewnego rodzaju oporu i poświęcenia własnego czasu. Wskazówkę do działania daje nam P. Korzyński, który w swojej monografii weryfikował hipotezę: „Pokonywanie ograniczeń motywacyjnych na platformach społecznościowych jest dodatnio skorelowane z czasem spędzonym na internetowych platformach społecznościowych”¹¹. Posługiwanie się narzędziami niezbędnymi do aktywnego uczestnictwa w świecie IT, stanowi bardzo ważny element kompetencyjny, który jest wymagany przez pracodawców oraz jest niezbędny w codziennym funkcjonowaniu jednostki społecznej.

Wyzwania w zakresie określenia obszarów kompetencyjnych są coraz intensywniejsze, a dowody na to odnajdujemy w dokumentach opracowanych w Unii Europejskiej. Pierwsze zalecenie¹² wydane zostało przez parlament europejski już w 2006 roku, a dotyczyło kompetencji kluczowych w procesie uczenia się przez całe życie. Zmienne uwarunkowania społeczne, techniczne, polityczne, prawne, ekonomiczne, fizyczne i kulturowe, jakie zachodziły w rozwijającej się Europie i na świecie – zainicjowały kolejną próbę zdefiniowania kompetencji kluczowych i w 2018 roku określono nieco zmieniony kolejny ich zbiór¹³. Zestawienie porównawcze kompetencji kluczowych w procesie uczenia się przez całe życie przedstawiono w tabeli 1.

Tabela 1. Zestawienie porównawcze kompetencji kluczowych w procesie uczenia się przez całe życie

Kompetencje kluczowe z 2006 r.	Kompetencje kluczowe z 2018 r.
porozumiewanie się w języku ojczystym	kompetencje w zakresie rozumienia i tworzenia informacji
porozumiewanie się w językach obcych	kompetencje w zakresie wielojęzyczności
kompetencje matematyczne i podstawowe kompetencje naukowo-techniczne	kompetencje matematyczne oraz kompetencje w zakresie nauk przyrodniczych, technologii i inżynierii
kompetencje informatyczne	kompetencje cyfrowe
umiejętność uczenia się	kompetencje osobiste, społeczne i w zakresie umiejętności uczenia się
kompetencje społeczne i obywatelskie	kompetencje obywatelskie

¹⁰ G. Filipowicz, Zarządzanie kompetencjami, perspektywa firmowa i osobista, Warszawa 2014, s. 329.

¹¹ P. Korzyński, Przywództwo w erze cyfrowej, Warszawa 2018, s. 81.

¹² Zob. Zalecenie parlamentu europejskiego i rady z dnia 18 grudnia 2006 r. w sprawie kompetencji kluczowych w procesie uczenia się przez całe życie, Bruksela 18 grudnia 2006 r., PE-CONS 3650/1/06 REV 1, <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32006H0962>, [dostęp: 26.11.2025].

¹³ Ibidem, s. 1.

inicjatywność i przedsiębiorczość	kompetencje w zakresie przedsiębiorczości
świadomość i ekspresja kulturalna	kompetencje w zakresie świadomości i ekspresji kulturalnej

Źródło: opracowanie własne.

Czytelnik może się zastanawiać nad kategorią „kompetencji kluczowych”, dlatego zastosowano w tym miejscu wyjaśnienie tego terminu, aby uzyskać dodatkowo wzrost świadomości roli jaką pełnią one w życiu każdego z nas:

- kompetencje kluczowe są definiowane jako połączenie wiedzy, umiejętności i postaw odpowiednich do sytuacji, ponadto kompetencje kluczowe to te, których wszystkie osoby potrzebują do samorealizacji i rozwoju osobistego, bycia aktywnym obywatelem, integracji społecznej i zatrudnienia¹⁴;
- „kompetencje kluczowe to te kompetencje, których wszyscy potrzebują do samorealizacji i rozwoju osobistego, zatrudnienia, włączenia społecznego, zrównoważonego stylu życia, udanego życia w pokojowych społeczeństwach, kierowania życiem w sposób prozdrowotny i aktywnego obywatelstwa. Rozwijają się one w perspektywie uczenia się przez całe życie, począwszy od wczesnego dzieciństwa przez całe dorosłe życie, za pomocą uczenia się formalnego, pozaformalnego i nieformalnego, we wszystkich kontekstach, w tym w rodzinie, szkole, miejscu pracy, sąsiedztwie i innych społecznościach”¹⁵.

Wyjaśnienie pojęcia „kompetencji kluczowych” pozwala przejść do analizy i porównania, interesujących nas ze względu na problematykę podjętą w tym paragrafie, kompetencji informatycznych i kompetencji cyfrowych. Elementy składowe tych obszarów kompetencyjnych przedstawiono w tabeli 2, aby łatwiej można było dokonać ich analizy komparatystycznej.

Tabela 2. Porównanie definicji kompetencji informatycznych z kompetencjami cyfrowymi

Kompetencje informatyczne (2006)	Kompetencje cyfrowe (2018)
Obejmują umiejętność i krytyczne wykorzystywanie technologii społeczeństwa informacyjnego (TSI) w pracy, rozrywce i porozumiewaniu się. Opierają się one na podstawowych umiejętnościach w zakresie technologii informacyjnych i komunikacyjnych (TIK): wykorzystywania komputerów do uzyskiwania, oceny, przechowywania, tworzenia, prezentowania i wymiany informacji oraz do porozumiewania się i uczestnictwa w sieciach współpracy za pośrednictwem Internetu.	Obejmują pewne, krytyczne i odpowiedzialne korzystanie z technologii cyfrowych i interesowanie się nimi do celów uczenia się, pracy i udziału w społeczeństwie. Obejmują umiejętność korzystania z informacji i danych, komunikowanie się i współpracę, umiejętność korzystania z mediów, tworzenie treści cyfrowych (w tym programowanie), bezpieczeństwo (w tym komfort cyfrowy i kompetencje związane z cyberbezpieczeństwem), kwestie dotyczące własności intelektualnej, rozwiązywanie problemów i krytyczne myślenie.

Źródło: opracowanie własne.

¹⁴ Ibidem, s. 1-13.

¹⁵ Ibidem, s. 7.

Analiza porównawcza elementów składowych poszczególnych kompetencji przedstawionych w tabeli 2 umożliwia stwierdzenie istotnych zmian w postrzeganiu kompetencji cyfrowych w 2018 roku, po upływie 12 lat od pierwszego ich zdefiniowania w 2006 roku. Pojawiają się takie elementy jak:

- umiejętność korzystania z mediów;
- tworzenie treści cyfrowych (w tym programowanie);
- bezpieczeństwo (w tym komfort cyfrowy i kompetencje związane z cyberbezpieczeństwem);
- kwestie dotyczące własności intelektualnej;
- rozwiązywanie problemów i krytyczne myślenie.

Zmienne środowisko cyberbezpieczeństwa zainicjowało konieczność dodania umiejętności wykorzystywania mediów (prasa, radio, telewizja i Internet). Natomiast w tworzenie treści cyfrowych wpisano programowanie. Prawdopodobnie odpowiedzią na wzrost poziomu cyberzagrożeń było umiejscowienie w kompetencjach cyfrowych wiedzy i umiejętności związanych z cyberbezpieczeństwem. Dodatkowymi elementami, których nie było wcześniej, stały się sprawy związane z własnością intelektualną oraz rozwiązywaniem pojawiających się problemów, a także zdolność do krytycznego myślenia.

Kompetencje cyfrowe jako zmieniający się zbiór elementów określonych przez Parlament Europejski i Radę Unii Europejskiej, stanowią podstawę do dalszych rozważań nad tym obszarem badawczym.

Trendy rozwojowe kompetencji cyfrowych

Tendencje rozwojowe Internetu Rzeczy, a także technologii komputerowych i sztucznej inteligencji, które opisuje w swojej monografii P. Krzykowski¹⁶ oraz przemiany społeczne i polityczne drugiej dekady XXI wieku, zapoczątkowały najistotniejsze zmiany w strukturze rządowej Polski, co skutkowało pojawianiem się nowych trendów ewaluacyjnych w zakresie kompetencji cyfrowych.

Pierwszym krokiem było utworzenie w 2015 roku Ministerstwa Cyfryzacji, które funkcjonowało do jego likwidacji w 2020 roku, aby zostać przywrócone do funkcjonowania 3 lata później. Zasoby strony tego ministerstwa zawierają informację, że: „kompetencje cyfrowe, obok czytania, pisania, umiejętności matematycznych i językowych, stanowią zespół fundamentalnych umiejętności współczesnego człowieka”¹⁷. Ponadto dowiadujemy się, że są one harmonijną kompozycją trzech elementów: wiedzy, umiejętności i postaw. Umożliwiają one życie, uczenie się i pracę w społeczeństwie cyfrowym, które wykorzystuje w swoim codziennym funkcjonowaniu osiągnięcia technologii cyfrowych¹⁸.

Przyjęto w materiale zamieszczonym 23 stycznia 2020 roku następujące elementy składowe kompetencji cyfrowych¹⁹:

- kompetencje informatyczne obejmujące posługiwanie się komputerem i innymi urządzeniami elektronicznymi, bezpieczne korzystanie z Internetu, aplikacji i oprogramowania, nowych inteligentnych technologii cyfrowych

¹⁶ Zob. P. Krzykowski, *Współczesny wymiar bezpieczeństwa. Wyzwania dla Polski*, Warszawa 2020, s. 91-93.

¹⁷ Kompetencje cyfrowe, <https://www.gov.pl/web/cyfryzacja/kompetencje-cyfrowe>, [dostęp: 27.11.2025].

¹⁸ Ibidem.

¹⁹ Ibidem.

oraz umiejętność stosowania metod pochodzących z informatyki przy programowaniu i tworzeniu rozwiązań informatycznych dla problemów z różnych dziedzin (myślenie komputacyjne);

- kompetencje informacyjno-komunikacyjne, polegające na umiejętności wyszukiwania informacji, rozumienia jej, a także selekcji i oceny krytycznej, jak również komunikowania się na odległość za pomocą technologii cyfrowych
- kompetencje funkcjonalne, czyli realne wykorzystanie powyższych kompetencji w różnych sferach codziennego życia, takich jak finanse, praca i rozwój zawodowy, utrzymywanie relacji, zdrowie, hobby, zaangażowanie obywatelskie, życie duchowe itd., zgodnie z zasadami bezpiecznego korzystania z technologii cyfrowych.

Analiza tego rozszerzonego zbioru kompetencji cyfrowych w porównaniu z zaproponowanymi wcześniej przez Parlament Europejski i Radę Unii Europejskiej w 2006 i 2018 roku, pozwala na wyciągnięcie następujących wniosków:

- wiedza i umiejętności służące do wymiany informacji stają się nie wystarczające;
- wzrasta rola wiedzy i umiejętności związanych z posługiwaniem się narzędziami komputerowymi, w tym oprogramowaniem;
- upowszechnienie stosowania rozwiązań informatycznych w rozwiązywaniu problemów z różnych dziedzin;
- istotną rolę przypisuje się krytycznemu podejściu do pojawiających się informacji oraz właściwemu ich rozumieniu;
- zaczyna się mówić o kompetencjach funkcjonalnych rozumianych jako realne wykorzystanie wiedzy i umiejętności cyfrowych we wszystkich sferach życia społecznego;
- wzrasta znaczenie bezpieczeństwa w cyberprzestrzeni.

Koniec drugiej dekady XXI wieku zamyka pewien rozdział przemian w kompetencjach cyfrowych, które ciągle wydają się być niewystarczające, aby sprostać wyzwaniom nadchodzącej kolejnej dekady trzeciego tysiąclecia naszej ery.

Rok 2021 charakteryzuje się prowadzeniem na szeroką skalę działań preparacyjnych Federacji Rosyjskiej do agresji zbrojnej na Ukrainę w 2022 roku. Wykorzystywane były do tego celu posiadane zdolności prowadzenia walki informacyjnej, o której pisał M. Wrzosek: „Znaczny wpływ na stan stosunków międzynarodowych wywiera także walka informacyjna, realizowana głównie w cyberprzestrzeni...”,²⁰. Cyberprzestrzeń, jako czwarta domena, (oprócz lądowej, morskiej i powietrznej) zaczyna odgrywać bardzo poważną rolę nie tylko do prowadzenia walki, ale nawet wojny informacyjnej. Ramy operacyjne walki wielodomenowej muszą również uwzględniać wszystkie domeny, rozszerzając się na przestrzeń kosmiczną i cyberprzestrzeń, a także spektrum elektromagnetyczne i środowisko informacyjne, ponieważ działania w tych domenach w czasie wywołują efekty taktyczne, operacyjne i strategiczne, które nie są uwzględnione w ramach działań głębokich/bliskich/wspierających²¹. Krótkiego wyjaśnienia wymagają jednak następujące fakty:

²⁰ M. Wrzosek, op.cit. s. 13.

²¹ Zob. Multi-Domain Battle. Evolution of Combined Arms for the 21st Century 2025-2040, s. 8, <https://www.govinfo.gov/content/pkg/GOVPUB-D101-PURL-gpo129084/pdf/GOVPUB-D101-PURL-gpo129084.pdf>, [dostęp: 27.11.2025].

- „Walka w cyberprzestrzeni znacznie różni się od tradycyjnych działań militarnych”²²;
- „ ... wojna informacyjna występuje zarówno w obszarze militarnym, jak i cywilnym”²³;
- Operacje informacyjne prowadzone są z wykorzystaniem cyberprzestrzeni oraz przy zastosowaniu dezinformacji²⁴;
- Dezinformacja wpływa na rządy państw, siły zbrojne, przestrzeń międzynarodową oraz życie polityczne, społeczne i ekonomiczne²⁵;
- „W erze cyfrowej i realiach społeczeństw cyfrowych, które obecnie stanowią większość ludności świata, działania preparacyjne skupiają się na zastosowaniu dezinformacji”²⁶.

Potwierdzone naukowo fakty oraz doświadczenia zdarzeń jakie miały miejsce w przestrzeni publicznej Polski i jej najbliższym otoczeniu geopolitycznym od roku 2022, skłaniają do refleksji nad przyszłymi wymaganiami kompetencji cyfrowych.

Inspirację do podjęcia takich działań wzmacniają wnioski, które przedstawia J. Syta: „Ataki cybernetyczne nie odgrywają znaczącej roli podczas konfliktu z punktu widzenia działań ofensywnych. Mogą one jednak wywoływać zamieszanie, angażując zasoby i wpływając na morale żołnierzy”²⁷. Uwzględnić można jeszcze wszelkie zmiany w jakie zachodzą w sztuce wojennej²⁸. Pamiętać wypada również o ograniczonym potencjale specjalistów zajmujących się realizacją zadań w obszarze cyberbezpieczeństwa, a sygnalizował to już w 2022 roku G. Pilarski²⁹. Trzeba też mieć świadomość, że rozwój technologii oraz wejście społeczeństw w erę informacji jest skutkiem utworzenia się środowiska sieciocentrycznego obejmującego swym zasięgiem wymiar strukturalny, organizacyjny, procesowy i mentalny³⁰. Zadania realizowane z wykorzystaniem kompetencji cyfrowych przez podmioty należące do podsystemu militarnego

²² L. Klich, C. Sochala, Działania w cyberprzestrzeni jako zagrożenia dla bezpieczeństwa i obronności państwa, [w:] D. Nowak, C. Sochala, A. Warmiński (red.), Wyzwania dla bezpieczeństwa i obronności Rzeczypospolitej Polskiej w aspekcie nowych zagrożeń, Warszawa 2019, s. 235.

²³ M. Mogilnicki, Komunikacja strategiczna wobec zagrożeń informacyjnych. Teoria i praktyka, Warszawa 2024, s. 10.

²⁴ Zob. Z. Modrzejewski, Współczesne postrzeganie operacji informacyjnych, [w:] A. Czupryński, G. Stolarski (red.), Teoria wojny. Nowe i stare wyzwania, Siedlce-Warszawa 2019, s. 52.

²⁵ Zob. T. Dukiewicz, Threats to State Security in the Aspect of Disinformation, “Security Dimensions”, s. 73, <https://securitydimensions.publisherspanel.com/article/153293/en> [dostęp: 27.11.2025]. DOI: 10.5604/01.3001.0015.3293

²⁶ M. Mogilnicki, Rosyjskie przygotowania dezinformacyjne do wojny z Ukrainą, „Cybersecurity & Cybercrime” 2024, nr 1(4), s. 273.

²⁷ J. Syta, Cyber operations in hybrid conflicts - lessons from the war in ukraine, “Cybersecurity & Cybercrime”, 1(2), s. 47, <https://doi.org/10.5604/01.3001.0053.8019> [dostęp: 28.11.2025].

²⁸ Zob. szerzej: R. Chrupek, Wpływ doświadczeń wojennych na ewolucję sztuki wojennej w poglądach wybranych polskich teoretyków i praktyków wojskowych, [w:] J. Lasota, M. Przybylak, A. Niewiński (red.), Animus Belli: Duch wojny. T. III, Zmienność w historii sztuki wojennej, Warszawa 2021, s. 131-165.

²⁹ Zob. G. Pilarski, Audyt zdolności do realizacji cyberedukacji w Akademii Sztuki Wojennej na potrzeby kształcenia w systemie bezpieczeństwa narodowego RP, [w:] A. Szczygalska (red.), Organizacja systemu rozpoznania zagrożeń państwa. Zarządzanie wiedzą w podsystemie militarnym państwa, Warszawa 2022, s. 227-228.

³⁰ Por. M. Wrzosek, W. Scheffs, Informacja rozpoznawcza w działaniach wojsk w środowisku sieciocentrycznym, [w:] W. Scheffs (red.), Konteksty teoretyczne i praktyczne informacji w organizacji, Kalisz 2022, s. 245.

będą związane z koniecznością działania w zautomatyzowanych systemach wsparcia dowodzenia oraz obsługi różnego rodzaju oprogramowania i aplikacji.

Podmioty podsystemu niemilitarnego w ramach realizacji zadań obronnych również wykorzystują posiadane kompetencje cyfrowe, które są szczególnie przydatne do wykonywania zadań informacyjnych. „Zadania informacyjne obejmują wszelką działalność związaną z realizacją celów obrony narodowej poprzez informacyjne oddziaływanie na zachowania i postawy podmiotów międzynarodowych i krajowych, ochronę interesów narodowych przed negatywnymi skutkami oddziaływań tych podmiotów, a także ochronę technicznych urządzeń informatycznych przed oddziaływaniami człowieka, a w razie potrzeby oddziaływanie na techniczne urządzenia informacyjne innego podmiotu (grupy społecznej, państwa)”³¹. Są to bardzo ważne zadania wykonywane permanentnie w czasie pokoju, a w razie konieczności również podczas kryzysu i wojny. Wpływają bezpośrednio na poziom odporności systemu obronnego naszego państwa.

Dynamiczny rozwój zmiennego środowiska cyberbezpieczeństwa stanowi uwarunkowania do konfigurowania zestawu kompetencji cyfrowych, które odegrają kluczową rolę w perspektywie kolejnych pięciu lat do roku 2030. Dzisiaj jesteśmy świadkami dokonującego się skoku technologicznego, o którym pisał już 5 lat temu P. Krzykowski: „Technologie nowej rewolucji już przynoszą ogromne korzyści gospodarcze i społeczne większości światowej populacji. Następna fala nowych technologii radykalnie przekształci gospodarkę i społeczeństwa. Medycyna precyzyjna, pojazdy autonomiczne i drony to szybko rozwijające się rynki, podczas gdy sama sztuczna inteligencja ma przyspieszyć globalny wzrost gospodarczy o 14% do 2030 roku”³². Rozwój niesie ze sobą jednak nie tylko same korzyści, ale także stanowi źródło różnorodnych zagrożeń. Podobnie jest z nauką, o której mówią nam B.M. Szulc i K. Pierzchała: „Wskazywaliśmy już, że w dziejach ludzkości nauka odgrywała niezwykle istotną rolę, stanowiła o postępie i rozwoju ludzkości, ale też wpływała na rozwój technologii sprzyjającej niszczeniu i śmierci”³³. Rozwój techniczny i naukowy oprócz wzrostu gospodarczego może być źródłem różnego rodzaju niebezpieczeństw stanowiących zagrożenia bezpieczeństwa.

Trzydzieści lat temu A. Pieczywok pisał: „Wiek XXI to okres napięć i konfliktów nie zawsze noszących znamiona typowych starć zbrojnych. To także czas wzrostu skali i zasięgu zagrożeń społecznych, politycznych, ekologicznych, cywilnych, czy też terrorystycznych. (...) W ostatnich latach zmniejszyło się poczucie bezpieczeństwa obywateli”³⁴. Słowa te najlepiej opisują sytuację, która zapanowała na kontynencie europejskim i nie tylko, biorąc pod uwagę obecne zagrożenia bezpieczeństwa w takich miejscach świata, jak: Strefa Gazy, Wenezuela, Tajwan, a także dążenia mocarstw do zwiększania stref wpływu w Afryce.

Konfigurowanie zbioru kompetencji cyfrowych, jako odpowiedzi na tego typu przemiany w horyzoncie 2030 roku, nie powinno odbywać się w oderwaniu od osiągnięć naukowych. Taką drogę postępowania bowiem proponuje B. Szulc,

³¹ W. Kitler, Organizacja bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty ustrojowe, prawno-administracyjne i systemowe, Toruń 2018, s. 379-380.

³² P. Krzykowski, op.cit., s. 93.

³³ B.M. Szulc, K. Pierzchała, Człowiek we współczesnym społeczeństwie (Wybrane problemy), Toruń 2022, s. 144.

³⁴ A. Pieczywok, Edukacja dla bezpieczeństwa wobec zagrożeń i wyzwań współczesności, Warszawa 2012, s. 349.

który przedstawiając wybrane podejścia do nauki, wiedzy i mądrości – inspirowany teoriami Karla Poppera – wskazuje, że: „Zadanie nauki jest częściowo teoretyczne – wyjaśnianie, a częściowo praktyczne – przewidywanie i techniczne zastosowania”³⁵. Taka droga wydaje się być racjonalna i może gwarantować sukces. Potwierdzają to działania w naszym państwie, ponieważ zbiór kompetencji cyfrowych, który jest wskazany na stronie internetowej ministerstwa cyfryzacji jest spójny z wynikami ekspertyzy wykonywanej przez Polskie Towarzystwo Informatyczne na zlecenie Kancelarii Prezesa Rady Ministrów, której byłem współautorem.

Oprócz wskazanych już wcześniej w tym paragrafie kompetencji cyfrowych, które określono w 2020 roku, Ministerstwo Cyfryzacji opracowało „Program Rozwoju Kompetencji Cyfrowych”³⁶, a także zgodnie z Uchwałą nr 125 Rady Ministrów z dnia 22 października 2024 r. w sprawie Krajowego planu działania do programu polityki „Droga ku cyfrowej dekadzie” do 20230 r.³⁷, wdrożyło ten plan działania i jest on obecnie realizowany w Polsce. Zapisy zawarte w tym programie wyznaczają główne trendy i uwarunkowania cyfrowej transformacji, w tym również w zakresie kompetencji cyfrowych, w perspektywie 2030 roku. Największym wyzwaniem jest kształtowanie podstawowych umiejętności cyfrowych społeczeństwa u osób w wieku od 16 do 74 lat, ponieważ na podstawie badań zawartych na stronie 30 programu, dostrzega się linię trendu z której wynika, że tylko około 50% osób będzie posiadało podstawowe kompetencje cyfrowe w 20230 roku, natomiast cel programowy zakłada poziom 54,5% już w roku 2025 i poziom 80% w roku 2030.

Podsumowanie

Rola kluczowych kompetencji cyfrowych ciągle wzrasta proporcjonalnie do rozwoju technologicznego, a także przemian społecznych, gospodarczych i politycznych. Wiedza i umiejętności wykorzystywane do wymiany informacji jeszcze dziesięć lat temu, obecnie są już niewystarczające do sprawnego funkcjonowania w świecie cyfrowym. Coraz bardziej dostrzegana jest potrzeba posiadania wiedzy i umiejętności związanych z tworzeniem i obsługą różnego rodzaju oprogramowania i aplikacji. Zastosowanie technologii komputerowych przenika niemal wszystkie sfery ludzkiej aktywności zawodowej i prywatnej. Lawina informacyjna wzbudza pilną potrzebę posiadania krytycznego podejścia do źródeł z jakich przekazywane są informacje oraz do weryfikowania ich treści w różnych kanałach informacyjnych o dużej wiarygodności.

Cyberzagrożenia oraz walka i wojna informacyjna z dezinformacją podnoszą wymagania posiadania kompetencji cyfrowych na znacznie wyższym poziomie niż podstawowy. Cyberprzestrzeń stała się domeną prowadzenia operacji wielodomenowych podsystemu militarnego, ale stanowi też doskonały obszar oddziaływania na podsystem niemilitarny w systemie obronnym państwa.

Osiągnięcia naukowe i skoordynowane działania rządowe, wyznaczają trendy rozwoju kompetencji cyfrowych. Zasadnym jest zarekomendowanie

³⁵ B. Szulc, Nauka. Wiedza. Mądrość, Warszawa 2011, s. 61.

³⁶ Zob. Program Rozwoju Kompetencji Cyfrowych, <https://www.gov.pl/web/cyfryzacja/kompetencje-cyfrowe> [dostęp: 29.11.2025].

³⁷ Zob. Uchwała nr 125 Rady Ministrów z dnia 22 października 2024 r. w sprawie Krajowego planu działania do programu polityki „Droga ku cyfrowej dekadzie” do 20230 r. <https://www.gov.pl/web/cyfryzacja/program-polityki-droga-ku-cyfrowej-dekadzie-do-2030-r2> [dostęp: 29.11.2025].

przeprowadzenia badań porównawczych posiadania podstawowych umiejętności cyfrowych u osób w wieku od 16 do 74, aby ewentualnie zintensyfikować programy wspierające ich rozwój na poziomie lokalnym (wieś, miasto, gmina, powiat).

Bibliografia

- Artificial Intelligence (AI) in Cybersecurity: The Future of Threat Defense, Fortinet, <https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity>.
- Bogdański A., Good practices in military cybersecurity training, „Edukacyjna analiza transakcyjna” 2024, nr 13.
- Chrupek R., Wpływ doświadczeń wojennych na ewolucję sztuki wojennej w poglądach wybranych polskich teoretyków i praktyków wojskowych, [w:] Lasota J., Przybylak M., Niewiński A. (red.), Animus Belli: Duch wojny. T. III, Zmienność w historii sztuki wojennej, Warszawa 2021.
- Dukiewicz T., Threats to State Security in the Aspect of Disinformation, “Security Dimensions”, <https://securitydimensions.publisherspanel.com/article/153293/en> DOI: 10.5604/01.3001.0015.3293.
- Farrand B., Carrapico H., Turobov A., The new geopolitics of EU cybersecurity: security, economy and sovereignty, „International Affairs” 2024, t. 100, nr 6.
- Filipowicz G., Zarządzanie kompetencjami, perspektywa firmowa i osobista, Warszawa 2014.
- Kitler W., Organizacja bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty ustrojowe, prawno-administracyjne i systemowe, Toruń 2018.
- Klich L., Sochala C., Działania w cyberprzestrzeni jako zagrożenia dla bezpieczeństwa i obronności państwa, [w:] Nowak D., Sochala C., Warmiński A. (red.), Wyzwania dla bezpieczeństwa i obronności Rzeczypospolitej Polskiej w aspekcie nowych zagrożeń, Warszawa 2019.
- Kompetencje cyfrowe, <https://www.gov.pl/web/cyfryzacja/kompetencje-cyfrowe>.
- Korzyński P., Przywództwo w erze cyfrowej, Warszawa 2018.
- Krzykowski P., Współczesny wymiar bezpieczeństwa. Wyzwania dla Polski, Warszawa 2020.
- Modrzejewski Z., Współczesne postrzeganie operacji informacyjnych, [w:] Czupryński A., Stolarski G. (red.), Teoria wojny. Nowe i stare wyzwania, Siedlce-Warszawa 2019.
- Mogilnicki M., Komunikacja strategiczna wobec zagrożeń informacyjnych. Teoria i praktyka, Warszawa 2024.
- Mogilnicki M., Rosyjskie przygotowania dezinformacyjne do wojny z Ukrainą, „Cybersecurity & Cybercrime” 2024.
- Multi-Domain Battle. Evolution of Combined Arms for the 21st Century 2025-2040, <https://www.govinfo.gov/content/pkg/GOVPUB-D101-PURL-gpo129084/pdf/GOVPUB-D101-PURL-gpo129084.pdf> (dostęp: 27.11.2025).
- Pieczwok A., Edukacja dla bezpieczeństwa wobec zagrożeń i wyzwań współczesności, Warszawa 2012.
- Pilarski G., Audyt zdolności do realizacji cyberedukacji w Akademii Sztuki Wojennej na potrzeby kształcenia w systemie bezpieczeństwa narodowego RP, [w:] Szczygielska A. (red.), Organizacja systemu rozpoznania zagrożeń państwa. Zarządzanie wiedzą w podsystemie militarnym państwa, Warszawa 2022.
- Pilarski G., Przegląd współczesnych zagrożeń w cyberprzestrzeni, „Problemy techniki uzbrojenia” 2023, t. 167, nr 5. <https://ptu-biuletyn.pl/article/542998/pl>, DOI: 10.5604/01.3001.0054.2998 <https://doi.org/10.5604/01.3001.0054.2998>.
- Pilarski G., Zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni, „Wiedza obronna” 2025, t. 292, nr 3.

- Program Rozwoju Kompetencji Cyfrowych, <https://www.gov.pl/web/cyfryzacja/kompetencje-cyfrowe>.
- Ropski J., Bezpieczeństwo edukacji w świecie VUCA, [w:] D. Kaźmierczak, J. Ropski, O. Wasiuta i W. Zakrzewski (red.), Edukacja w świecie VUCA, Szanse, Wyzwania, Zagrożenia, Kraków 2021.
- Syta J., Cyber operations in hybrid conflicts - lessons from the war in Ukraine. "Cybersecurity & Cybercrime" 2023, nr 1(2), <https://doi.org/10.5604/01.3001.0053.8019>.
- Szulc B., Nauka. Wiedza. Mądrość, Warszawa 2011.
- Szulc B.M., Pierzchała K., Człowiek we współczesnym społeczeństwie (Wybrane problemy), Toruń 2022.
- Uchwała nr 125 Rady Ministrów z dnia 22 października 2024 r. w sprawie Krajowego planu działania do programu polityki „Droga ku cyfrowej dekadzie” do 2030 r. <https://www.gov.pl/web/cyfryzacja/program-polityki-droga-ku-cyfrowej-dekadzie-do-2030-r2>.
- Wrzosek M., Zarządzanie wiedzą oficerów rozpoznania wojskowego, [w:] Szczygielska A. (red.), Organizacja systemu rozpoznania zagrożeń państwa. Zarządzanie wiedzą w podsystemie militarnym państwa, Warszawa 2022.
- Wrzosek M., Scheffs W., Informacja rozpoznawcza w działaniach wojsk w środowisku sieciocentrycznym, [w:] Scheffs W. (red.), Konteksty teoretyczne i praktyczne informacji w organizacji, Kalisz 2022.
- Zaborowski P., Kozłowski M., Zastosowanie sztucznej inteligencji w rozwiązaniach cyberbezpieczeństwa, „Cybersecurity and Law” 2025, t. 1, nr 13.
- Zalecenie parlamentu europejskiego i rady z dnia 18 grudnia 2006 r. w sprawie kompetencji kluczowych w procesie uczenia się przez całe życie, Bruksela 18 grudnia 2006 r., PE-CONS 3650/1/06 REV 1, <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32006H0962>.
- Zalecenie Rady z dnia 22 maja 2018 r. w sprawie kluczowych kompetencji w zakresie uczenia się przez całe życie (Tekst mający znaczenie dla EOG), [https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32018H0604\(01\)](https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32018H0604(01)).