NASK Cyber POLICY

Cyberbezpieczeństwo A.D. 2019

Strategia. Policy. Rekomendacje
– cyberbezpieczeństwo w perspektywie policy

cyberpolicy.nask.pl | ISBN 978-83-954637-2-3

NASK

Cyber POLICY

Cyberbezpieczeństwo A.D. 2019

Strategia. Policy. Rekomendacje – cyberbezpieczeństwo w perspektywie *policy*

Redakcja: dr Magdalena Wrzosek

Zespół Redakcyjny: Rafał Babraj, Justyna Balcewicz-Majewska, Paweł Zegarow

Opracowanie graficzne: Piotr Klicki

Warszawa, maj 2020

NASK Państwowy Instytut Badawczy – cyberpolicy.nask.pl

ISBN 978-83-954637-2-3

9 788395 463723

Spis treści

Legenda

- Unia Europejska
- Polska
- Organizacja Narodów Zjednoczonych
- Sojusz Północnoatlantycki
- Organizacja Współpracy Gospodarczej i Rozwoju
- Sieć 5G
- Umiejętności cyfrowe
- Cyberbezpieczeństwo
- Sztuczna Inteligencja (AI)
- Dezinformacja

Wstęp

Szanowni Państwo,

Państwowy Instytut Badawczy NASK (NASK PIB) od wielu lat działa na rzecz podnoszenia poziomu bezpieczeństwa teleinformatycznego w Polsce. Od 1996 roku w strukturze Instytutu funkcjonuje zespół CERT Polska, pierwszy w Polsce zespół reagowania na incydenty komputerowe. Prowadzimy wiele projektów badawczo-rozwojowych w dziedzinie cyberbezpieczeństwa (krajowych i międzynarodowych). Kompetencje technologiczne i badawcze instytutu w tej dziedzinie systematycznie rozszerzamy o działania na rzecz propagowania wiedzy z obszaru organizacyjnego, regulacyjnego i strategicznego. Po przyjęciu w 2016 roku tzw. Dyrektywy NIS, rozpoczęliśmy w NASK działania zmierzające do budowy kompetencji w zakresie tzw. *policy*. W efekcie już rok później uruchomiliśmy portal CyberPolicy (https://cyberpolicy.nask.pl/), który stanowi kompendium wiedzy na temat cyberbezpieczeństwa w aspekcie strategicznym, regulacyjnym i organizacyjnym.

Ustawa o krajowym systemie cyberbezpieczeństwa nałożyła na NASK PIB, rolę CSIRT NASK – jednego z trzech CSIRT poziomu krajowego. Poza działaniami operacyjnymi, legitymizuje ona także działania na poziomie *policy* – prowadzenie analiz strategicznych i opracowywanie rekomendacji, proponowanie rozwiązań systemowych w postaci standardów i dobrych praktyk, czy też wspieranie uczestników krajowego systemu cyberbezpieczeństwa w budowaniu potencjału i zdolności w obszarze cyberbezpieczeństwa.

Publikacja *Cyberbezpieczeństwo A.D. 2019* to podsumowanie ubiegłego roku w zakresie strategiczno-regulacyjnym. Znajdziecie tu Państwo informacje na temat najważniejszych aktów legislacyjnych i strategicznych w Polsce, Unii Europejskiej, Organizacji Narodów Zjednoczonych, Sojuszu Północnoatlantyckim i Organizacji Współpracy Gospodarczej i Rozwoju. Dodatkowo, w tym roku wzbogaciliśmy raport o pięć artykułów analitycznych, podsumowujących najważniejsze tematy w zakresie cyberbezpieczeństwa i nowoczesnych technologii w 2019 roku.

Cyberbezpieczeństwo A.D. 2019 stanowi przegląd najważniejszych inicjatyw dziedzinowych i wydarzeń z 2019 roku oraz próbę przybliżenia tego, jak kształtuje się dyskusja w zakresie cyberbezpieczeństwa i nowoczesnych technologii na świecie, przed jakimi nowymi wyzwaniami stajemy i jak są one adresowane na różnych forach.

Zapraszam do lektury!

Krzysztof Silicki,
Zastępca Dyrektora NASK PIB,
Dyrektor ds. Cyberbezpieczeństwa i Innowacji

Kalendarium

Styczeń

21 stycznia

OECD publikuje raport
Trends Shaping Education 2019.

25 stycznia

Rada Ministrów przyjmuje
Zintegrowaną Strategię Umiejętności 2030
(część ogólną).

Luty

5 lutego

Minister Obrony Narodowej przedstawia koncepcję budowy wojsk obrony cyberprzestrzeni, której częścią jest program CYBER.MIL. W ramach programu uruchomiono działania na rzecz edukacji i szkoleń z cyberbezpieczeństwa.

12 lutego

Agencja NATO ds. Komunikacji i Informacji (NCI) inicjuje centrum współpracy w zakresie cyberbezpieczeństwa *(Cyber Security Collaboration Hub).*

12 lutego

NASK publikuje poradnik na temat tworzenia ISAC[1] (Centrum Wymiany i Analizy Informacji). Wydanie poradnika stało się impulsem do utworzenia w Polsce ekosystemu ISAC w sektorach kluczowych.

Marzec

11 marca

Szczyt OECD *Summit on Going Digital*, na którym podsumowano zakończenie pierwszej fazy projektu *Going Digital*.

1 Poradnik na temat tworzenia ISAC *(Centra Wymiany i Analizy Informacji)* (https://cyberpolicy.nask.pl/poradnik-na-temat-tworzenia-isac-centra-wymiany-i-analizy-informacji/)

17 marca

Wchodzi w życie Ustawa o Fundacji Platforma Przemysłu Przyszłości. Celem Fundacji jest wsparcie przedsiębiorców w budowaniu konkurencyjności Polski w Przemyśle 4.0.

26 marca

Komisja Europejska publikuje rekomendacje dotyczące działań i środków operacyjnych bezpieczeństwa sieci 5G w Unii Europejskiej.

Kwiecień

1 kwietnia

37 instytutów badawczych i Polski Ośrodek Rozwoju Technologii wchodzi w skład Sieci Badawczej Łukasiewicz.

7 kwietnia

NASK PIB prezentuje raport *Cyberbezpieczeństwo A.D. 2018. Strategia. Policy. Rekomendacje*, który zawiera rekomendacje i podsumowanie ubiegłego roku w zakresie *policy*.

8 kwietnia

Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji publikuje *Wytyczne w zakresie etyki dotyczące godnej zaufania Sztucznej Inteligencji*.

8 kwietnia

Światowy Szczyt Społeczeństwa Informacyjnego *(World Summit on the Information Society – WSIS)*.

13 kwietnia

Powołanie Prezesa Urzędu Ochrony Danych Osobowych.

17 kwietnia

Przyjęcie Rozporządzenia Parlamentu Europejskiego i Rady UE w sprawie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) oraz certyfikacji cyberbezpieczeństwa **(Akt o cyberbezpieczeństwie).**

25 kwietnia

OECD publikuje raport
The Future of Work. OECD Employment Outlook 2019.

26 kwietnia

W Ministerstwie Cyfryzacji odbywa się spotkanie z przedsiębiorcami świadczącymi usługi z zakresu cyberbezpieczeństwa oraz operatorami usług kluczowych. W czasie spotkania zgłaszane są liczne uwagi do *Ustawy o krajowym systemie cyberbezpieczeństwa* oraz rozporządzeń wykonawczych.

Maj

22 maja

OECD publikuje nową Strategię Umiejętności *(OECD Skills Strategy 2019).*

23 maja

Druga konferencja podsumowująca *Cyber Defence Pledge* w Londynie.

26 maja

Minister Cyfryzacji, Minister Inwestycji i Rozwoju, Minister Nauki i Szkolnictwa Wyższego oraz Minister Przedsiębiorczości i Technologii podpisują memorandum na rzecz rozwoju Sztucznej Inteligencji w Polsce.

Czerwiec

6 czerwca

Rozpoczyna się formowanie Zespołu Działań Cybernetycznych w strukturze Wojsk Obrony Terytorialnej.

7 czerwca

Komisja Europejska publikuje Akt o Cyberbezpieczeństwie *(Cybersecurity Act)*. Drugą, po Dyrektywie NIS, ogólnoeuropejską regulację w zakresie cyberbezpieczeństwa.

10 czerwca

Panel Wysokiego Szczebla ds. Współpracy Cyfrowej składa raport ze swojej działalności ONZ.

11 czerwca

Komisja Europejska publikuje wyniki *Indeksu Gospodarki Cyfrowej i Społeczeństwa Cyfrowego DESI 2019*.

26 czerwca

Podpisanie polsko-amerykańskiej umowy o współpracy w cyberprzestrzeni w obszarze militarnym.

26 czerwca

Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji publikuje *Wytyczne w zakresie regulacji i inwestycji dla godnej zaufania Sztucznej Inteligencji*.

27 czerwca

Wchodzi w życie Akt o cyberbezpieczeństwie *(Cybersecurity Act)*.

Lipiec

4 lipca

Podpisanie umowy o współpracy w obszarze obrony cyberprzestrzeni pomiędzy Ministerstwem Obrony Narodowej a NATO.

16 lipca

Zarząd Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) wybiera nowego Dyrektora Wykonawczego.

23 lipca

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) zaprasza do składania wniosków o dołączenie do *The Stakeholder Cybersecurity Certification Group*.

31 lipca

Aktualizacja *Krajowego Planu Działań zmiany przeznaczenia pasma 700 MHz w Polsce*.

Sierpień

5 sierpnia

Ministerstwo Cyfryzacji ogłasza konsultacje projektu *Strategii Cyberbezpieczeństwa na lata 2019-2024*.

6 sierpnia

ENISA informuje, że otrzymała zadanie przygotowania pierwszej propozycji europejskiego programu certyfikacji cyberbezpieczeństwa. Grupa ekspertów pomoże wypracować „spadkobiercę" SOG-IS.

8 sierpnia

ITU publikuje nowy standard, który stwarza podstawę efektywnej integracji uczenia maszynowego z siecią 5G.

21 sierpnia

Rozpoczynają się konsultacje społeczne dokumentu *Polityka Rozwoju Sztucznej Inteligencji w Polsce na lata 2019-2027*.

31 sierpnia

Minister Cyfryzacji inauguruje działalność Wirtualnej Katedry Etyki i Prawa.

Wrzesień

4-5 września

Podczas XXIX Forum Ekonomicznego w Krynicy odbywa się I Forum Cyberbezpieczeństwa zorganizowane przez NASK i Ministerstwo Cyfryzacji.

10 września

Prezydent RP podpisuje *ustawę o zmianie ustawy o wspieraniu rozwoju usług i sieci telekomunikacyjnych oraz niektórych innych ustaw (tzw. megaustawę).*

24 września

W siedzibie NASK odbywa się premiera raportu *Dezinformacja w dobie rewolucji cyfrowej.*

25 września

W siedzibie NASK odbywają się warsztaty *7th National Cybersecurity Strategies Workshop* zorganizowane we współpracy NASK i ENISA.

30 września

Kick-off event inicjujący Europejski Miesiąc Cyberbezpieczeństwa (ECSM), koordynowany przez NASK.

Październik

1 października

Rusza kampania *Europejski Miesiąc Cyberbezpieczeństwa* (ECSM).

9 października

Grupa Współpracy NIS publikuje unijną skoordynowaną ocenę ryzyka związanego z cyberbezpieczeństwem w sieciach 5G.

10 października

Rozpoczyna się kampania *CyberLiga* w ramach ECSM.

10 października

Minister Obrony Narodowej zatwierdza *Plan Modernizacji Technicznej na lata 2021-2035 z uwzględnieniem 2020 roku.*

16 października

Nowy Dyrektor Wykonawczy ENISA, Juhan Lepassaar, oficjalnie rozpoczyna pełnienie obowiązków.

21 października

Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji publikuje raport poświęcony odpowiedzialności za Sztuczną Inteligencję i inne nowe technologie.

22 października

Rada Ministrów przyjmuje uchwałę w sprawie *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024*.

22-23 października

Odbywa się 23. edycja SECURE, najstarszej w Polsce konferencji dotyczącej bezpieczeństwa teleinformatycznego.

23 października

Komisja Europejska publikuje sprawozdanie na temat funkcjonowania Tarczy Prywatności UE-USA.

25 października

Ministrowie Obrony NATO przyjmują nowe wymagania odporności cywilnej infrastruktury telekomunikacyjnej, w tym 5G.

28 października

Memorandum dotyczące opracowania modelu biznesowego dla spółki #Polskie5G.

Listopad

20 listopada

Ministerstwo Cyfryzacji podpisuje listy intencyjne z 10 uczelniami wchodzącymi w skład Akademii Innowacyjnych Zastosowań Technologii Cyfrowych.

21 listopada

Publikacja raportu *ENISA Threat Landscape for 5G Network*.

22 listopada

Zakończenie *World Radio Conference (WRC-19)*. Identyfikacja dodatkowych pasm częstotliwości powyżej 6 GHz dla usług 5G.

25-29 listopada

Forum Zarządzania Internetem w Berlinie.

Grudzień

2 grudnia

Komisja Europejska prosi ENISA o przygotowanie planu certyfikacji cyberbezpieczeństwa dla usług w chmurze.

3-4 grudnia

Szczyt NATO w Londynie. W deklaracji końcowej zapisy nawiązujące m.in. do zapewnienia cyberbezpieczeństwa sieci 5G oraz uznania przestrzeni kosmicznej za obszar działań operacyjnych Sojuszu.

9 grudnia

UKE rozpoczyna postępowanie konsultacyjne w sprawie rozdysponowania częstotliwości w paśmie 3,6 GHz dla sieci 5G.

11 grudnia

OECD publikuje raport *Strategia Umiejętności OECD: Polska*.

17 grudnia

Minister Zdrowia publikuje rozporządzenie w sprawie dopuszczalnych poziomów pól elektromagnetycznych w środowisku (PEM).

23 grudnia

Publikacja nowego rozporządzenia *Ministra Cyfryzacji w sprawie warunków organizacyjnych i technicznych dla operatorów usług kluczowych.*

TAK BYŁO

Przegląd wydarzeń w Polsce
i w organizacjach międzynarodowych


OECD


POLSKA

Najważniejsze wydarzenia dotyczące cyberbezpieczeństwa w Polsce w 2019 roku:

5 lutego

Minister Obrony Narodowej przedstawia koncepcję budowy wojsk obrony cyberprzestrzeni, której częścią jest program CYBER.MIL. W ramach programu uruchomiono działania na rzecz edukacji i szkoleń z cyberbezpieczeństwa.

17 marca

Wchodzi w życie Ustawa o Fundacji Platforma Przemysłu Przyszłości. Celem Fundacji jest wsparcie przedsiębiorców w budowaniu konkurencyjności Polski w Przemyśle 4.0.

1 kwietnia

37 instytutów badawczych i Polski Ośrodek Rozwoju Technologii tworzą Sieć Badawczą Łukasiewicz.

26 maja

Podpisanie przez Ministra Cyfryzacji, Ministra Inwestycji i Rozwoju, Ministra Nauki i Szkolnictwa Wyższego oraz Ministra Przedsiębiorczości i Technologii memorandum na rzecz rozwoju Sztucznej Inteligencji w Polsce.

6 czerwca

Rozpoczyna się formowanie Zespołu Działań Cybernetycznych w strukturze Wojsk Obrony Terytorialnej.

21 sierpnia

Rozpoczynają się konsultacje społeczne dokumentu *Polityka Rozwoju Sztucznej Inteligencji w Polsce na lata 2019-2027.*

30 sierpnia

Przyjęcie ustawy o zmianie ***ustawy o wspieraniu rozwoju usług i sieci telekomunikacyjnych oraz niektórych innych ustaw.*** Tzw. megaustawa obowiązuje od października. Nowe przepisy mają wspierać usuwanie barier administracyjno-prawnych dla budowy sieci szerokopasmowych.

22 października

Rada Ministrów przyjmuje uchwałę w sprawie *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024*.

28 października

Memorandum dotyczące opracowania modelu biznesowego dla spółki #Polskie5G.

20 listopada

Ministerstwo Cyfryzacji podpisuje listy intencyjne z 10 uczelniami wchodzącymi w skład Akademii Innowacyjnych Zastosowań Technologii Cyfrowych.

23 grudnia

Opublikowanie nowej wersji *Rozporządzenia Ministra Cyfryzacji w sprawie warunków organizacyjnych i technicznych dla operatorów usług kluczowych.*

Rok 2019 był pierwszym rokiem obowiązywania *Ustawy o Krajowym Systemie Cyberbezpieczeństwa*. Jednym z większych wyzwań było wyznaczenie operatorów usług kluczowych oraz ich dostosowanie się do wymogów ustawowych. Równocześnie, z uwagi na liczne uwagi operatorów, zmieniono *Rozporządzenie Ministra Cyfryzacji w sprawie warunków organizacyjnych i technicznych dla operatorów usług kluczowych*, które opublikowano w grudniu. Dwukrotnie zmieniano też samą ustawę – raz we wrześniu przy okazji zmian w *Prawie zamówień publicznych*, a drugi raz w październiku przy okazji zmian w *Prawie oświatowym*.

Zgodnie z zapisami ustawy, Rada Ministrów przyjęła w październiku uchwałę w sprawie *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024*. Dokument obowiązuje od 31 października 2019 roku. Głównym celem przyjęcia i wdrożenia *Strategii* jest podniesienie poziomu odporności na cyber-zagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym, a także promowanie dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji. Niestety rząd nie zapewnił funduszy na realizację zadań wynikających ze *Strategii*. Dokument jest realizowany z budżetów poszczególnych jednostek oraz ze środków Narodowego Centrum Badań i Rozwoju, a także z funduszy europejskich.

Rok 2019 był także bardzo istotny ze względu na budowę kompetencji RP w zakresie cyber-obrony. 5 lutego 2019 roku Minister Obrony Narodowej przedstawił koncepcję budowy wojsk ochrony cyberprzestrzeni, której częścią jest program CYBER.MIL. W ramach programu uruchomiono liczne działania na rzecz edukacji i szkoleń z zakresu cyberbezpieczeństwa.

6 czerwca 2019 roku rozpoczęło się natomiast formowanie Zespołu Działań Cybernetycznych w strukturze Wojsk Obrony Terytorialnej.

Rząd polski podejmował także liczne działania związane z budową w Polsce sieci 5G oraz stworzeniem warunków do rozwoju Sztucznej Inteligencji.

Wdrażanie i zmiany Ustawy o krajowym systemie cyberbezpieczeństwa

Identyfikacja operatorów usług kluczowych i sektorowe zespoły ds. cyberbezpieczeństwa

Ustawa z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa weszła w życie 29 sierpnia 2018 roku. Jest to pierwszy akt prawny dotyczący cyberbezpieczeństwa w Polsce, a implementacja przepisów stanowi duże wyzwanie zarówno dla sektora publicznego, jak i prywatnego. Po wejściu w życie ustawy, rozpoczął się proces identyfikacji operatorów usług kluczowych w sektorach objętych regulacją (energetyczny, transportowy, bankowy i infrastruktury rynków finansowych, ochrony zdrowia, zaopatrzenia w wodę pitną wraz z dystrybucją, infrastruktury cyfrowej). Wyznaczono 156[2] operatorów, a zatem znacznie mniej, niż zakładały wstępne szacunki Ministerstwa Cyfryzacji przedstawione w ocenie skutków regulacji do ustawy (szacowano, że operatorów będzie około 300). Najwięcej operatorów wskazano w sektorze energii, a najmniej w sektorze zaopatrzenia w wodę pitną. Proces ich identyfikacji był dużym wysiłkiem dla organów właściwych, które równocześnie

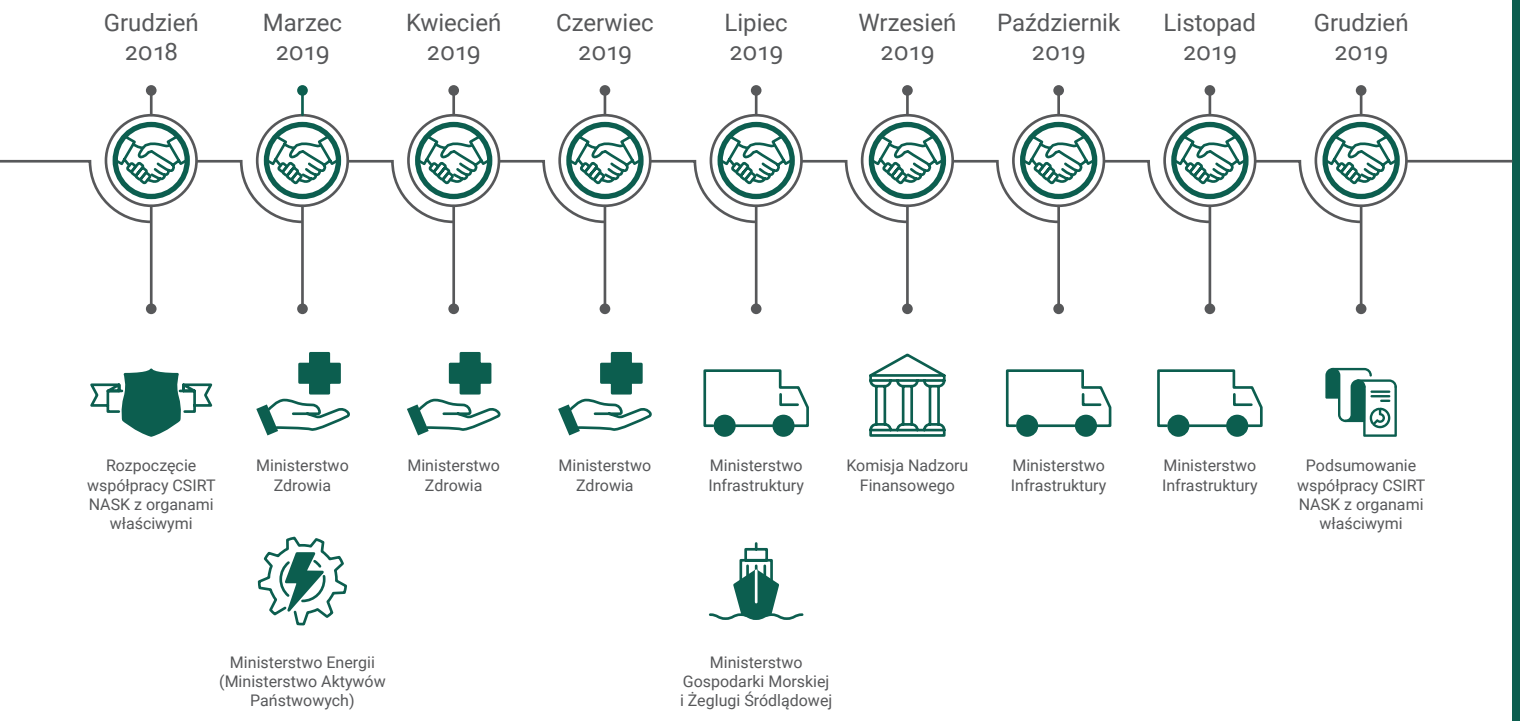
2 Na podstawie informacji publikowanych przez Ministerstwo Cyfryzacji.

z wykonywaniem nowych obowiązków ustawowych, rozpoczęły budowę kompetencji w zakresie cyberbezpieczeństwa.

Ważnym elementem było budowanie współpracy pomiędzy organami właściwymi, a CSIRT poziomu krajowego. W 2019 roku CSIRT NASK odbył w sumie 11 spotkań z organami właściwymi, w ramach których wypracowano m.in. standardowe procedury operacyjne w przypadku incydentów poważnych oraz procedury komunikacji.

Rok współpracy dla polskiego cyberbezpieczeństwa

11 spotkań z organami właściwymi ds. cyberbezpieczeństwa



Wypracowane dokumenty:

- Jak zgłosić incydent poważny? **Toolbox** dla operatorów usług kluczowych.
- **Ankiety** we współpracy z sektorami: zdrowia, transportu, zaopatrzenia w wodę pitną.
- **Procedura komunikacji** między CSIRT NASK a MAP oraz KNF.
- **Rekomendacje** dla MZ, KNF oraz innych organów właściwych.

Mimo że ustawa umożliwia powoływanie **sektorowych zespołów cyberbezpieczeństwa**, w 2019 roku żaden organ właściwy nie podjął działań w tym zakresie. Inicjatywę utworzenia sektorowego zespołu zapowiedział w grudniu 2019 roku Urząd Komisji Nadzoru Finansowego, w czasie prezentacji Cyfrowej Agendy Nadzoru[3]. W samym dokumencie brakuje jednak zapisów na ten temat[4]. Kilka sektorów podjęło także działania zmierzające do powołania sektorowych **Centrów Wymiany i Analizy Informacji** (ISAC). ISAC jest formą partnerstwa publiczno-prywatnego (PPP). To centra wymiany wiedzy i doświadczeń doty-

3 Prezentacja Cyfrowej Agendy Nadzoru odbyła się 19 grudnia 2019 roku (https://www.knf.gov.pl/aktualnosci?articleId=68265&p_id=18)
4 KNF, Cyfrowa Agenda Nadzoru (https://www.knf.gov.pl/knf/pl/komponenty/img/Cyfrowa_agenda_nadzoru_68264.pdf)

czących incydentów cyberbezpieczeństwa w danym sektorze gospodarki. ISAC stanowią alternatywę dla CSIRT sektorowych[5]. Są tańszą i „lżejszą" formą współpracy w obrębie sektora. Temat ISAC był przedmiotem licznych spotkań roboczych, pomiędzy organami właściwymi, a CSIRT NASK. Najbardziej zaawansowane prace w tym zakresie prowadzi podsektor transportu kolejowego, wspierany przez Ministerstwo Infrastruktury oraz NASK PIB.

Zmiany w Ustawie o krajowym systemie cyberbezpieczeństwa

W 2019 roku wprowadzono także dwie zmiany w *Ustawie o krajowym systemie cyberbezpieczeństwa*. Pierwsza była efektem modyfikacji przepisów związanych z *Prawem zamówień publicznych*[6]. Zmiana ta dotyczy artykułu 33, który odnosi się do badania urządzenia informatycznego lub oprogramowania w celu identyfikacji podatności, mogących mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa. Zmiany umożliwiają Pełnomocnikowi[7] wydawanie rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania, bez konsultacji z Kolegium[8], a tylko w porozumieniu z CSIRT poziomu krajowego (CSIRT MON, CSIRT GOV i CSIRT NASK). Warto podkreślić, że rekomendacje te mogą być wydane tylko wtedy, gdy Pełnomocnik uzyska informację o zagrożeniu cyberbezpieczeństwa, która uprawdopodobni możliwość wystąpienia incydentu krytycznego[9].

Druga zmiana w *Ustawie o krajowym systemie cyberbezpieczeństwa* była związana ze zmianami w *Prawie oświatowym*[10]. Dotyczą one budowania kompetencji cyberbezpieczeństwa i zadań Ministerstwa Edukacji Narodowej w tym zakresie. Wydłużony został czas na ich realizację do 31 marca 2021 roku.

Zmiana rozporządzenia w sprawie warunków organizacyjnych i technicznych dla operatorów usług kluczowych

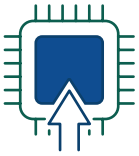
23 grudnia 2019 roku opublikowano nową wersję Rozporządzenia *Ministra Cyfryzacji w sprawie warunków organizacyjnych i technicznych dla operatorów usług kluczowych*[11]. Wprowadzone zostały mniej restrykcyjne wymogi zabezpieczenia pomieszczeń. Uzależniono także dostosowanie poziomu zabezpieczeń od szacowanego ryzyka. Ponadto dopuszczono możliwość pracy zdalnej personelu realizującego zadania z zakresu cyberbezpieczeństwa, pod warunkiem odpowiedniego zabezpieczenia systemu i minimalizacji ryzyka.

Nowa wersja rozporządzenia:

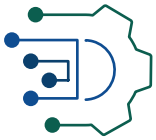
- Mniej restrykcyjne wymogi zabezpieczenia pomieszczeń.
- Poziom zabezpieczeń uzależniony od szacowanego ryzyka.
- Dopuszczenie pracy zdalnej personelu realizującego zadania z zakresu cyberbezpieczeństwa, pod warunkiem zabezpieczenia systemu i minimalizacji ryzyka.

5 Więcej na temat ISAC w poradniku wydanym wspólnie przez NASK PIB i Narodowe Centrum Cyberbezpieczeństwa w Holandii 12 lutego 2019 roku (https://cyberpolicy.nask.pl/poradnik-na-temat-tworzenia-isac-centra-wymiany-i-analizy-informacji/)
6 Ustawa z dnia 11 września 2019 roku – Przepisy wprowadzające ustawę – *Prawo zamówień publicznych.*
7 Ustawa o krajowym systemie cyberbezpieczeństwa wprowadza funkcję Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa. Zgodnie z art. 60 koordynuje on działania i odpowiada za realizowanie polityki rządu w zakresie zapewnienia cyberbezpieczeństwa RP.
8 Ustawa o krajowym systemie cyberbezpieczeństwa wprowadza Kolegium do Spraw Cyberbezpieczeństwa. Jest to organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa, działający przy Radzie Ministrów. Zadania Kolegium opisuje art. 65 ustawy. Są w nich m.in. wydawanie opinii kierunków i planów na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa oraz organizacja wymiany informacji istotnych dla cyberbezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej między organami administracji rządowej;
9 Zgodnie z art. 2 Ustawy o krajowym systemie cyberbezpieczeństwa incydent krytyczny skutkuje znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi. Klasyfikację incydentu krytycznego nadaje właściwy CSIRT poziomu krajowego – CSIRT MON, CSIRT NASK lub CSIRT GOV
10 Ustawa z dnia 11 września 2019 roku – Przepisy wprowadzające ustawę – *Prawo zamówień publicznych.*
11 Poprzednie rozporządzenie przyjęto 10 września 2018 roku – *Rozporządzenie w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo.*

Ustawa o krajowym systemie cyberbezpieczeństwa nakłada konkretne obowiązki na firmy oraz instytucje, które zostały wyznaczone jako operatorzy usług kluczowych[12]. Są to zadania, mające zapewnić bezpieczeństwo świadczonych usług kluczowych oraz ciągłość ich świadczenia, takie jak:



Wdrożenie systemu zarządzania bezpieczeństwem



Obsługa i zgłaszanie incydentów

Systematyczne przeprowadzanie audytów bezpieczeństwa

Aby zrealizować te zadania, **operator usługi kluczowej musi albo powołać wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo, albo zawrzeć umowę z podmiotem zewnętrznym, który świadczy usługi z zakresu cyberbezpieczeństwa.**

Szczegółowe warunki organizacyjne i techniczne, jakie muszą spełnić operatorzy usług kluczowych, zostały określone w rozporządzeniu z 10 września 2018 roku. Jednak przepisy spotkały się z krytyką ze strony przedsiębiorców, którzy postulowali zmianę rozporządzenia. Przedsiębiorcy zgłaszali konieczność m.in.:

Wprowadzenia wymogu zastosowania zabezpieczeń adekwatnych do oszacowanego ryzyka w danej instytucji, a nie wpisanych „na sztywno" w rozporządzeniu.

Doprecyzowania zapisów o minimalnych wymogach ochrony fizycznej, w tym wprowadzenie mniej radykalnych przepisów dotyczących ochrony pomieszczeń.

Doprecyzowania zapisów dotyczących zabezpieczania śladów kryminalistycznych na potrzeby postępowań prowadzonych przez organy ścigania[13].

Stąd aktualizacja rozporządzenia[14].

Nowa Strategia Cyberbezpieczeństwa RP

22 października 2019 roku Rada Ministrów przyjęła uchwałę w sprawie *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024*. Dokument obowiązuje od 31 października 2019 roku i zastępuje *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022*. Przyjęcie *Strategii* wynika z *Ustawy o krajowym systemie cyberbezpieczeństwa z 5 lipca 2018 roku (art. 68)*.

Strategia jest dokumentem podobnym do *Krajowych Ram*, przyjętych w maju 2017 roku. O ile jednak *Krajowe Ramy* stanowiły zbiór założeń, którymi kierował się rząd przy opracowywaniu *Ustawy o krajowym systemie cyberbezpieczeństwa*, o tyle po przyjęciu samej ustawy, wizja zakłada „systematyczne wzmacnianie i rozwój krajowego systemu cyberbezpieczeństwa". Głównym celem przyjęcia i wdrożenia *Strategii* jest podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym, a także promowanie dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji.

12 Zgodnie z *Ustawą o krajowym systemie cyberbezpieczeństwa* operatorzy usług kluczowych to firmy i instytucje świadczące usługi o istotnym znaczeniu dla utrzymania krytycznej działalności społecznej lub gospodarczej. Operatorzy usług kluczowych są identyfikowani przez organy właściwe ds. cyberbezpieczeństwa na podstawie kryteriów określonych w rozporządzeniu z dnia 11 września 2018 roku. Wykaz tych podmiotów jest prowadzony przez ministra właściwego do spraw informatyzacji. Wpisanie do wykazu wiąże się z nałożeniem zadań określonych w ustawie.

13 Podsumowanie spotkania z przedsiębiorcami z branży cyberbezpieczeństwa (https://www.gov.pl/web/cyfryzacja/podsumowanie-spotkania-z-przedsiebiorcami-swiadczacymi-uslugi-z-zakresu-cyberbezpieczenstwa)

14 Więcej na ten temat możesz przeczytać na stronie: https://cyberpolicy.nask.pl/nowe-rozporzadzenie-ws-warunkow-organizacyjnych-i-technicznych-dla-operatorow-uslug-kluczowych/

Pięć celów szczegółowych polityki rządu określonych w Strategii

Rozwój krajowego systemu cyberbezpieczeństwa

Zwiększanie potencjału narodowego w zakresie bezpieczeństwa w cyberprzestrzeni

Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa

Zbudowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa

Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty

W obrębie każdego celu szczegółowego wyznaczono priorytety działania administracji.

- **Rozwój krajowego systemu cyberbezpieczeństwa:** wdrożenie i ocena funkcjonowania przepisów o krajowym systemie cyberbezpieczeństwa; podniesienie efektywności funkcjonowania krajowego systemu cyberbezpieczeństwa; rozbudowa systemu wymiany informacji na potrzeby kierowania bezpieczeństwem narodowym; zwiększenie cyberbezpieczeństwa usług kluczowych i cyfrowych oraz infrastruktury krytycznej; wypracowanie i wdrożenie metodyki szacowania ryzyka na poziomie krajowym oraz zwiększanie zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa i zdarzeń o charakterze terrorystycznym. Oznacza to, że rząd przewiduje aktualizację *Ustawy o krajowym systemie cyberbezpieczeństwa*, na podstawie doświadczeń wynikających z jej wdrażania. Bardzo ważnym elementem będzie także wypracowanie i wdrożenie metodyki szacowania ryzyka, co pozwoli na odpowiednie zarządzanie ryzykiem w skali kraju. Jest to bardzo duże przedsięwzięcie organizacyjne, ponieważ do tej pory analiza ryzyka nie była spójna. Taki cel pojawił się już w *Krajowych Ramach*, jednak nie udało się go zrealizować.
- **Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty:** opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa oraz promowanie dobrych praktyk i zaleceń; bezpieczeństwo łańcucha dostaw; testy i audyty cyberbezpieczeństwa. Opracowanie Narodowych

Standardów Cyberbezpieczeństwa ma wpłynąć przede wszystkim na zwiększenie odporności systemów teleinformatycznych administracji publicznej. Przewidziane są prace nad standardami dla aplikacji, urządzeń mobilnych oraz serwerów i sieci. W tym aspekcie bardzo istotne jest także wdrożenie *Aktu o Cyberbezpieczeństwie*, wprowadzającego certyfikację produktów i usług ICT. W Polsce musi zostać utworzony krajowy system oceny i certyfikacji w zakresie cyberbezpieczeństwa (m.in. powołanie lub ustanowienie Krajowego organu ds. certyfikacji cyberbezpieczeństwa (KOCC), Krajowej jednostki akredytującej oraz jednostek oceniających zgodność).

- **Zwiększenie potencjału narodowego w zakresie technologii cyberbezpieczeństwa: rozbudowa zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa:** nastawienie na rozwój współpracy między sektorem publicznym i prywatnym; stymulowanie badań i rozwoju w obszarze cyberbezpieczeństwa, a także uzyskanie zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni. Realizacja tego celu wydaje się szczególnie istotna, wobec trwającej w Europie i na świecie dyskusji na temat tzw. suwerenności cyfrowej.
- **Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa: zwiększanie kompetencji kadry podmiotów istotnych dla cyberbezpieczeństwa Rzeczypospolitej Polskiej:** stworzenie warunków do bezpiecznego korzystania z cyberprzestrzeni przez obywateli oraz rozwijanie świadomości społecznej w kierunku bezpiecznego korzystania z cyberprzestrzeni.
- **Zbudowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa:** rząd będzie prowadził aktywną współpracę międzynarodową na poziomie strategiczno-politycznym oraz operacyjnym i technicznym. Działania te są szczególnie istotne wobec planowanej nowelizacji dyrektywy NIS oraz uznania przez NATO cyberprzestrzeni za domenę działań operacyjnych.

Zarządzanie Strategią

Strategia, zgodnie z ustawą, jest uchwalana na 5 lat, a koordynatorem jej wdrażania jest minister właściwy ds. informatyzacji. Po dwóch latach dokument podlega przeglądowi i aktualizacji. Natomiast po sześciu miesiącach od przyjęcia strategii (kwiecień 2020 roku), minister właściwy ds. informatyzacji ma przedstawić *Plan działań na rzecz wdrożenia Strategii Cyberbezpieczeństwa*, opracowany we współpracy z członkami Rady Ministrów, kierownikami urzędów centralnych, dyrektorem Rządowego Centrum Bezpieczeństwa oraz innymi organami właściwymi określonymi w Ustawie o KSC.

Finansowanie

Rząd nie zapewnił funduszy na realizację zadań wynikających ze strategii. Dokument ma być realizowany z budżetów poszczególnych jednostek oraz ze środków Narodowego Centrum Badań i Rozwoju, a także z funduszy europejskich.

Budowa kompetencji RP w zakresie cyberobrony

Rok 2019 był okresem wzmożonej aktywności Ministra Obrony Narodowej w zakresie wzmacniania polskiej cyberobrony. Jest to bezpośrednie następstwo szczytu NATO, który w 2016 roku odbył się w Warszawie. Sojusz Północnoatlantycki uznał wtedy cyberprzestrzeń za kolejną domenę operacji oraz przyjął *Cyber Defence Pledge*[15]. Członkowie Sojuszu zadecydowali o zintegrowaniu swoich krajowych zasobów w zakresie cyberbezpieczeństwa z zasobami NATO.

W lutym 2019 roku powołano **pełnomocnika ds. utworzenia wojsk obrony cyberprzestrzeni (gen. Karol Molenda).** Był to początek centralizacji środowiska cyberbezpieczeństwa w Ministerstwie Obrony Narodowej. W marcu uruchomiono Program **CYBER.MIL.PL**. Jego celem jest zwiększenie bezpieczeństwa państwa i obywateli w cyberprzestrzeni. Program ma dwa obszary strategiczne: **kompleksowe wsparcie dla procesu formowania wojsk obrony cyberprzestrzeni oraz zintegrowanie środowiska cyberbezpieczeństwa resortu obrony narodowej.** Wojska obrony cyberprzestrzeni mają stanowić osobny rodzaj wojsk, a uzyskanie przez nie pełnej gotowości zajmie 4 lata. Bazą do ich powołania stanie się Centrum Operacji Cybernetycznych, które najpierw zostanie przekształcone w Siły Obrony Cyberprzestrzeni, a potem w wojska obrony cyberprzestrzeni. Uruchomienie programu zostało poprzedzone pracami zespołu roboczego, który wypracował szczegółową koncepcję budowania kompetencji MON w cyberprzestrzeni.

W resorcie, na bazie Narodowego Centrum Kryptologii, powołana została także nowa struktura: Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni (NCBC). Jest to wyspecjalizowana, elitarna jednostka podległa Ministrowi Obrony Narodowej, która odpowiada za kluczowe obszary związane z konsolidacją kompetencji i zasobów resortu w zakresie kryptologii i cyberbezpieczeństwa. Ma to być pewnego rodzaju hub, centralizujący działania MON w zakresie cyberbezpieczeństwa. W obrębie zdań NCBC znalazła się m.in. kryptologia. Dodatkowo centrum działa w trybie 24/7/365, zajmując się analizą i monitoringiem cyberprzestrzeni. W NCBC funkcjonuje także CSIRT MON – jeden z trzech CSIRT poziomu krajowego. W marcu 2019 roku pod NCBC podporządkowany został także Inspektorat Informatyki.

W ramach działań edukacyjnych Programu CYBER.MIL.PL, w marcu 2019 roku uruchomiona została inicjatywa *CYBER.MIL z klasą*. W jej ramach MON razem z Politechniką Łódzką, Polską Grupą Zbrojeniową oraz Liceum Ogólnokształcącym im. Józefa Chełmońskiego w Łowiczu zainicjowało pilotażowy program nauczania w zakresie cyberbezpieczeństwa. Program zakłada powstanie klas o profilu cyberbezpieczeństwo w liceach ogólnokształcących w mniejszych miejscowościach. MON podjął także działania związane ze wzmacnianiem oferty edukacyjnej na uczelniach wyższych. 1 września 2019 roku, przy Wojskowej Akademii Technicznej (WAT), rozpoczęło działalność Wojskowe Ogólnokształcące Liceum Informatyczne. Dodatkowo zwiększono limity przyjęć na studia wojskowe. Celem tych działań jest budowanie wyspecjalizowanych kadr na potrzeby Ministerstwa Obrony Narodowej[16].

Działaniem komplementarnym do Programu CYBER.MIL.PL jest formowanie Zespołu Działań Cybernetycznych w strukturze Wojsk

15 Dokument przyjęty na szczycie w Warszawie w 2016 roku jest wynikiem dążenia Sojuszu do zwiększenia nacisku na cyberodporność na poziomie krajowym. Sojusznicy zobowiązali się do podniesienia swojego poziomu cyberbezpieczeństwa. Najważniejsze postanowienia to m.in.: konieczność wzmocnienia cyberbezpieczeństwa krajowych sieci oraz infrastruktury; dotrzymywanie kroku szybko rozwijającym się cyberzagrożeniom, tak aby państwa NATO były w stanie skutecznie bronić się w cyberprzestrzeni; stosowanie prawa międzynarodowego w cyberprzestrzeni oraz współpraca z UE; międzynarodowa współpraca poprzez edukację, szkolenia oraz wymianę informacji.

16 Wojska Obrony Cyberprzestrzeni (https://www.gov.pl/web/obrona-narodowa/wojska-obrony-cyberprzestrzeni)

Obrony Terytorialnej, które rozpoczęło się 6 czerwca 2019 roku. Ofertę skierowano do osób, które nie chcą rezygnować ze swojej cywilnej kariery, ale są gotowe do służby na rzecz bezpieczeństwa militarnego w cyberprzestrzeni. Utworzenie w WOT komponentu odpowiedzialnego za cyberbezpieczeństwo daje możliwość pozyskania dla potrzeb obronności kraju wysokiej klasy specjalistów, którzy np. ze względów finansowych, nie chcą wstępować do wojska.

Polskie 5G – wiodąca rola państwa w budowaniu sieci nowej generacji?

Proces budowy w Polsce sieci 5G rozpoczął się w 2017 roku, kiedy przyjęto **porozumienie na rzecz Strategii 5G dla Polski.** Celem porozumienia było zainicjowanie współpracy pomiędzy sektorem publicznym, akademickim i prywatnym. Dokument został podpisany m.in. przez Urząd Komunikacji Elektronicznej i Instytut Łączności PIB, a także przedstawicieli operatorów, dostawców sprzętu, izb gospodarczych oraz uczelni technicznych. Efektem porozumienia było wypracowanie projektu strategii *5G dla Polski*, której konsultacje rozpoczęły się w styczniu 2018 roku. Po zakończeniu konsultacji, prace nad strategią zostały wstrzymane, a do końca 2019 roku dokument nie został oficjalnie przyjęty.

Natomiast w czerwcu 2018 roku opublikowano *Krajowy Plan działań zmiany przeznaczenia pasma 700 MHz w Polsce*, które docelowo ma być przeznaczone na usługi szerokopasmowe (sieć 5G). Obecnie pasmo zajmuje naziemna telewizja cyfrowa, która musi być przeniesiona w zakres 470-694 MHz (bez straty jakości). Jednak tym celu konieczne jest osiągniecie porozumienia z Federacją Rosyjską, która

użytkuje w paśmie 700 MHz systemy radiokomunikacyjne oraz telewizyjne. Dotąd się to nie udało. Z tego powodu przyjęta w lipcu 2019 roku aktualizacja *Krajowego Planu* wprowadziła zmianę terminu wykorzystania pasma 700 MHz dla sieci 5G do 30 czerwca 2022 roku.

W sierpniu 2019 roku Sejm RP przyjął **ustawę o zmianie ustawy o wspieraniu rozwoju usług i sieci telekomunikacyjnych oraz niektórych innych ustaw.** Tzw. megaustawa obowiązuje od października. Nowe przepisy mają wspierać usuwanie barier administracyjno-prawnych dla budowy sieci szerokopasmowych. Krótszy i prostszy ma być proces inwestycyjno-budowlany, dzięki czemu spadną koszty inwestycji, a operatorzy będą mogli w większym stopniu wykorzystywać infrastrukturę techniczną. Ustawa powołała także Fundusz Szerokopasmowy z rocznym budżetem 140 mln. zł. Środki te posłużą m.in. na dofinansowanie budowy i rozwoju sieci telekomunikacyjnych.

W październiku 2019 roku Polski Fundusz Rozwoju, Exatel, a także przedstawiciele T-Mobile, Orange i Polkomtela podpisali memorandum w sprawie analizy modelu biznesowego **dla spółki #Polskie5G.** Spółka ma być hurtowym operatorem ogólnopolskiej bezprzewodowej sieci 5G w paśmie 700 MHz i zapewniać dostęp do usług 5G w całej Polsce. Zaproponowany model zakłada, że poprzez spółkę celową, to właśnie państwo będzie właścicielem jednolitej infrastruktury dla pasma pokryciowego 700 MHz. Efektem będzie kontrola państwowa nad tym, jakie firmy zostaną dopuszczone do budowy sieci 5G w Polsce. Takie rozwiązanie pozwoli na obniżenie kosztów budowy infrastruktury telekomunikacyjnej, co przełoży się na konkurencyjne ceny usług.

Przedłużające się poszukiwania polskiej Sztucznej Inteligencji

W 2018 roku rozpoczęły się w Polsce prace nad założeniami do strategii Sztucznej Inteligencji. W Ministerstwie Cyfryzacji powołano wtedy grupy robocze, składające się z przedstawicieli biznesu, nauki i przemysłu, które wypracowały dokument *Założenia do strategii AI w Polsce*. Zawierał on plan na lata 2018-2019. Działania podjęte w 2018 roku nie miały jednak żadnych poważnych następstw[17].

26 maja 2019 roku Minister Cyfryzacji, Minister Inwestycji i Rozwoju, Minister Nauki i Szkolnictwa Wyższego oraz Minister Przedsiębiorczości i Technologii podpisali memorandum na rzecz rozwoju Sztucznej Inteligencji w Polsce. W memorandum zapowiedziano podjęcie wspólnych działań, zmierzających do utworzenia strategicznych ram dla dynamicznego rozwoju technologii i szerokich zastosowań Sztucznej Inteligencji w Polsce.

Efektem było powołanie międzyresortowego zespołu analityczno-redakcyjnego, który opracował projekt *Polityki Rozwoju Sztucznej Inteligencji w Polsce na lata 2019-2027*. Jest to bardzo obszerny dokument. Zgodnie z jego zapisami, Polska do 2025 roku ma dołączyć do grona 20-25 % państw wiodących w rozwoju Sztucznej Inteligencji na świecie. Oznacza to, że w ciągu najbliższych 5 lat przedsiębiorstwa rozwijające Sztuczną Inteligencję, muszą zwiększyć swoją wielkość blisko 25-krotnie.

21 sierpnia 2019 roku rozpoczęły się konsultacje społeczne, które wypadły niekorzystnie. Do końca 2019 roku nie zaprezentowano kolejnej wersji dokumentu.

17 Więcej na ten temat możesz przeczytać w: *Raport Cyberbezpieczeństwo A.D. 2018. Strategia. Policy. Rekomendacje – cyberbezpieczeństwo w perspektywie policy* (https://cyberpolicy.nask.pl/wp-content/uploads/2019/04/Raport-Cyberbezpiecze%C5%84stwo-A.D.-2018.pdf)

UNIA EUROPEJSKA

Unia Europejska, UE *(European Union)* powstała w 1993 roku w wyniku wieloletniego procesu integracji zakończonego podpisaniem Traktatu z Maastrich. Obecnie UE skupia 27 państw członkowskich. Najważniejsze unijne organy to: Komisja Europejska, KE *(European Commission)* reprezentująca władzę wykonawczą i posiadająca inicjatywę wykonawczą, Rada Unii Europejskiej, Rada UE *(Council of the European Union)* główny organ decyzyjny oraz Parlament Europejski, PE *(European Parliament)* reprezentujący władzę ustawodawczą.

Najważniejsze wydarzenia w UE w 2019 roku

26 marca

Komisja Europejska opublikowała rekomendacje dotyczące działań i środków operacyjnych bezpieczeństwa sieci 5G w Unii Europejskiej.

8 kwietnia

Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji opublikowała wytyczne w sprawie etycznej i godnej zaufania Sztucznej Inteligencji.

17 kwietnia

Parlament Europejski i Rada UE wydały rozporządzenie w sprawie Europejskiej Agencji ds. Cyberbezpieczeństwa (ENISA) oraz certyfikacji cyberbezpieczeństwa *(Akt o cyberbezpieczeństwie)*.

11 czerwca

Komisja Europejska opublikowała wyniki Indeksu Gospodarki Cyfrowej i Społeczeństwa Cyfrowego DESI 2019.

26 czerwca

Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji opublikowała wytyczne w sprawie regulacji i inwestycji dla godnej zaufania Sztucznej Inteligencji.

27 czerwca

Wejście w życie Aktu o Cyberbezpieczeństwe *(Cybersecurity Act, CA)*. To druga, po dyrektywie NIS, ogólnoeuropejska regulacja w dziedzinie cyberbezpieczeństwa. CA składa się z dwóch części:

- Nowy permanentny mandat dla ENISA, której nazwa została zmieniona z Europejskiej Agencji Bezpieczeństwa Sieci i Informacji na Agencja UE ds. Cyberbezpieczeństwa. Rola ENISA została znacznie wzmocniona, nie tylko poprzez permanentny mandat, ale także poprzez szereg nowych obowiązków związanych z wejściem w życie Dyrektywy NIS oraz europejskich ram certyfikacji.
- Rozporządzenie tworzące europejskie ramy certyfikacji cyberbezpieczeństwa dla produktów i usług ICT. Jest to bardzo istotna regulacja, która znacznie zmieni funkcjonujący obecnie model certyfikacji, zdominowany przez SOG-IS *(Senior Official Group Information Security Systems*[18]*)*.

16 lipca

Zarząd Europejskiej Agencji ds. Cyberbezpieczeństwa (ENISA) wybrał nowego Dyrektora Wykonawczego.

18 Porozumienie SOG-IS zostało zawarte w 1997 roku, w odpowiedzi na decyzję Rady UE z marca 1992 roku. Sygnatariusze porozumienia mogą samodzielnie oceniać i certyfikować produkty i usługi sektora IT, zgodnie z międzynarodową normą OSO/IEC 15408, która pozwala zweryfikować bezpieczeństwo systemów teleinformatycznych pod względem formalnym. Polska dołączyła do grupy państw sygnatariuszy porozumienia SOG-IS w 2017 roku.

6 sierpnia

Europejska Agencja ds. Cyberbezpieczeństwa (ENISA) otrzymała zadanie przygotowania pierwszej propozycji europejskiego programu certyfikacji cyberbezpieczeństwa.

9 października

Grupa Współpracy NIS opublikowała unijną skoordynowaną ocenę ryzyka związanego z cyberbezpieczeństwem w sieciach 5G.

21 października

Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji opublikowała raport poświęcony odpowiedzialności za Sztuczną Inteligencję i inne nowe technologie.

21 listopada

Europejska Agencja ds. Cyberbezpieczeństwa (ENISA) opublikowała raport poświęcony zagrożeniom związanym z siecią 5G.

2 grudnia

Komisja Europejska zwróciła się z prośbą do Europejskiej Agencji ds. Cyberbezpieczeństwa (ENISA) o przygotowanie planu certyfikacji cyberbezpieczeństwa dla usług w chmurze.

W 2019 roku Unia Europejska prowadziła aktywne działania na rzecz ułatwienia państwom członkowskim przygotowań do zmian społeczno-gospodarczych spowodowanych cyfrową rewolucją. Jednym z najważniejszych wydarzeń minionego roku było przyjęcie *Aktu o Cyberbezpieczeństwie (Cybersecurity Act),* drugiej po Dyrektywie NIS ogólnoeuropejskiej regulacji w obszarze cyberbezpieczeństwa. Wprowadzenie permanentnego mandatu dla ENISA i przekazanie Agencji nowych obowiązków znacznie wzmocniło pozycję ENISA w unijnych strukturach. *Akt o Cyberbezpieczeństwie* ustanowił również *Ramy Europejskiej Certyfikacji Cyberbezpieczeństwa.* Jest to pierwsze prawo dotyczące rynku wewnętrznego.

Niezwykle istotnym tematem, który w znacznym stopniu zdominował 2019 rok, jest doprowadzenie do wdrożenia sieci 5G. Według KE ma ona kluczowe znaczenie dla rozwoju społeczno-gospodarczego Unii Europejskiej, ale konieczne jest zapewnienie odpowiedniego poziomu bezpieczeństwa. W związku z tym 26 marca 2019 roku Komisja Europejska opublikowała rekomendacje dotyczące działań i środków operacyjnych bezpieczeństwa sieci 5G w Unii Europejskiej *(Cybersecurity of 5G networks).* Państwa członkowskie zostały zobligowane m.in. do przygotowania krajowych ocen ryzyka infrastruktury sieci 5G. Wypracowane dokumenty stanowiły wkład dla wspólnego unijnego przeglądu podatności związanych z siecią nowej generacji, który opublikowano w październiku.

Rok 2019 przyniósł także nowe wytyczne i rekomendacje w obszarze etyki i prawnej odpowiedzialności za Sztuczną Inteligencję. Inicjatywy rozpoczęte jeszcze w 2018 roku[19], były kontynuowane. UE dokłada starań, aby rozwiązania wypracowane w Europie były

19 Więcej na ten temat możesz przeczytać w: *Raport Cyberbezpieczeństwo A.D. 2018. Strategia. Policy. Rekomendacje – cyberbezpieczeństwo w perspektywie policy,* str. 32-34 (https://cyberpolicy.nask.pl/wp-content/uploads/2019/04/Raport-Cyberbezpiecze%C5%84stwo-A.D.-2018.pdf)

zgodne z prawami człowieka i europejskim prawodawstwem. Grupa Ekspertów ds. Sztucznej Inteligencji opublikowała:

- *Wytyczne w sprawie etyki godnej zaufania Sztucznej Inteligencji (The Ethics Guidelines for Trustworthy Artificial Intelligence (AI)).*
- *Definicję Sztucznej Inteligencji (A definitione of AI: Main capabilities and disciplines).*
- *Wytyczne w sprawie regulacji i inwestycji dla godnej zaufania Sztucznej Inteligencji (Policy and investment recommendations for trustworthy Artificial Intelligence).*

Komisja Europejska wydała również komunikat *Budowanie zaufania do Sztucznej Inteligencji ukierunkowanej na człowieka (Building Trust in Human Centric Artificial Intelligence)*, w którym stwierdziła, że Sztuczna Inteligencja nie może być celem samym w sobie, ale godnym zaufania narzędziem, szanującym demokrację, ludzką godność i ostatecznie służącym wzmacnianiu dobrobytu człowieka.

Wiele działo się także w tematyce danych. Po regulacjach związanych z ochroną prywatności (RODO/GDPR) oraz ponownym wykorzystaniem *(Dyrektywa PSI/reuse – Dyrektywa w sprawie ponownego wykorzystania informacji sektora publicznego)*, przyszedł czas na dane nieosobowe. 29 maja 2019 roku Komisja Europejska opublikowała komunikat na temat wytycznych dotyczących rozporządzenia w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej. W czerwcu została przyjęta *Dyrektywa w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego*. Zgodnie z regulacją, państwa członkowskie mają zapewnić możliwość ponownego wykorzystania: dokumentów organów sektora publicznego, dokumentów przedsiębiorstw publicznych oraz danych badawczych.

Najważniejsze tematy podejmowane przez UE w 2019 roku

Cybersecurity Act – nowe prawo UE w zakresie cyberbezpieczeństwa

Jednym z najważniejszych wydarzeń w Unii Europejskiej w 2019 roku było przyjęcie *Aktu o Cyberbezpieczeństwie (Cybersecurity Act, CA)*[20]. **CA wszedł w życie 27 czerwca 2019 roku** i jest drugą, po Dyrektywie NIS ogólnoeuropejską regulacją w dziedzinie cyberbezpieczeństwa.

Akt o Cyberbezpieczeństwie składa się z dwóch części:

Nowego permanentnego mandatu dla Agencji UE ds. Cyberbezpieczeństwa *(European Union Agency for Cybersecurity, ENISA)*

Rozporządzenia tworzącego europejskie ramy certyfikacji cyberbezpieczeństwa dla produktów i usług informacyjno-komunikacyjnych.

Nowy, permanentny mandat ENISA

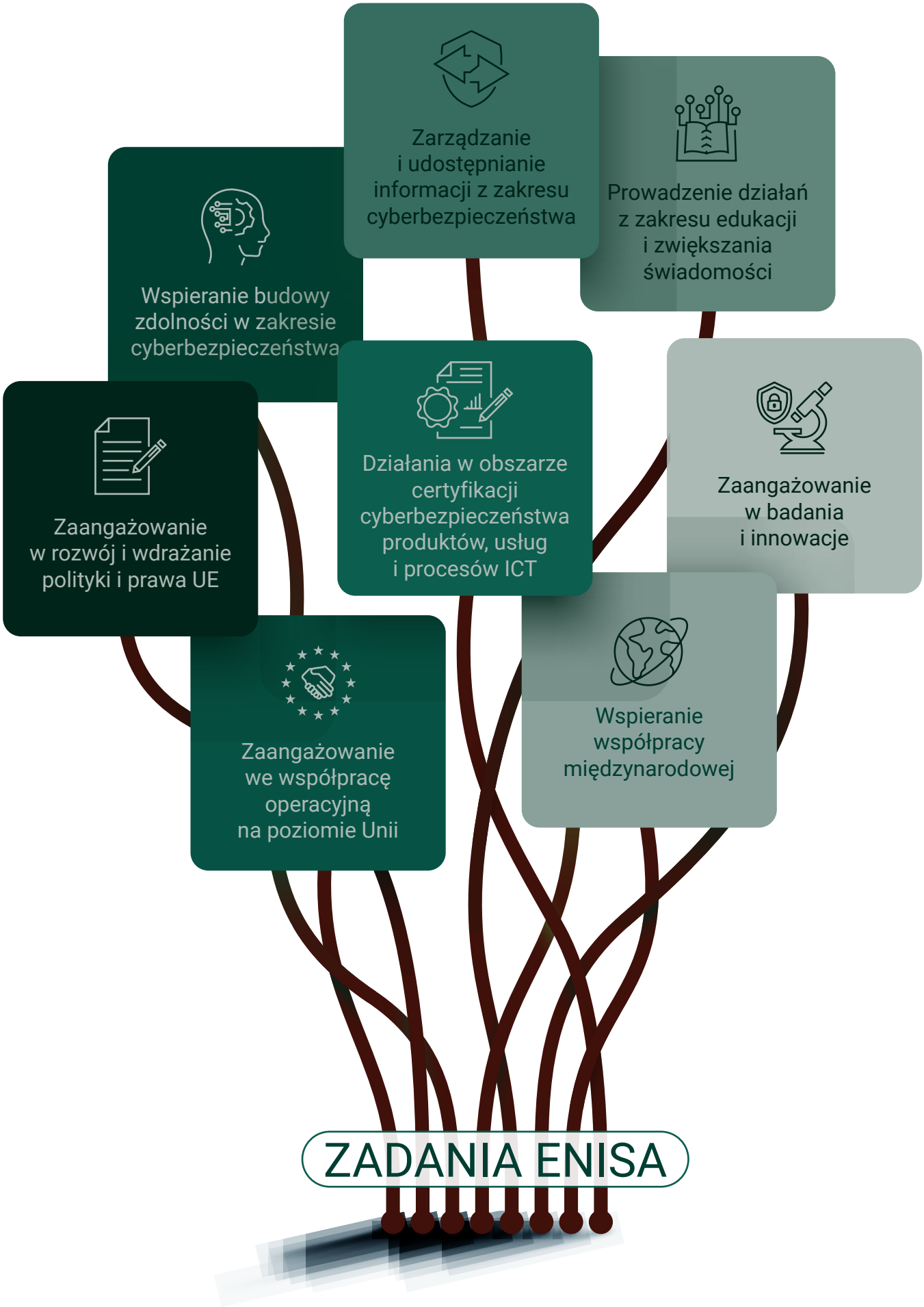
Wraz z przyjęciem CA, Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji otrzymała permanentny mandat. Zmieniła się także nazwa Agencji, która obecnie brzmi: Agencja UE ds. Cyberbezpieczeństwa. CA wzmacnia rolę ENISA w zakresie współpracy z państwami członkowskimi, zespołami CERT i CERT-EU, służbami i organami nadzorującymi ochronę prywatności. W ramach współpracy ENISA monitoruje stan cyberbezpieczeństwa UE i przygotowuje raport z uwzględnieniem zgłoszeń naruszenia bezpieczeństwa ze wszystkich państw członkowskich. Nowym obszarem odpowiedzialności Agencji jest wspieranie i promowanie wdrożenia certyfikacji produktów, usług i procesów ICT. To właśnie ENISA przygotowuje propozycje programu certyfikacji, które następnie są przekazywane do KE. W 2019 roku Agencja rozpoczęła już prace nad przygotowaniem pierwszej propozycji europejskiego programu certyfikacji cyberbezpieczeństwa. Grupa ekspertów pomoże wypracować "spadkobiercę" SOG-IS[21]. ENISA przewodniczy również Grupie Interesariuszy ds. Certyfikacji Cyberbezpieczeństwa. Grupa zajmuje się doradztwem KE w kwestiach strategicznych dot. certyfikacji[22].

Reprezentantem ENISA jest Dyrektor Wykonawczy. W ramach Agencji działa Zarząd, Rada Wykonawcza, Dyrektor Wykonawczy, Grupa Doradcza ENISA i Sieć Krajowych Urzędników Łącznikowych. 16 lipca 2019 roku Zarząd ENISA wybrał Juhana Lapassaara na stanowisko nowego Dyrektora Wykonawczego. Potem, podczas październikowych wyborów, wybrano Przewodniczącego i Wiceprzewodniczącego Zarządu. Wiceprzewodniczącym ponownie został Krzysztof Silicki – Zastępca Dyrektora NASK PIB, Dyrektor ds. Cyberbezpieczeństwa i Innowacji NASK.

20 **Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013**

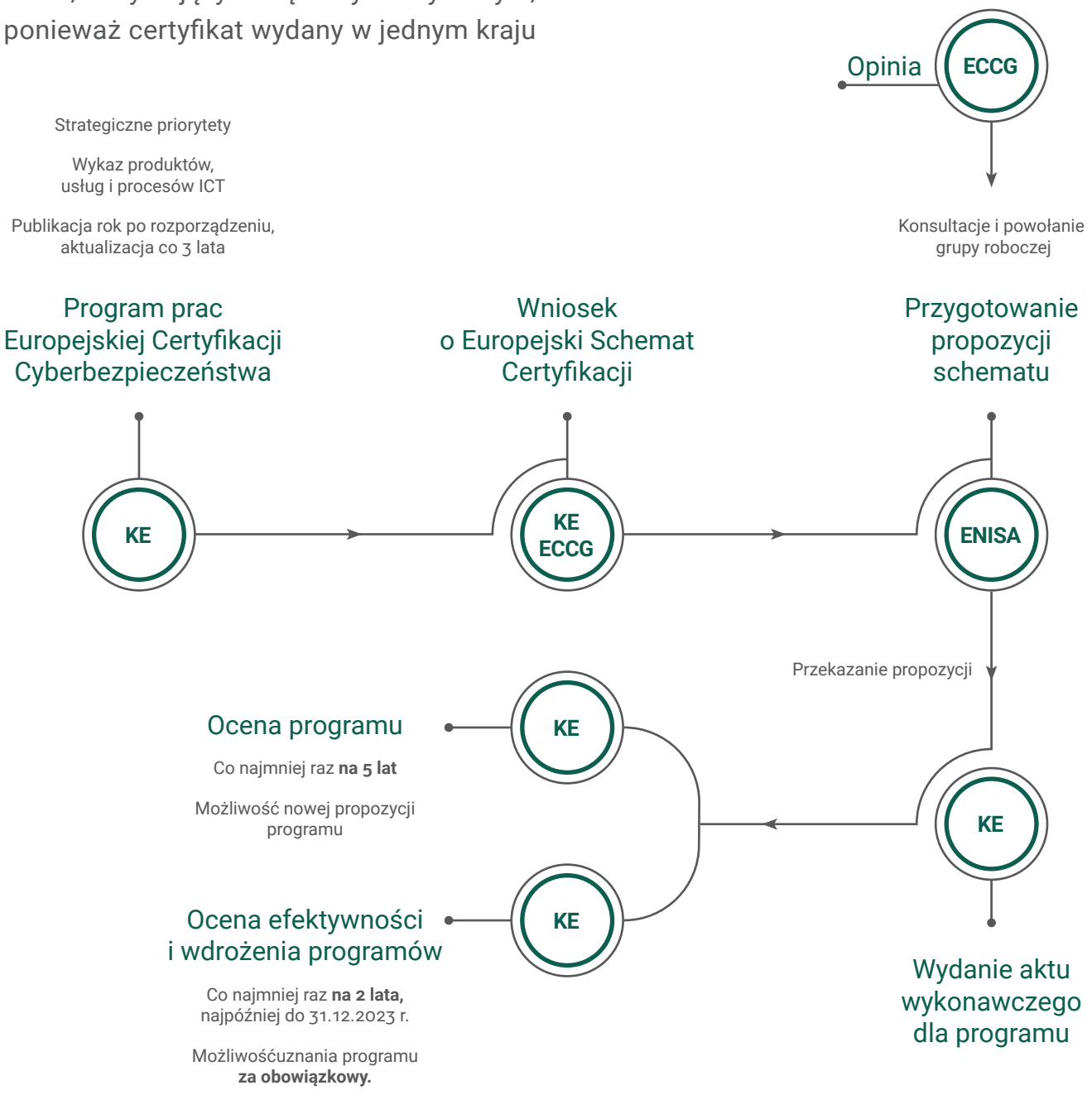
21 SOG-IS *(Senior Official Group Information Security Systems)* Porozumienie SOG-IS zostało zawarte w 1997 roku, w odpowiedzi na decyzję Rady UE z marca 1992. Sygnatariusze porozumienia mogą samodzielnie oceniać i certyfikować produkty i usługi sektora IT, zgodnie z międzynarodową normą OSO/IEC 15408, która pozwala zweryfikować bezpieczeństwo systemów teleinformatycznych pod względem formalnym. Polska dołączyła do grupy państw sygnatariuszy porozumienia SOG-IS w 2017 roku.

22 Więcej na temat nowego mandatu ENISA na stronie: https://cyberpolicy.nask.pl/akt-o-cyberbezpieczenstwie-nowy-mandat-enisa/


Zarządzanie i udostępnianie informacji z zakresu cyberbezpieczeństwa
Prowadzenie działań z zakresu edukacji i zwiększania świadomości
Wspieranie budowy zdolności w zakresie cyberbezpieczeństwa
Działania w obszarze certyfikacji cyberbezpieczeństwa produktów, usług i procesów ICT
Zaangażowanie w badania i innowacje
Zaangażowanie w rozwój i wdrażanie polityki i prawa UE
Wspieranie współpracy międzynarodowej
Zaangażowanie we współpracę operacyjną na poziomie Unii
ZADANIA ENISA

Certyfikacja produktów i usług ICT

Poza permanentnym mandatem dla ENISA, *Akt o Cyberbezpieczeństwie* wprowadza również **Ramy Europejskiej Certyfikacji Cyberbezpieczeństwa.** Rozporządzenie w sprawie certyfikacji cyberbezpieczeństwa to pierwsze prawo dotyczące rynku wewnętrznego, które odpowiada na potrzebę podniesienia poziomu bezpieczeństwa produktów, usług i procesów ICT. Stworzenie *Ram Europejskiej Certyfikacji Cyberbezpieczeństwa* jest pewnego rodzaju przełomem, który ma umożliwić zniesienie barier, utrzymujących się na rynku cyfrowym, ponieważ certyfikat wydany w jednym kraju członkowskim będzie ważny na obszarze całej UE. Jednak, aby to osiągnąć, konieczne jest wypracowanie harmonijnego podejścia do certyfikacji cyberbezpieczeństwa. Dlatego rozporządzenie określa mechanizm ustanawiania europejskich programów certyfikacji cyberbezpieczeństwa oraz potwierdzania, że dane produkty bądź usługi spełniają określone wymogi bezpieczeństwa (tzw. poziom uzasadnienia zaufania). Poniższy schemat przedstawia proces tworzenia certyfikatu na poziomie UE.



Celem regulacji jest doprowadzenie do sytuacji, w której konsument będzie mógł wybierać takie urządzenia i rozwiązania, które są przetestowane i spełniają odpowiednie normy bezpieczeństwa. Z kolei firmy nie będą musiały ubiegać się o certyfikat w każdym kraju, w którym chciałyby oferować swoje usługi bądź produkty, co pozwoli na oszczędzenie czasu i środków. Co więcej, firmy które zainwestują w cyberbezpieczeństwo, będą mogły wykorzystać ten fakt jako swoją przewagę nad konkurencją.

Wejście w życie tych przepisów oznacza liczne wyzwania dla państw, takich jak Polska, które nie podejmowały dotąd żadnych kroków w kierunku stworzenia krajowych programów certyfikacji cyberbezpieczeństwa. W lepszej sytuacji znajdą się te państwa członkowskie, które nie będą musiały budować od podstaw odpowiednich kompetencji oraz infrastruktury np. do testowania certyfikowanego sprzętu (Francja, Niemcy).

O ile przygotowanie programów certyfikacji cyberbezpieczeństwa odbywa się na poziomie europejskim, o tyle sam proces certyfikacji przebiega na poziomie krajowym. CA nakłada na państwa członkowskie konkretne obowiązki, które mają pomóc w budowie sprawnego, krajowego systemu certyfikacji cyberbezpieczeństwa. Wprowadzenie rozporządzenia w Polsce będzie więc wymagało zmian prawnych. W Ministerstwie Cyfryzacji przy grupie ds. cyberbezpieczeństwa uruchomiono specjalną podgrupę, która zajmuje się tym wyzwaniem. Nie zdecydowano jeszcze, czy zmiany prawne zostaną dokonane poprzez nowelizacje *Ustawy o krajowym systemie cyberbezpieczeństwa*, czy innego aktu prawnego. Polska musi jednak zadbać o powołanie:

Krajowego organu ds. certyfikacji cyberbezpieczeństwa (KOCC)

Krajowej jednostki akredytującej[23]

Jednostek oceniających zgodność

Akt o Cyberbezpieczeństwie – certyfikacja produktów i usług na poziomie UE

- Wprowadzenie dobrowolnej certyfikacji produktów, usług i procesów ICT.
- Możliwość wprowadzenia obowiązkowej certyfikacji dla wybranych produktów, usług i procesów ICT.
- Określenie trzech poziomów bezpieczeństwa dla certyfikowanych usług, produktów i procesów ICT: podstawowy, istotny i wysoki.
- Obowiązek powołania przez państwa członkowskie krajowych organów ds. certyfikacji cyberbezpieczeństwa.
- Ustanowienie *Europejskiej Grupy Certyfikacji Cyberbezpieczeństwa.*
- Rozporządzenie wymaga zmian prawnych w Polsce (np. w *Ustawie o krajowym systemie cyberbezpieczeństwa*)[24].

23 Każde państwo członkowskie wyznacza jedną krajową jednostkę akredytującą. W Polsce jest to Polskie Centrum Akredytacji, które akredytuje jednostki oceniające zgodność, gdy spełniają określone wymogi. Na podstawie *Rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiającego wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93.*

24 Więcej na temat certyfikacji produktów i usług ICT na stronie: https://cyberpolicy.nask.pl/akt-o-cyberbepzieczenstwie-certyfikacja-cyberbezpieczenstwa/#_ftn2

Wdrożenie sieci 5G – nowe wyzwanie dla Europy

Sieć 5G, czyli co?

5G to piąta, a zarazem najnowsza, generacja mobilnych sieci telekomunikacyjnych. Trzy główne rodzaje usług, czyli tzw. scenariusze zastosowań dla 5G, określił Międzynarodowy Związek Telekomunikacyjny (ITU) w standardzie IMT-2020. Są to:

- **Ulepszony mobilny szerokopasmowy dostęp do internetu** (wirtualna rzeczywistość, streaming gier online, filmy w wysokiej jakości).
- **Masowa komunikacja między maszynami** (Internet Rzeczy, inteligentne miasta).
- **Niezwykle niezawodna transmisja o niskim opóźnieniu** (pojazdy autonomiczne, zdalne operacje medyczne).

5G nie jest po prostu rozwinięciem sieci 4G. Zupełnie nowe rozwiązania pojawią się w sieci szkieletowej: m.in. wirtualizacja sieci i możliwość jej segmentacji. Co ważne 5G wykorzysta trzy różne częstotliwości, a nowością będą częstotliwości milimetrowe (np. pasmo 26 GHz), których dotychczas nie stosowano w sieciach komórkowych. To z kolei wymusi daleko idące zmiany w radiowej sieci dostępowej. Zwłaszcza w miastach stacji bazowych będzie znacznie więcej.

Jednym z najważniejszych tematów, podejmowanych w 2019 roku, było wdrożenie sieci 5G. Zdaniem KE będzie ona miała kluczowe znaczenie dla rozwoju społeczno-gospodarczego Unii Europejskiej. W związku z tym podjęto działania zmierzające do zapewnienia wysokiego poziomu cyberbezpieczeństwa sieci 5G na obszarze całej UE, a także koordynacji wysiłku państw członkowskich w tym zakresie.

Najpierw, **26 marca** Komisja Europejska opublikowała rekomendacje *Cybersecurity of 5G networsks*[25]. Celem dokumentu, który zawierał opis działań operacyjnych na poziomie Unii Europejskiej i państw członkowskich, było wypracowanie wspólnego podejścia do bezpieczeństwa sieci 5G. KE zwróciła uwagę na konieczność przyjęcia specjalnych regulacji i ustanowienia spójnej polityki reagowania na incydenty w cyberprzestrzeni. Zdaniem Komisji podstawowym narzędziem, wspierającym wprowadzanie sieci 5G w państwach członkowskich, powinny być europejskie ramy certyfikacji cyberbezpieczeństwa, które w przyszłości zapewnią wysoki poziom bezpieczeństwa w całym cyklu sieci 5G. Ponadto państwa członkowskie zostały zobowiązane do przeprowadzenia krajowej analizy ryzyka sieci oraz aktualizacji wymagań bezpieczeństwa i zarządzania ryzykiem. Termin przekazania krajowych ocen ryzyka do ENISA został wyznaczony na 15 lipca 2019 roku. KE postanowiła również powołać działającą na szczeblu unijnym Grupę Współpracy, która do końca roku miała stworzyć niezbędny zestaw narzędzi do reagowania na incydenty zagrażające bezpieczeństwu sieci[26]. W rekomendacjach zalecono państwom członkowskim ścisłą współpracę z unijnymi organami przy tworzeniu wymogów bezpieczeństwa dla zamówień publicznych dotyczących sieci 5G.

25 Commission Recommendation of 26.3.2019 Cybersecurity of 5G networks. (https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58154)
26 Toolbox został ostatecznie opublikowany w dniu 29 stycznia 2020 roku.

Istotnym krokiem w kierunku wdrożenia sieci 5G w Europie było podjęcie przez Komisję Europejską *Decyzji wykonawczej w dniu 14 maja 2019*[27] w celu zharmonizowania widma radiowego w paśmie 24,25-27,5 GHz. KE zobligowała państwa członkowskie do wyznaczenia i udostępnienia na zasadzie braku wyłączności, zakresu częstotliwości 24,25-27,5 GHz na potrzeby naziemnych systemów świadczących szerokopasmowy dostęp do usług cyfrowych. Zakres tych częstotliwości został przyjęty przez KE jako odpowiedni do celów standardu Międzynarodowej Telekomunikacji Ruchomej (IMT-2020), opracowanego przez Sektor Radiokomunikacji Międzynarodowego Związku Telekomunikacyjnego (ITU). Termin wykonania zarządzenia upływa 30 marca 2020 roku. Państwa członkowskie zostały zobowiązane do złożenia KE sprawozdań z wykonania tej decyzji.

19 lipca 2019 roku Komisja Europejska wydała oświadczenie w sprawie przedłożenia przez państwa członkowskie UE krajowych ocen ryzyka bezpieczeństwa sieci 5G. Oceny te zostały następnie przeanalizowane przez KE i ENISA. Opis najważniejszych zagrożeń, podatności, słabych punktów i przykładowych scenariuszy ryzyka sieci 5G został opublikowany **9 października 2019 roku** w raporcie Grupy Współpracy NIS *EU coordinated risk assessment of the cybersecurity of 5G networks*[28]. Autorzy ekspertyzy zwrócili uwagę na szczególną rolę operatorów sieci komórkowych i producentów sprzętu telekomunikacyjnego w zapewnieniu cyberbezpieczeństwa sieci 5G. Warto podkreślić, że 17 maja 2019 roku Rada UE wydała r*ozporządzenie w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim*[29].

Pod koniec roku, **21 listopada 2019 roku** ENISA opublikowała raport *ENISA Threat Landscape for 5G Network*[30]. Publikacja przedstawia krajobraz zagrożeń i wyzwań związanych z bezpieczeństwem sieci 5G ze szczególnym uwzględnieniem architektury i komponentów sieci 5G. Raport stanowi uzupełnienie i rozwinięcie skoordynowanej unijnej oceny ryzyka cyberbezpieczeństwa sieci 5G[31] stworzonej przez Grupę Współpracy NIS w październiku 2019 roku. Publikacja zawiera również rekomendacje dotyczące UE, interesariuszy i właściwych organów krajowych. Wśród zaproponowanych przez autorów działań znalazły się m.in.: dzielenie się wiedzą na temat 5G z interesariuszami, promowanie współpracy między zainteresowanymi stronami, a także aktualizowanie informacji na temat zagrożeń teleinformatycznych i udostępnianie ich interesariuszom.

Europejska, godna zaufania Sztuczna Inteligencja (SI)

W 2019 roku UE kontynuowała, rozpoczęte rok wcześniej, działania w zakresie Sztucznej Inteligencji[32]. Zdaniem KE, technologie wykorzystujące Sztuczną Inteligencję mogą rozwiązać wiele problemów społecznych i istotnie przyczynić się do rozwoju gospodarczego Unii Europejskiej. Równocześnie jednak powstaje szereg wyzwań, które państwa członkowskie starają się zaadresować, przede wszystkim w prawnych i etycznych aspektach towarzyszących powstaniu SI. Chodzi o to, żeby europejska Sztuczna Inteligencja jak najbardziej przypominała obywatela UE, a więc miała poszanowanie dla unijnych regulacji prawnych np. w zakresie prywatności.

27 *Commission Implementing Decision(EU) 2019/784 of 14 May 2019 on harmonisation of the 24,25-27,5 GHz frequency band for terrestrial systems capable of providing wireless broadband electronic communications services in the Union* (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019D0784)
28 *Report on the EU coordinated risk assessment on cybersecurity in Fifth Generation (5G) networks* (https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049)
29 *Rozporządzenie w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim* (https://eur-lex.europa.eu/legal content/PL/TXT/PDF/?uri=CELEX:32019R0796&from=EN)
30 ENISA Threat Landscape for 5G Network (https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks)
31 https://cyberpolicy.nask.pl/unijna-ocena-ryzyka-cyberbezpieczenstwa-w-sieciach-5g/
32 Więcej na ten temat możesz przeczytać w Raporcie *Cyberbezpieczeństwo A.D. 2018. Strategia. Policy. Rekomendacje – cyberbezpieczeństwo w perspektywie policy* (https://cyberpolicy.nask.pl/wp-content/uploads/2019/04/Raport-Cyberbezpiecze%C5%84stwo-A.D.-2018.pdf)

Grupa Ekspertów ds. Sztucznej Inteligencji

W czerwcu 2018 roku Komisja Europejska powołała Grupę Ekspertów ds. Sztucznej Inteligencji. Składa się ona z 52 członków reprezentujących środowisko akademickie, przemysł i społeczeństwo obywatelskie. Celem grupy jest wspieranie procesu wdrażania europejskiej strategii dotyczącej Sztucznej Inteligencji ze szczególnym uwzględnieniem kwestii etycznych, prawnych i społecznych. Grupa ekspertów oprócz funkcji doradczej pełni również funkcję grupy sterującej *AI Alliance* – platformy wymiany wiedzy i doświadczeń z obszaru nowych technologii i Sztucznej Inteligencji. Gospodarzem platformy *AI Alliance*, zrzeszającej ponad 3500 członków, jest Komisja Europejska. Rola grupy sterującej polega na stymulowaniu dyskusji, zbieraniu opinii i wyznaczaniu przyszłego kierunku kształtowania polityki Sztucznej Inteligencji w Europie.

8 kwietnia 2019 roku Grupa Ekspertów ds. Sztucznej Inteligencji[33] opublikowała ostateczną wersję Wytycznych w sprawie etyki godnej zaufania sztucznej inteligencji *(The Ethics Guidelines for Trustworthy Artificial Intelligence (AI))*. Wytyczne zawierają **7 kluczowych wymagań dla godnej zaufania sztucznej inteligencji.** (więcej szczegółów w rozdziale Sztuczna Inteligencja). Dokument był przedmiotem konsultacji społecznych od grudnia 2018 roku.

3 cechy godnej zaufania Sztucznej Inteligencji

Solidna

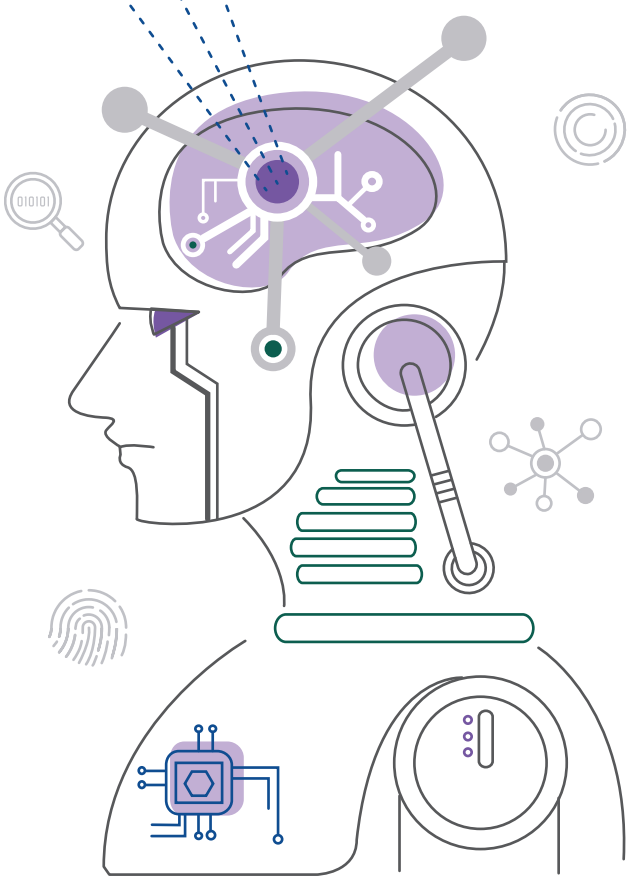
Zarówno z technicznego, jak i społecznego punktu widzenia, ponieważ systemy SI mogą wywoływać niezamierzone szkody nawet wówczas, gdy korzysta się z nich w dobrej wierze.

Zgodna z prawem

Zapewnia poszanowanie wszystkich obowiązujących przepisów ustawowych i wykonawczych.

Etyczna

Zapewnia zgodność z zasadami i wartościami etycznymi.



33 Grupa Ekspertów ds. Sztucznej Inteligencji została powołana przez KE w czerwcu 2018 roku. W jej skład weszło 52 ekspertów reprezentujących ośrodki akademickie, biznes i społeczeństwo obywatelskie. Zadaniem grupy było opracowanie rekomendacji w zakresie rozwoju polityki Sztucznej Inteligencji.

Równolegle (8 kwietnia 2019 roku) Grupa Ekspertów ds. Sztucznej Inteligencji opublikowała dokument *Definicja sztucznej inteligencji: główne funkcje i dyscypliny (A definitione of AI: Main capabilities and disciplines*[34]), w którym zawarta została rozszerzona definicja Sztucznej Inteligencji. Dokument wyjaśnia także pewne aspekty Sztucznej Inteligencji jako dyscypliny naukowej.

Definicja Sztucznej Inteligencji:

Przyjęto, że termin Sztuczna Inteligencja odnosi się do oprogramowania komputerowego (w tym sprzętu) stworzonego przez człowieka, które biorąc pod uwagę złożony cel, działają w wymiarze fizycznym lub cyfrowym poprzez postrzeganie ich otoczenia dzięki gromadzeniu danych, interpretacji zebranych ustrukturyzowanych lub nieustrukturyzowanych danych, rozumowaniu na podstawie wiedzy lub przetwarzaniu informacji pochodzących z tych danych oraz podejmowaniu decyzji w sprawie najlepszych działań, które należy podjąć w celu osiągnięcia określonego celu.

Systemy SI mogą wykorzystywać symboliczne reguły albo uczyć się modelu numerycznego, a także dostosowywać swoje zachowanie, analizując wpływ poprzednich działań na otoczenie. 26 czerwca odbyło się pierwsze zgromadzenie *AI Alliance*[35], na którym Grupa Ekspertów ds. Sztucznej Inteligencji opublikowała Wytyczne w sprawie regulacji i inwestycji dla godnej zaufania sztucznej inteligencji *(Policy and investment recommendations for trustworthy Artificial Intelligence*[36]*).* Dokument zawiera 33 rekomendacje odnoszące się do społeczeństwa, państwa, biznesu i nauki. Wśród postulatów grupy ekspertów znalazły się m.in.: wzrost świadomości społecznej w obszarze Sztucznej Inteligencji; stawianie człowieka w centrum w kontekście przemian na rynku pracy; monitorowanie wpływu Sztucznej Inteligencji na społeczeństwo; ochrona praw podstawowych w usługach publicznych opartych na AI. (więcej szczegółów w rozdziale Sztuczna Inteligencja).

Dodatkowo Komisja Europejska prowadziła aktywne działania na rzecz ułatwienia państwom członkowskim przygotowań do zmian społeczno-gospodarczych spowodowanych wdrażaniem Sztucznej Inteligencji. W tym zakresie opublikowano trzy dokumenty:

- **8 kwietnia: komunikat *Building Trust in Human Centric Artificial Intelligence* –** KE podkreśliła, że Sztuczna Inteligencja nie może być celem samym w sobie, ale godnym zaufania narzędziem, szanującym demokrację, ludzką godność i ostatecznie służącym wzmacnianiu dobrobytu człowieka. Dodatkowo zagadnienia etyczne nie mogą być traktowane, jako dodatek do Sztucznej Inteligencji, ale jako jej integralna część. KE zapowiedziała także rozpoczęcie ukierunkowanej fazy pilotażowej, która sprawdzi, czy zaproponowane przez ekspertów wytyczne dotyczące godnej zaufania Sztucznej Inteligencji mogą zostać wdrożone w praktyce.
- **3 maja: raport M. Servoz'a**[37] ***The future of work? Work of the future!* –** raport opisuje wpływ nowych technologii na rynek pracy i gospodarkę Unii Europejskiej. Oprócz analiz przedstawiających m.in. historyczne uwarunkowania procesu automatyzacji i jego wpływ na gospodarkę, w publikacji

34 *A definitione of AI: Main capabilities and disciplines* (https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341)
35 *AI Alliance* to platforma wymiany doświadczeń i wiedzy na temat rozwoju sztucznej inteligencji w Europie. Gospodarzem platformy AI Alliance zrzeszającej ponad 3500 członków jest Komisja Europejska.
36 *Policy and investment recommendations for trustworthy Artificial Intelligence* (https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60343)
37 Michel Servoz – starszy doradca prezydenta Junckera ds. sztucznej inteligencji, robotyki i przyszłości pracy.

znalazło się 20 rekomendacji. Wytyczne dotyczą edukacji młodzieży i dorosłych, cyfrowego potencjału, organizacji pracy i społecznego wsparcia (więcej szczegółów w rozdziale Sztuczna Inteligencja).

- **22 listopada: raport Grupy Ekspertów ds. Odpowiedzialności i Nowych Technologii *(Expert Group on Liability and New Technologies, NTF)* –** dokument dotyczy odpowiedzialności prawnej za szkody powstałe w wyniku działania Sztucznej Inteligencji i innych nowych technologii cyfrowych. Zdaniem ekspertów obecnie obowiązujące przepisy regulują kwestię prawnej odpowiedzialności za Sztuczną Inteligencję i nowe technologie cyfrowe, takie jak Internet Rzeczy czy Technologię Zdecentralizowanych Ksiąg Rachunkowych w sposób niewystarczający, nieefektywny, a w niektórych przypadkach niesprawiedliwy. Jednym z najważniejszych wniosków płynących z raportu jest problem nadawania osobowości prawnej Sztucznej Inteligencji. Eksperci uznali, że nie jest to konieczne, ani pożądane, ponieważ szkody powstałe w wyniku funkcjonowania nowych technologii mogą i powinny być przypisane odpowiedzialnym za nie osobom lub instytucjom (więcej szczegółów w rozdziale o SI).

10 kwietnia 2018 – podpisanie przez państwa członkowskie deklaracji o wzajemnej współpracy w dziedzinie rozwoju Sztucznej Inteligencji

25 kwietnia 2018 – zwiększenie inwestycji w obszarze Sztucznej Inteligencji do 20 mld euro rocznie w ramach europejskiej strategii rozwoju Sztucznej Inteligencji

1 czerwca 2018 – powołanie Grupy Ekspertów ds. Sztucznej Inteligencji i uruchomienie platformy AI Alliance

6 czerwca 2018 – przeznaczenie 2,5 miliarda euro na rozwój Sztucznej Inteligencji w ramach programu Digital Europe

7 czerwca 2019 – uruchomienie największego unijnego programu R&I o wartości 100 mld euro w ramach programu Horizon Europe

7 grudnia 2018 – Komisja Europejska zobowiązała państwa członkowskie do przygotowania krajowych strategii rozwoju Sztucznej Inteligencji

18 grudnia 2018 – Grupa ekspertów ds. Sztucznej Inteligencji przedstawiła pierwszą wersję Wytycznych dotyczących etyki godnej zaufania sztucznej inteligencji

1 stycznia 2019 – uruchomienie projektu AI4UE

8 kwietnia 2019 – opublikowanie przez Komisje Europejską komunikatu Budowanie zaufania do sztucznej inteligencji ukierunkowanej na człowieka

9 kwietnia 2019 – Grupa ekspertów ds. Sztucznej Inteligencji przedstawiła Wytyczne dotyczące etyki godnej zaufania sztucznej inteligencji

26 kwietnia 2019 – Grupa ekspertów ds. Sztucznej Inteligencji przedstawiła Wytyczne w sprawie regulacji i inwestycji dla godnej zaufania sztucznej inteligencji

Dane, dane, dane… – nowa ropa?

Komisja Europejska wychodzi z założenia, że gospodarka UE w coraz większym stopniu zależy od danych i nowoczesnych technologii cyfrowych. Dlatego, zdaniem KE, swobodny przepływ danych pomiędzy państwami członkowskimi zapewni zwiększenie produktywności i konkurencyjności Unii Europejskiej na globalnym rynku. W związku z tym podejmowane są liczne działania, zmierzające do ułatwienia swobodnego przepływu danych pomiędzy państwami członkowskimi. Warto przy tym zwrócić uwagę, że dyskusja, która przetoczyła się przez Europę przy okazji wdrażania sieci 5G (czytaj więcej w części II raportu w rozdziale poświęconym 5G), pokazuje że następuje pewnego rodzaju zmiana paradygmatu – z danych na technologię.

W 2019 roku KE przedstawiła 3 istotne dokumenty w zakresie danych osobowych i nieosobowych:

- **29 maja 2019 roku komunikat na temat *wytycznych dotyczących rozporządzenia w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej*[38].** Wytyczne mają ułatwić małym i średnim przedsiębiorcom zrozumienie powiązań między *Rozporządzeniem w sprawie swobodnego przepływu danych nieosobowych a Rozporządzeniem o ochronie danych osobowych (RODO).* Oba rozporządzenia zapewniają transgraniczny rozwój danych, a także odwołują się do mobilności danych i stawiają za cel łatwiejsze przenoszenie danych z jednego środowiska IT do innego.
- **20 czerwca 2019 przyjęta została *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego.*** Zgodnie z regulacją państwa członkowskie mają zapewnić możliwość ponownego wykorzystania: dokumentów organów sektora publicznego, dokumentów przedsiębiorstw publicznych oraz danych badawczych. Dyrektywa upoważnia przedsiębiorstwa publiczne do wydawania pozwolenia na ponowne wykorzystanie ich dokumentów. Przedsiębiorstwa same mogą decydować, czy chcą umożliwić innym podmiotom wykorzystywanie ich danych. Komisja Europejska zobowiązała się do przeprowadzenia oceny dyrektywy do **17 lipca 2025 roku.**
- **24 lipca Komisja Europejska opublikowała komunikat *Data protection rules as a trust-enabler in the EU and beyond – taking stock*[39],** w którym dokonała wstępnej oceny pierwszego roku stosowania RODO. KE pozytywnie oceniła pierwszy rok stosowania rozporządzenia. Zwróciła jednak uwagę na pilną konieczność uzupełnienia krajowych ram prawnych dotyczących ochrony danych w trzech państwach członkowskich. Ponadto Komisja zaleciła państwom członkowskim zwiększenie zasobów ludzkich, finansowych i technicznych dla krajowych organów ochrony danych, tak aby mogły one w pełni wykorzystać swój potencjał.

Wzmacnianie cyfrowej rewolucji w UE

Rewolucja cyfrowa otwiera przed europejskimi przedsiębiorstwami ogromne możliwości rozwoju. Niestety, pomiędzy przedsiębiorstwami z poszczególnych państw członkowskich Unii Europejskiej wciąż istnieją silne dysproporcje w poziomie rozwoju technologicznego. Wiele firm, zwłaszcza małych i średnich, ma trudno-

38 Komunikat Komisji do Parlamentu Europejskiego i Rady Wytyczne dotyczące rozporządzenia w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej. (https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52019DC0250)
39 Data protection rules as a trust-enabler in the EU and beyond – taking stock (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0374)

ści zarówno z inwestowaniem w technologie cyfrowe, ale także z ich wdrażaniem. W kwietniu 2016 roku Komisja Europejska zainicjowała cyfryzację europejskiego przemysłu *(Digitising European Industry, DEI)*.

Strategia Jednolitego Rynku Cyfrowego dla Europy (A Digital Single Market Strategy for Europe) – Strategia DSM

6 maja 2015 roku Komisja Europejska opublikowała Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: *Strategia jednolitego rynku cyfrowego dla Europy.*

Dokument zakłada zniesienie ograniczeń regulacyjnych w kwestiach cyfrowych w taki sposób, aby możliwe było zbudowanie Wspólnego Europejskiego Rynku Cyfrowego. Ma to pomóc w szybszym rozwoju usług cyfrowych, a tym samym budować konkurencyjność europejskich firm.

Założenia strategii są oparte na trzech podstawowych filarach: **lepszy dostęp konsumentów i przedsiębiorców do towarów sprzedawanych przez Internet; środowisko, w którym sieci i usługi cyfrowe mogą się rozwijać; cyfrowość jako siła napędowa wzrostu.**

Uruchomiona w ramach strategii Jednolitego Rynku Cyfrowego, inicjatywa DEI ma na celu wzmocnienie konkurencyjności UE w zakresie technologii cyfrowych i zapewnienie, że każda firma w Europie – niezależnie od sektora, lokalizacji i wielkości – może czerpać pełne korzyści z technologii cyfrowych. Działania DEI zostały oparte na 5 filarach.

Europejska platforma krajowych inicjatyw dotyczących cyfryzacji przemysłu zrzeszająca wszystkie państwa członkowskie

Cyfrowe Centra Innowacji (DIH) punkty kompleksowej obsługi i wsparcia przedsiębiorstw w podnoszeniu poziomu cyfryzacji

Wzmocnienie przywództwa poprzez tworzenie partnerstw publiczno-prywatnych i platform przemysłowych

Ramy prawne dostosowane do ery cyfrowej

Przygotowanie Europejczyków do cyfrowej przyszłości

Raport DESI

11 czerwca Komisja Europejska opublikowała *Raport indeks gospodarki cyfrowej i społeczeństwa cyfrowego (DESI 2019)*. Celem publikacji była ocena postępów w realizacji celów gospodarki cyfrowej w Unii Europejskiej oraz monitorowanie stanu zaawansowania cyfrowego poszczególnych państw członkowskich. W raporcie, KE wskazała na konieczność zwiększenia tempa transformacji cyfrowej. Wśród państw z najniższym wskaźnikiem

zaawansowania gospodarki cyfrowej znalazły się: Bułgaria, Rumunia, Grecja i Polska. Wśród państw charakteryzujących się najwyższym wskaźnikiem znalazły się: Finlandia, Szwecja, Holandia i Dania. KE zapowiedziała wprowadzenie nowych regulacji mających usprawnić łączność i gospodarkę opartą na danych oraz pobudzić rozwój handlu elektronicznego. KE podkreśliła również, że jednym z kluczowych wyzwań stojących przed Unią Europejską będzie zapewnienie obywatelom dostępu do kompetencji cyfrowych dostosowanych do nowoczesnego rynku pracy.

Digital Innovation Hubs (DIH)

DIH *(Digital Innovation Hubs)* to koncepcja, która powstawała w UE stopniowo[40]. DIH ma zapewnić kompleksową pomoc firmom (zwłaszcza małym i średnim przedsiębiorstwom, start-upom) w ulepszeniu biznesu, procesów produkcyjnych, produktów i usług za pomocą technologii cyfrowej. Zgodnie z założeniem DIH mają powstawać w całej Europie, przy czym mogą to być organizacje, które do tej pory prowadziły zadania w tym zakresie i teraz otrzymają środki na ich wzmocnienie. W latach 2016-2020 Komisja Europejska przeznaczyła na budowę sieci DIH 100 mln euro rocznie. Do 2020 roku DIH mają powstać w każdym regionie Unii Europejskiej.

W 2019 roku UE zaprosiła organizacje, małe i średnie przedsiębiorstwa do składania wniosków w ramach programu *Smart Anything Everywhere* w ramach programu *Horyzont 2020*.

Prawo autorskie – wzmocnienie pozycji twórcy na rynku cyfrowym

Dynamiczny rozwój nowych technologii cyfrowych zmienił nie tylko sposób korzystania z dóbr kultury w Internecie, ale także modele biznesowe, które starają się zaspokajać rosnące potrzeby konsumentów w tych obszarach. W 2019 roku Komisja Europejska zmieniła przepisy dotyczące ochrony treści objętych prawem autorskim, które nie były adekwatne do rozwoju technologii. **17 kwietnia 2019 roku** Komisja Europejska przyjęła *Dyrektywę w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym*[41]. Dyrektywa wprowadza istotne zmiany w trzech obszarach: dostosowanie wyjątków i ograniczeń do środowiska cyfrowego i transgranicznego; poprawa praktyk w zakresie licencjonowania; zapewnienie szerszego dostępu do treści. Dyrektywa umożliwia wydawcom i twórcom czerpanie wynagrodzenia za rozpowszechnianie swoich utworów w Internecie. Zobowiązuje również wielkie platformy internetowe i agregatory treści do przestrzegania prawa autorskiego. Jeśli platformy nie uiszczą twórcom treści należnego wynagrodzenia i będą rozpowszechniać ich dzieła poniosą za to odpowiedzialność prawną. Na implementację zapisów dyrektywy do swoich porządków prawnych, państwa członkowskie mają czas do 7 czerwca 2021 roku.

Wciąż czekamy na… – przedłużające się negocjacje rozporządzeń

Wciąż trwają negocjacje dwóch istotnych rozporządzeń: *ePrivacy* i rozporządzenia ustanawiającego Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych wraz z siecią krajowych ośrodków koordynacji.

40 Więcej na ten temat możesz przeczytać w raporcie *Cyberbezpieczeństwo A.D. 2018. Strategia. Policy. Rekomendacje – cyberbezpieczeństwo w perspektywie policy* (https://cyberpolicy.nask.pl/wp-content/uploads/2019/04/Raport-Cyberbezpiecze%C5%84stwo-A.D.-2018.pdf)

41 *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790 z dnia 17 kwietnia 2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE.* (https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32019L0790)

Rozporządzenie ePrivacy

Projekt rozporządzenia *ePrivacy* został przedstawiony 10 stycznia 2017 roku Rozporządzenie miało wejść w życie razem z RODO i stanowić specjalną regulację w zakresie prywatności w Internecie (tzw. lex specialis do RODO). Negocjacje wciąż jednak trwają. Rozporządzenie jest aktem obowiązującym bezpośrednio, co oznacza że po przyjęciu *ePrivacy* jego implementacja do porządków prawnych państw członkowskich nie będzie konieczna[42].

Projekt *ePrivacy* wzmacnia pozycję użytkowników w Internecie. Wprowadza ochronę zarówno osób fizycznych, jak i prawnych i podkreśla ich prawo do decydowania o zakresie i celu gromadzenia danych. Nakłada na dostawców usług obowiązek jasnego i wyraźnego informowania o przetwarzanych danych i umożliwia użytkownikom odwołanie zgody na takie operacje tam, gdzie nie jest to konieczne do wykonania żądanej usługi.

Ważnym elementem rozporządzenia jest zwiększenie przejrzystości plików *cookies* (służących do zapamiętywania preferencji i personalizowania stron internetowych), a także objęcie ochroną metadanych, które dostarczają szczególnie chronione informacje takie jak lokalizacja, historia przeglądarki czy godzina połączenia i czas wysłania wiadomości.

Z perspektywy użytkowników, dużą zmianą będzie wprowadzenie ograniczeń niechcianej komunikacji marketingowej, a także konieczność oznaczania treści o charakterze marketingowym i kanałów, którymi takie treści są udostępniane.

Impas w negocjacjach spowodowany jest dużą liczbą uwag o podłożu legislacyjnym zgłaszanych przez prawa członkowskie, a także silnym lobby przedstawicieli biznesu, którzy obawiają się, że ograniczenia w przetwarzaniu i wykorzystywaniu danych negatywnie wpłyną na rozwój innowacyjnych produktów i usług w UE.

Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa

Komisja Europejska przedstawiła propozycję rozporządzenia ustanawiającego *Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych wraz z siecią krajowych ośrodków koordynacji* 12 września 2018 roku[43]. Celem regulacji jest stymulowanie europejskiego ekosystemu technologicznego i przemysłowego oraz wzmacnianie współpracy w dziedzinie cyberbezpieczeństwa między różnymi branżami i środowiskami naukowymi. Propozycja budzi jednak wiele kontrowersji. Przede wszystkim, nie do końca uzasadniona wydaje się dominująca rola Komisji Europejskiej w radzie zarządzającej, a także uzależnienie prawa głosu w radzie dla państw członkowskich od funduszy wpłacanych na Centrum. Dodatkowo część zadań Centrum wyraźnie pokrywa się z nowym mandatem ENISA. Negocjacje przedłużają się, ponieważ państwa członkowskie starają się wypracować nową koncepcję Centrum.

42 Więcej na ten temat możesz przeczytać w raporcie *Cyberbezpieczeństwo A.D. 2018. Strategia. Policy. Rekomendacje – cyberbezpieczeństwo w perspektywie policy, str. 32* (https://cyberpolicy.nask.pl/wp-content/uploads/2019/04/Raport-Cyberbezpiecze%C5%84stwo-A.D.-2018.pdf)

43 Więcej na ten temat możesz przeczytać w raporcie *Cyberbezpieczeństwo A.D. 2018. Strategia. Policy. Rekomendacje – cyberbezpieczeństwo w perspektywie policy* (https://cyberpolicy.nask.pl/wp-content/uploads/2019/04/Raport-Cyberbezpiecze%C5%84stwo-A.D.-2018.pdf)

ORGANIZACJA NARODÓW ZJEDNOCZONYCH

Prawo międzynarodowe a cyberbezpieczeństwo

Organizacja Narodów Zjednoczonych jest instytucją mocno zaangażowaną w działania na rzecz wspierania procesu transformacji cyfrowej z korzyścią dla wszystkich obywateli. Działania te wpisują się w prace nad realizacją celów zrównoważonego rozwoju ONZ: zapewnienia dobrej jakości życia, edukacji, równości, wzrostu gospodarczego, innowacyjności. Najważniejszymi wydarzeniami w 2019 roku w ONZ był Światowy Szczyt Społeczeństwa Informacyjnego i Forum Zarządzania Internetem w Berlinie. Kluczowe znaczenie miała również Światowa Konferencja Radiokomunikacyjna, która jest organizowana przez ITU co 3-4 lata i odgrywa ważną rolę w dostosowaniu technicznych i regulacyjnych aspektów usług radiokomunikacyjnych do rozwoju nowoczesnych technologii. Rok 2019 był również ważny pod kątem dialogu na temat zastosowania prawa międzynarodowego w cyberprzestrzeni. W grudniu odbyło się pierwsze spotkanie szóstej grupy UN GGE. Równolegle do grupy GGE działa również grupa OEWG. Po raz pierwszy ONZ powołało dwie niemal równoległe grupy robocze – ekspercką i otwartą dla wszystkich państw. Rezultaty z prac tych grup będą przedstawione odpowiednio w 2020 i 2021 roku.

Najważniejsze wydarzenia dotyczące cyberbezpieczeństwa w ONZ w 2019 roku.

10-12 grudnia 2018

XVI Światowe Sympozjum Telekomunikacji – WTIS, to jedno z ważniejszych światowych forów poświęconych aktualnym trendom ICT i społeczeństwa informacyjnego.

22 grudnia 2018

Powołanie **szóstej grupy GGE –** kontynuacja pracy nad wspólnym zrozumieniem **zagrożeń bezpieczeństwa teleinformatycznego i zastosowaniem prawa międzynarodowego w cyberprzestrzeni.**

22 grudnia 2018

Powołanie **Otwartej grupy roboczej ds. Rozwoju technologii teleinformatycznych w kontekście bezpieczeństwa międzynarodowego (OEWG).** Jest to nowy mechanizm współpracy wszystkich członków ONZ w zakresie wypracowania sposobów zastosowaniem prawa międzynarodowego w cyberprzestrzeni.

8-12 kwietnia 2019

Światowy Szczyt Społeczeństwa Informacyjnego 2019. Dyskusja nad narzędziami realizacji celów zrównoważonego rozwoju ONZ, przede wszystkim na temat wsparcia transformacji cyfrowej poprzez odpowiednie ramy regulacyjne i działanie na rzecz wyrównywania szans pomiędzy państwami.

Lipiec 2019

Raport Panelu Wysokiego Szczebla ds. Współpracy Cyfrowej. Dokument podkreśla konieczność wspólnego działania w celu zbudowania lepszej przyszłości cyfrowej.

Październik-listopad 2019

Światowa Konferencja Radiokomunikacyjna. Odbywa się przegląd regulacji radiowych i telekomunikacyjnych, a także zdefiniowanie dodatkowych pasm częstotliwości radiowej dla 5G.

Grudzień 2019

Forum Zarządzania Internetem 2019 w Berlinie. Dyskusja nad priorytetowymi obszarami tematycznymi: zarządzanie danymi; włączenie cyfrowe; bezpieczeństwo, stabilność i odporność na zagrożenia.

XVI Światowe Sympozjum Telekomunikacji

W dniach 10-12 grudnia 2018 roku w Genewie odbyło się XVI Światowe Sympozjum Telekomunikacji *(16th World Telecommunication/ ICT Indicators Symposium – WTIS)*. WTIS jest jednym z ważniejszych światowych forów gromadzących przedstawicieli rządów, liderów biznesu, przedstawicieli organów regulacyjnych, organizacji statystycznych, naukowców, producentów i analityków ICT. Ich celem jest obserwacja oraz analiza aktualnych trendów ICT i społeczeństwa informacyjnego. W trakcie trwania forum wydano raport podsumowujący stan społeczeństwa informacyjnego na rok 2018[44]. Wśród głównych tez znalazły się:

- Pod koniec 2018 roku 51,2% (3.9 mld) osób na świecie używało Internetu. Zgodnie z założeniami ITU do 2023 roku ma być to 70%, a do 2025 roku – 75%.
- Prawie cała populacja świata żyje obecnie w zasięgu sygnału sieci komórkowej.
- Brak umiejętności w zakresie ICT stanowi ważną przeszkodę w dostępie do Internetu, szczególnie dla krajów rozwijających się.
- Sektor telekomunikacyjny odgrywa ważną rolę w gospodarce globalnej. W 2016 roku przychody z telekomunikacji osiągnęły 2,3% światowego PKB.
- W ostatniej dekadzie, wraz ze wzrostem dostępu do produktów i usług, spadły ceny technologii ICT na całym świecie.

Szósta Grupa UN GGE

Grupa ekspertów rządowych ds. rozwoju w dziedzinie informacji i telekomunikacji w kontekście bezpieczeństwa międzynarodowego (*Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* – UN GGE) po raz pierwszy została powołana w 2003 roku. Do tej pory utworzono sześć grup GGE, których głównym osiągnięciem było opracowanie zasad stosowania prawa międzynarodowego w cyberprzestrzeni[45]. Prace piątej grupy GGE w latach 2016-2017 zakończyły się brakiem konsensusu.

44 Raport *Measuring the Information Society Report 2018*
45 *Grupa UN GGE – na ile prawo międzynarodowe ma zastosowanie w cyberprzestrzeni?, Cyberbezpieczeństwo A.D. 2018. Strategia.Policy. Rekomendacje – cyberbezpieczeństwo w perspektywie policy, str. 39-40.* (https://cyberpolicy.nask.pl/wp-content/uploads/2019/04/Raport-Cyberbezpiecze%C5%84stwo-A.D.-2018.pdf)

Historia grup UN-GGE w latach 2004-2020*

22 grudnia 2018 roku na 73. Zgromadzeniu Ogólnym ONZ powołano **szóstą grupę GGE,** która ma kontynuować pracę poprzednich grup. Przewodniczącym został Ambasador Guilherme de Aguiar Patriota z Brazylii. Grupa liczy 25 osób z 25 państw członkowskich, ekspertów z dziedziny bezpieczeństwa informacji, dyplomacji, a także o zapleczu technicznym[46]. Eksperci będą pracować nad wspólnym zrozumieniem istniejących i potencjalnych zagrożeń, a także możliwych środków zapobiegawczych. Będą również rozwijać podejście zastosowania prawa międzynarodowego do nowych technologii informacyjno-komunikacyjnych, a także opracowywać normy i wytyczne z zakresu *policy* oraz środki budowy zaufania wśród państw członkowskich. Grupa spotka się na czterech tygodniowych sesjach, z których pierwsza odbyła się 9-13 grudnia 2019 roku. Następne planowane są na marzec 2020, sierpień 2020 i maj 2021. W latach 2019-2021 odbędą się również konsultacje z organizacjami regionalnymi[47]. Efektem prac grupy będzie raport, który zostanie ogłoszony na 76. Zgromadzeniu Ogólnym ONZ w 2021 roku.

Otwarta grupa robocza (OEWG) – nowy mechanizm współpracy w ramach ONZ

Równolegle z szóstą grupą GGE utworzono Otwartą grupę roboczą ds. Rozwoju technologii teleinformatycznych w kontekście bezpieczeństwa międzynarodowego *(Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security – OEWG).* W grupie uczestniczą wszystkie państwa, które wyraziły chęć udziału w jej pracach. Głównym zadaniem OEWG jest dyskusja na temat:

46 Do szóstej grupy GGE powołano ekspertów z następujących państw: Australia, Brazylia, Chiny, Estonia, Francja, Niemcy, Indie, Indonezja, Japonia, Jordania, Kazahstan, Kenia, Mauritius, Meksyk, Maroko, Holandia, Norwegia, Rumunia, Rosja, Singapur, RPA, Szwajcaria, Wielka Brytania, USA, Urugwaj. (https://dig.watch/processes/un-gge)
47 Do konsultacji zaproszono organizacje regionalne. Należą do nich: Unia Afrykańska, Unia Europejska, Organizacja Państw Amerykańskich, OBWE, Forum Regionalne ASEAN.

Prac nad środkami budowy zaufania

Budowy zdolności ochrony systemów IT przed istniejącymi i potencjalnymi zagrożeniami

Dalszego rozwijania zasad i norm, a także sposobów ich wdrażania

Prac nad zastosowaniem prawa międzynarodowego w cyberprzestrzeni

Regularnego dialogu instytucjonalnego z szerokim udziałem wszystkich interesariuszy

Grupa jest prowadzona w formie otwartej i każde państwo członkowskie ONZ może się zaangażować w jej pracę. Mechanizm przewiduje jednoczesną wymianę wiedzy i doświadczeń z biznesem, organizacjami pozarządowymi oraz przedstawicielami świata nauki. Przewodniczącym grupy jest Ambasador Jürg Lauber ze Szwajcarii, a raport z jej działalności zostanie ogłoszony na 75. Zgromadzeniu Ogólnym ONZ w 2020 roku.

Grupy ONZ – odpowiedzialne zachowanie w cyberprzestrzeni

Grupa UN GGE 2019 – 2021		Grupa UN OEWG 2019 – 2020
Powołana po raz		Powołana po raz
25 państw członkowskich		**WSZYSTKIE** państwa członkowskie (grupa otwarta)
Przewodniczący: **Guilherme de Aguiar Patriota**		Przewodniczący: **Jürg Lauber**
6 organizacji regionalnych (Unia Afrykańska, Unia Europejska, Organizacja Państw Amerykańskich, OBWE, Forum Regionalne ASEAN), **a także 2 konsultacje z członkami ONZ**	Konsultacje	**Wszyscy interesariusze:** biznes, organizacje pozarządowe, przedstawiciele świata nauki.
• prawo międzynarodowe w cyberprzestrzeni • normy, zasady, wytyczne • środki budowy zaufania	Tematyka	• prawo międzynarodowe w cyberprzestrzeni • normy, zasady, wytyczne • środki budowy zaufania • ochrona przed istniejącymi i potencjalnymi zagrożeniami • budowanie zdolności państw • dialog instytucjonalny ze wszystkimi interesariuszami (pod egidą ONZ)
Raport: **76. Zgromadzenie Ogólne ONZ (2021)**		Raport: **75. Zgromadzenie Ogólne ONZ (2020)**

Światowy Szczyt Społeczeństwa Informacyjnego 2019

8-12 kwietnia 2019 roku odbył się kolejny Światowy Szczyt Społeczeństwa Informacyjnego *(World Summit on the Information Society – WSIS)*. Na szczycie podkreślono znaczenie wdrażanych w latach 2005-2015 *WSIS Action Lines* i Genewskiego planu działania[48], które obecnie mogą służyć do lepszej realizacji celów zrównoważonego rozwoju ONZ w kontekście społeczeństwa informacyjnego. Wśród najważniejszych wniosków ze szczytu znalazły się:

1. Potrzeba stworzenia zintegrowanych ram regulacyjnych wspierających proces transformacji cyfrowej.
2. Likwidacja podziałów i inwestowanie w rozwój kompetencji w krajach rozwijających się.
3. Otwarty rynek telekomunikacyjny dla handlu cyfrowego.
4. Dostęp do technologii rewolucji cyfrowej dla wszystkich (5G, IoT, SI).
5. Strategie i regulacje stworzone tak, aby nie pogłębiać podziałów społecznych.
6. Nowe technologie – etyczne, bezpieczne, budzące zaufanie.
7. Zastosowanie ICT ukierunkowane na korzyść dla ludzkości (w tym zarządzanie zasobami naturalnymi, gospodarowanie odpadami, zmiany klimatyczne).
8. Wysokiej jakości infrastruktura cyfrowa: dostępna cenowo i niezawodna.
9. Ochrona własności intelektualnej dla rozwoju wiedzy i ochrony dziedzictwa kulturowego.

Raport Panelu Wysokiego Szczebla ds. Współpracy Cyfrowej

W lipcu 2019 roku 20 niezależnych ekspertów wchodzących w skład Panelu Wysokiego Szczebla ds. Współpracy Cyfrowej[49] *(Secretary-General's High-level Panel on Digital Cooperation)* zakończyło pracę nad raportem. Dokument wskazuje 5 obszarów priorytetowych, w których należy podjąć natychmiastowe działania w celu zbudowania lepszej przyszłości cyfrowej: z poszanowaniem zrównoważonego rozwoju, zmniejszaniem nierówności społecznych, a także uwzględnieniem działań na rzecz pokoju, bezpieczeństwa i rozwoju gospodarczego ludzkości[50].

48 Genewski plan działania został opracowany w 2003 roku podczas pierwszego Światowego Szczytu Społeczeństwa Informacyjnego. Plan zakładał podłączenie do Internetu 50% populacji, do roku 2015. Opracowano 11 obszarów – *Action Lines*, w których należy podjąć działania, aby zrealizować postawiony cel. Obszary te obejmowały: współpracę pomiędzy sektorem publicznym, prywatnym i NGO; zapewnienie równego dostępu do wiedzy; wprowadzenie technologii informacyjnych do usług publicznych; kwestie etyczne i międzynarodową współpracę. Wdrażanie Genewskiego planu działania zakończyło się w 2015 roku. (https://www.itu.int/net/wsis/index.html)

49 *ONZ. Panel Wysokiego Szczebla ds. Współpracy Cyfrowej, Cyberbezpieczeństwo A.D. 2018.*, str. 45 (https://cyberpolicy.nask.pl/wp-content/uploads/2019/04/Raport-Cyberbezpiecze%C5%84stwo-A.D.-2018.pdf)

50 *The Age of Digital Interdependence Report of the UN Secretary-General's High-level Panel on Digital Cooperation* (https://digitalcooperation.org/wp-content/uploads/2019/06/HLP-on-Digital-Cooperation-Report-Executive-Summary-ENG.pdf)

5 obszarów priorytetowych wskazanych przez Panel:

1. **Gospodarka cyfrowa dostępna dla całego społeczeństwa –** priorytetem jest dostęp do sieci i e-usług dla każdego dorosłego obywatela do 2030 roku, a także działania na rzecz włączenia cyfrowego kobiet i grup marginalizowanych.

2. **Budowanie zdolności i kompetencji z obszaru cyfryzacji dla obywateli i organizacji –** rekomendacja utworzenia międzynarodowego biura wsparcia w rozwiązywaniu problemów cyfrowych i budowania zdolności w obszarze nowoczesnych technologii.

3. **Poszanowanie Praw Człowieka –** priorytetem jest zapewnienie poszanowania praw człowieka w świecie nowoczesnych technologii i przegląd nowych zagrożeń w tym obszarze.

4. **Zaufanie, bezpieczeństwo i stabilność –** rekomendacja utworzenia Globalnego Porozumienia na rzecz Zaufania i Bezpieczeństwa Cyfrowego *(Global Commitment on Digital Trust and Security)*.

5. **Globalna współpraca cyfrowa –** rekomendacja rozpoczęcia w ramach ONZ otwartych konsultacji w celu zbudowania mechanizmów globalnej współpracy cyfrowej.

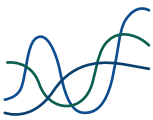
Światowa Konferencja Radiokomunikacyjna – WRC19

Światowa Konferencja Radiokomunikacyjna *(The World Radiocommunication Conference 2019 – WRC19)* jest organizowana przez ITU co 3-4 lata. W 2019 roku konferencja odbyła się od 28 października do 22 listopada w Egipcie. Wzięło w niej udział ponad 3500 uczestników z 193 państw, członków ITU, a także przedstawicieli sektora prywatnego, innych organizacji międzynarodowych i niezależnych obserwatorów.

WRC odgrywa kluczową rolę w kształtowaniu technicznych i regulacyjnych ram dotyczących świadczenia usług radiokomunikacyjnych we wszystkich krajach, w przestrzeni kosmicznej, lotniczej, morskiej i lądowej. Postanowienia konferencji przyczyniają się do realizacji celów zrównoważonego rozwoju ONZ. Dodatkowo WRC wspiera rozwój nowoczesnych technologii, które są podstawą gospodarki cyfrowej. Na każdej konferencji WRC odbywa się przegląd regulacji radiowych i międzynarodowych umów kontrolujących użycie widma częstotliwości radiowych, orbit satelitów geostacjonarnych i niegeostacjonarnych. Wśród wybranych rezultatów WRC19 znalazły się:

Przydzielenie dodatkowego widma dla systemów platform na dużych wysokościach *(High Altitude Platform Systems – HAPS)*[51]

Zmiana ram regulacyjnych dla niegeostacjonarnych systemów satelitarnych *(Non-Geostationary Satellite Systems – non-GSO)*[52]



Zdefiniowanie dodatkowych pasm częstotliwości radiowych dla Międzynarodowej Telekomunikacji Mobilnej (IMT), które ułatwią rozwój sieci 5G[53]

Zatwierdzenie nowego zalecenia w sprawie inteligentnych systemów transportowych (ITS), a także nowej rezolucji w sprawie kolejowych systemów radiokomunikacyjnych (RSTT)

Dokument zawierający listę wszystkich decyzji podjętych podczas WRC19 znajduje się na stronie ITU[54].

Forum Zarządzania Internetem – Berlin 2019

W grudniu 2019 roku w Berlinie odbyło się czternaste Forum Zarządzania Internetem *(Internet Governance Forum – IGF)*[55]. Forum jest miejscem dialogu na temat rozwoju sieci i platformą wymiany wiedzy. Spotkania IGF organizowane są co roku i biorą w nich udział wszyscy członkowie WSIS *(World Summit on Information Society)*. W 2019 roku było to 3679 przedstawicieli, którzy reprezentowali 161 państw. Tematy priorytetowe forum zostały wybrane w ramach otwartego naboru propozycji. Ostatecznie zidentyfikowano trzy najbardziej priorytetowe obszary:

Zarządzanie danymi

Włączenie cyfrowe – dostęp do nowoczesnych technologii dla wszystkich

Bezpieczeństwo, stabilność i odporność na zagrożenia

Hasło IGF 2019 brzmiało: *One World. One Net. One Vision.* Hasło było odpowiedzią na tendencję do wznoszenia barier, która widoczna jest nie tylko w świecie realnym, ale również w świecie online. Bariery te wynikają z różnic prawnych i systemowych, ale także z zagrożeń cyberbezpieczeństwa, rozpowszechniania dezinformacji i braku rozwiązań zmniejszających rosnące podziały cyfrowe[56].

W 2019 roku zadbano o to, aby wzmocnić reprezentację państw rozwijających się i umożliwić wszystkim udział w dyskusji na temat globalnego, otwartego, wolnego i szanującego prawa człowieka Internetu. Państwa rozwijające się mogły skorzystać

51 *WRC-19: Enabling global radiocommunications for a better tomorrow* (https://news.itu.int/wrc%e2%80%9119-enabling-global-radiocommunications-for-a-better-tomorrow/)
52 *WRC-19: Enabling global radiocommunications for a better tomorrow* (https://news.itu.int/wrc%e2%80%9119-enabling-global-radiocommunications-for-a-better-tomorrow/)
53 *WRC-19 identifies additional frequency bands for 5G* (https://news.itu.int/wrc-19-agrees-to-identify-new-frequency-bands-for-5g/)
54 *Provisional Final Acts WRC-19* (https://www.itu.int/pub/R-ACT-WRC.13-2019/en)
55 *Raport Cyberbezpieczeństwo A.D. 2018. ONZ. Forum Zarządzania Internetem (IGF), str. 44* (https://cyberpolicy.nask.pl/wp-content/uploads/2019/04/Raport-Cyberbezpiecze%C5%84stwo-A.D.-2018.pdf)
56 *IGF 2019 Chair's Summary* (https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/9299/1809)

ze specjalnych funduszy na udział w forum. Po raz pierwszy, w ramach forum, odbyła się sesja parlamentarna, która miała na celu promowanie wdrażania rezultatów dyskusji na poziomach krajowych. Pierwszego dnia zorganizowano również sesję wysokiej rangi, w której brali udział przedstawiciele rządów, biznesu i społeczeństwa obywatelskiego.

Najważniejsze wnioski z IGF 2019 można sformułować w obszarze 3 tematów priorytetowych.

Zarządzanie danymi:

- Istnieje związek pomiędzy postępem cyfrowym, a wykluczeniem, który musi być dobrze rozumiany. Szczególnie, że nierówności w dostępie do cyfryzacji niosą ze sobą skutki w postaci niepokojów społecznych i konfliktów.
- Atak na łączność z Internetem stał się niebezpiecznym narzędziem politycznym, któremu należy zapobiegać.

Włączenie cyfrowe:

- Przepływy danych łączą społeczności, miasta, kraje i kontynenty ponad podziałami kulturowymi, religijnymi i wynikającymi ze statusu.
- Brak zarządzania Sztuczną Inteligencją sprawi, że będzie ona wykorzystana do manipulowania zachowaniem obywateli, nakłaniania ich do zakupów poprzez spersonalizowany i agresywny marketing, a także wpływania na wybory i wolność słowa.

Bezpieczeństwo:

- Poziom wspólnego bezpieczeństwa zależy od umiejętności współpracy ponad podziałami.
- Konflikty w cyberprzestrzeni nie są już prognozą przyszłości, ale teraźniejszością. Należy skupić się na wspólnym wypracowaniu narzędzi budowy zaufania i współpracy[57].

W 2020 roku IGF odbędzie się w Polsce, w Katowicach.

57 *IGF 2019 Chair's Summary* (https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/9299/1809)

OECD

Ekonomiczne aspekty cyfrowej rewolucji

Organizacja Współpracy Gospodarczej i Rozwoju *(Organisation for Economic Co-operation and Development, OECD;)* została utworzona na mocy Konwencji o Organizacji Współpracy Gospodarczej i Rozwoju podpisanej w Paryżu przez 20 państw 14 grudnia 1960 roku. OECD to organizacja międzynarodowa o profilu ekonomicznym skupiająca 36 wysoko rozwiniętych i demokratycznych państw. Jej celem jest wspieranie państw członkowskich w osiągnięciu jak najwyższego poziomu wzrostu gospodarczego i stopy życiowej obywateli. OECD działa poprzez wypracowywanie międzynarodowych wytycznych, standardów i diagnozy aktualnego rozwoju w danej dziedzinie. Wraz z rosnącym wpływem zmian wynikających z rewolucji cyfrowej, coraz więcej obszarów tematycznych związanych z nowoczesnymi technologiami znalazło odzwierciedlenie w działaniach OECD w 2019 roku.

Najważniejsze wydarzenia dotyczące cyberbezpieczeństwa OECD w 2019 roku:

Marzec 2019

Szczyt *Going Digital Summit* w marcu 2019 roku – podsumowanie pierwszej fazy projektu *Going Digital*, w trakcie której opracowano: rekomendacje działań na rzecz efektywnego zarządzania transformacją, narzędzie pomiaru stopnia zaawansowania transformacji w kraju i zalecenia z obszaru policy. Druga faza projektu zakończy się w 2020 roku.

2019-2020

Prace w ramach inicjatywy OECD BEPS[58] na rzecz wdrożenia międzynarodowego podatku cyfrowego. Planowo ostateczna propozycja OECD ma zostać zatwierdzona **do końca 2020 roku.** W oczekiwaniu na międzynarodowy konsensus prace nad własnym rozwiązaniem zawiesiła UE, a także Polska.

Going Digital Summit

Od 2017 roku, w ramach projektu ***Going Digital,*** OECD zajmuje się diagnozą wpływu transformacji cyfrowej na kształtowanie się polityki w obszarach: infrastruktury, gospodarki, nauki, finansów, edukacji, handlu i wielu innych. Istotą projektu jest zapewnienie rozwoju i wzrostu gospodarczego, przy jednoczesnej dbałości o jak najszerszą dystrybucję korzyści wynikających z transformacji cyfrowej.

W marcu 2019 roku odbył się Szczyt *Going Digital Summit,* podsumowujący zakończenie pierwszej fazy projektu, która trwała w latach 2017-2019. Na szczycie zaprezentowano dotychczasowe działania, wraz z raportem podsumowującym aktualny stan transformacji cyfrowej w państwach OECD. Wśród opracowanych publikacji i narzędzi udostępniono:

- **Raport *Measuring the Digital Transformation: A Roadmap for the Future***[59]

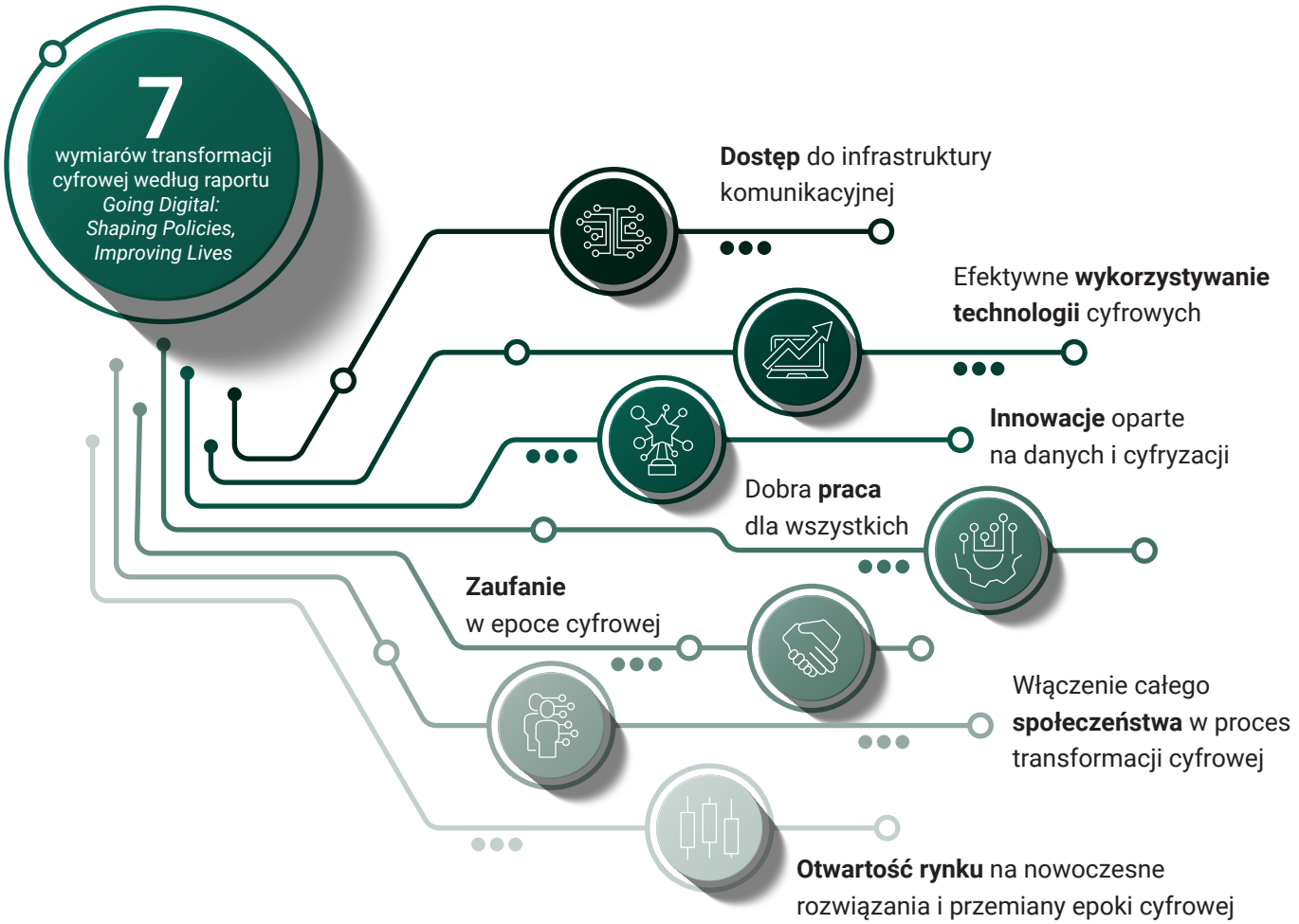
  Dokument zawiera zestaw dziewięciu działań, które przyczynią się do zwiększenia zdolności krajów do monitorowania przebiegu transformacji cyfrowej i jej skutków. Pierwsze cztery działania dotyczą budowania wskaźników nowej generacji: uwzględnienie transformacji cyfrowej w sta-

58 *Tax base erosion and profit shifting*
59 *Measuring the Digital Transformation. A Roadmap for the Future* (https://www.oecd-ilibrary.org/sites/9789264311992-en/index.html?itemId=/content/publication/9789264311992-en&mimeType=text/html)

tystykach gospodarczych; zapoznanie się z ekonomicznymi skutkami transformacji cyfrowej; pomiar poziomu dobrobytu; wdrożenie nowego podejścia do gromadzenia danych. Kolejne pięć działań ukierunkowanych jest na monitoring poszczególnych obszarów: technologie transformacyjne, przepływ danych, kompetencje w erze cyfrowej, zaufanie w środowisku online i cyfryzacja administracji. Monitorowanie transformacji cyfrowej jest pierwszym krokiem na drodze ku efektywnemu zarządzaniu jej skutkami i wypracowaniu regulacji, które przyczynią się do wzrostu dobrobytu całego społeczeństwa[60].

- **Raport *Going Digital: Shaping Policies, Improving Lives***

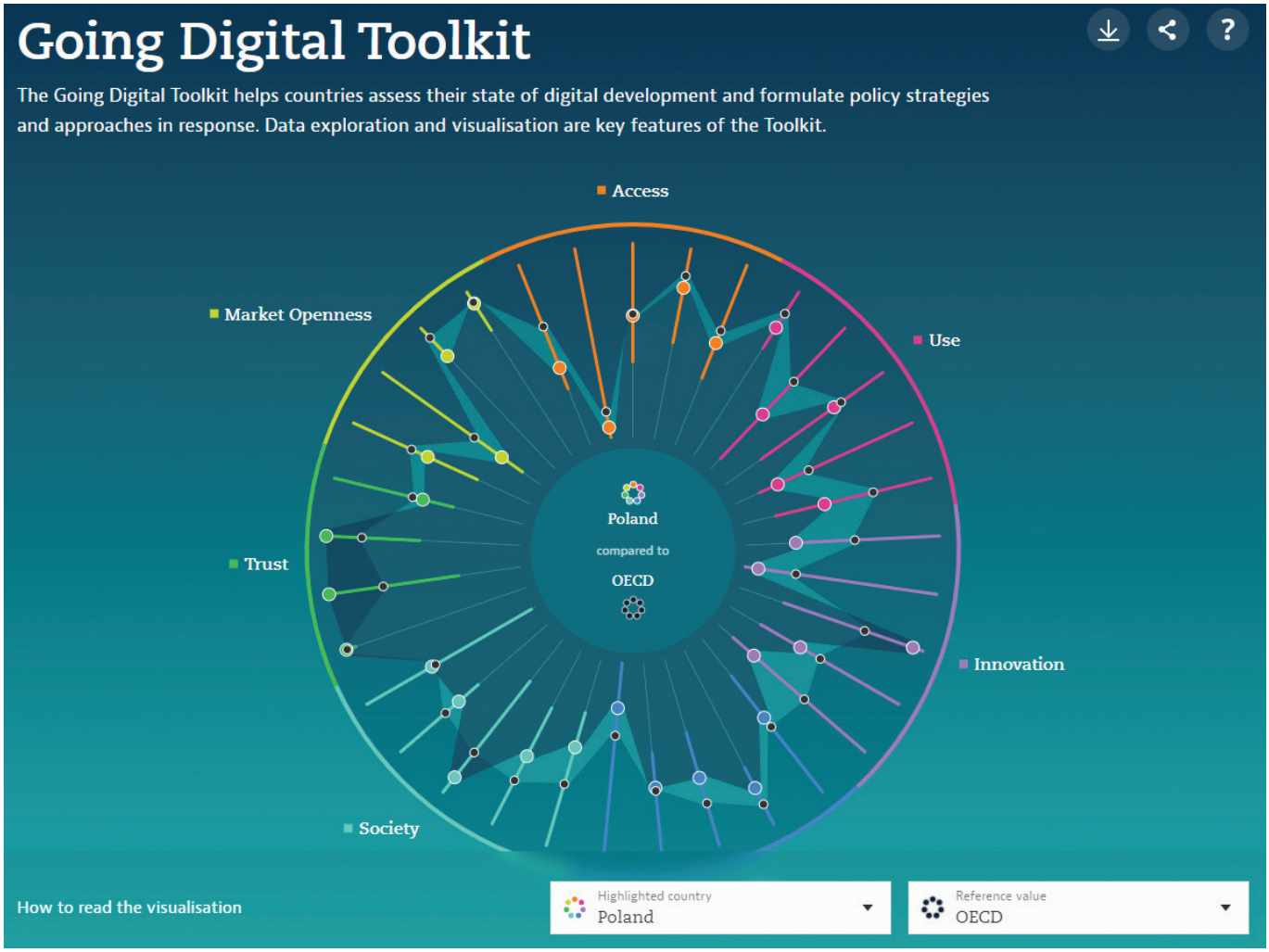
Kolejnym krokiem, po wypracowaniu wskaźników monitoringu transformacji cyfrowej, jest opracowanie regulacji, które przyczynią się do minimalizacji ryzyk wynikających z cyfryzacji i zwiększenia korzyści. Raport *Going Digital: Shaping Policies, Improving Lives*[61] zawiera szereg wskazówek i wytycznych dla decydentów z obszaru *policy*, którzy są odpowiedzialni za wyznaczanie kierunków działań państw. Rekomendacje zostały podzielone na 7 przenikających się wymiarów transformacji cyfrowej. W każdym z tych wymiarów raport określa kluczowe szanse i zagrożenia, a także dostarcza analiz i narzędzi oceny stanu transformacji cyfrowej państwa.



60 *Measuring the Digital Transformation. A Roadmap for the Future* (https://www.oecd.org/publications/measuring-the-digital-transformation-9789264311992-en.htm)
61 *Going Digital: Shaping Policies, Improving Lives* (https://www.oecd.org/going-digital/going-digital-synthesis-summary.pdf)

- **Going Digital Toolkit**

Wraz z raportem *Going Digital: Shaping Policies, Improving Lives,* OECD udostępniło także *Going Digital Toolkit.* Jest to **narzędzie, które pozwala państwom dokonać oceny aktualnego stanu zaawansowania transformacji cyfrowej.** Ocenie podlega 7 wymienionych wyżej wymiarów. Narzędzie jest interaktywne i pozwala zestawić wyniki każdego z wymiarów, a także umożliwia porównanie wyników w stosunku do średniej OECD. Do narzędzia dołączono także pakiet rekomendacji opracowanych przez OECD, które mają pomóc państwom podjąć działania na rzecz rozwoju w każdym z ocenianych wymiarów. *Going Digital Tookit* jest narzędziem darmowym, dostępnym na stronie internetowej: https://goingdigital.oecd.org/en/.



Źródło: https://goingdigital.oecd.org/en/

Druga faza projektu *Going Digital* została zaplanowana na okres 2019-2020. Tym razem działania będą koncentrować się na wsparciu w zakresie wdrażania polityki sprzyjającej transformacji cyfrowej, przeglądzie sytuacji krajowych i dzieleniu się dobrymi praktykami.

Opodatkowanie międzynarodowych korporacji działających w przestrzeni cyfrowej

OECD i G20 w ramach współpracy 137 państw zaangażowało się w inicjatywę **BEPS** *(tax base erosion and profit shifting)*, której głównym celem jest praca nad **wprowadzeniem międzynarodowych minimalnych standardów dotyczących zasad opodatkowania globalnych korporacji.** Wytyczne odnoszą się do podatku cyfrowego, którym mają być objęte korporacje działające w przestrzeni cyfrowej i wytwarzające zysk poza krajem jurysdykcji podatkowej. Przykładem takich korporacji mogą być platformy internetowe, które działają online i generują przychody w wielu krajach na całym świecie, a podatek płacą jedynie w kraju, w którym mają zarejestrowaną działalność. Miejsce rejestracji wybierają, kierując się kryterium najbardziej korzystnego dla nich systemu podatkowego, np. w tzw. rajach podatkowych. Takie praktyki prowadzą do unikania podatków, a tym samym obniżają potencjalne zyski wszystkich krajów, w których dana korporacja operuje. Według szacunków OECD, straty finansowe wynoszą rocznie 100-240 miliardów dolarów, co stanowi 4-10% globalnych wpływów z podatku dochodowego od osób prawnych[62].

Inicjatywa BEPS po raz pierwszy została ogłoszona i przyjęta przez kraje G20 w 2013 roku. Powstał wtedy Plan Działania *(OECD Action Plan)* międzynarodowych strategii podatkowych, które miałyby uniemożliwić wykorzystywanie rozbieżności i luk w przepisach w celu przenoszenia zysków do rajów podatkowych. W 2015 roku OECD opublikowało kompleksowy pakiet działań *(BEPS package)* zawierający konkretne wytyczne do zastosowania w krajowych systemach podatkowych i propozycję zmian przepisów. W pakiecie znalazły się również minimalne standardy, które są priorytetowe i powinny zostać wdrożone jak najszybciej. W czerwcu 2016 roku, w odpowiedzi na propozycję grupy G20, OECD przygotowało ramy włączenia do inicjatywy BEPS *(Inclusive Framework on BEPS)* krajów rozwijających się, na równych zasadach, przy jednoczesnym zobowiązaniu się tych państw do wdrożenia w swoich systemach podatkowych minimalnych standardów zawartych w pakiecie[63]. W grudniu 2016 roku zakończono negocjacje nad konwencją wielostronną, implementującą środki traktatowego prawa podatkowego i mającą zapobiegać erozji podstawy opodatkowania i przenoszenia zysku, tzw. Konwencją MLI *(Multilateral convention to implement tax treaty-related measures to prevent base erosion and profit shifting).* Celem konwencji jest zapobieganie uchylaniu się od opodatkowania[64].

W styczniu 2019 roku OECD zapowiedziało kontynuację inicjatywy BEPS w celu dalszej pracy nad osiągnięciem globalnego konsensusu dotyczącego sposobu opodatkowania międzynarodowych przedsiębiorstw w erze cyfrowej[65]. Na początku 2020 roku OECD przyjęło stanowisko uwzględniające dwa podejścia, tzw. dwa filary:

- **1 filar –** opiera się na założeniu, że podatek cyfrowy obejmie firmy, których globalne przychody przekraczają 750 mln dolarów. Zgodnie z założeniem OECD, firmy miałyby płacić podatki w krajach macierzystych, do kwoty powyższego limitu, a powyżej tej kwoty zyski z podatku byłyby dzielone zgodnie z geografią sprzedaży.

62 *International collaboration to end tax avoidance* (https://www.oecd.org/tax/beps/)
63 *Implementing OECD/G20 BEPS Package in Developing Countries*, str.9 (https://www.ibfd.org/sites/ibfd.org/files/content/pdf/wp_implementing_beps_package_developing_countries.pdf)
64 *Konwencja MLI* (https://www.podatki.gov.pl/podatkowa-wspolpraca-miedzynarodowa/konwencja-mli/)
65 *International community makes important progress on the tax challenges of digitalisation* (http://www.oecd.org/tax/international-community-makes-important-progress-on-the-tax-challenges-of-digitalisation.htm)

- **2 filar –** opiera się na propozycji wdrożenia obowiązujących na całym świecie minimalnych stawek podatkowych, co miałoby utrudnić korzystanie z tzw. rajów podatkowych. Minimalne stawki byłyby niezależne od jurysdykcji podatkowej.

Z proponowanym przez OECD rozwiązaniem nie zgadzają się Stany Zjednoczone, które stoją na stanowisku, że regulacje spowodują dyskryminację amerykańskich firm technologicznych. W dyskursie pojawiają się również obawy związane z obsługą administracyjną podatku, a także koniecznością dostosowania prawa podatkowego wielu państw. Ostateczne rozwiązanie ma zostać wypracowane do końca 2020 roku. W oczekiwaniu na międzynarodowy konsensus prace nad wprowadzeniem własnego podatku cyfrowego zawiesiła Unia Europejska, a także Polska. Do końca 2020 roku trwa również wstrzymanie rozmów na temat podatku cyfrowego między USA a Francją[66].

66 W 2019 r. Francja wprowadziła 3% podatek nałożony na firmy o globalnych obrotach powyżej 750 mln dolarów i 25 mln dolarów we Francji. W odpowiedzi prezydent USA Donald Trump zagroził wprowadzeniem ceł na francuskie towary. W styczniu 2020 roku na Światowym Forum Ekonomicznym w Davos obaj prezydenci uzgodnili wstrzymanie zarówno podatku, jak i ceł, do końca 2020 roku, czyli do czasu wypracowania międzynarodowego rozwiązania przez OECD.

SOJUSZ PÓŁNOCNOATLANTYCKI

Rozbudowa współpracy w ramach Cyber Defence Pledge i modernizacja systemów NATO

Sojusz Północnoatlantycki *(North Atlantic Treaty Organization, NATO)* to układ wojskowy zrzeszający obecnie 29 państw. Został ustanowiony w 1949 roku, kiedy to w Waszyngtonie przedstawiciele 12 krajów podpisali Traktat Północnoatlantycki. Polska dołączyła do NATO 12 marca 1999 roku.

Celem istnienia NATO była obrona przed Związkiem Socjalistycznych Republik Radzieckich. Po jego rozpadzie Sojusz zaczął pełnić rolę stabilizacyjną. Wraz z rozwojem nowoczesnych technologii, cyberbezpieczeństwo staje się coraz istotniejszym tematem na forum NATO. Podczas szczytu w Warszawie w 2016 roku, Sojusz uznał cyberprzestrzeń za czwartą domenę prowadzenia działań bojowych. Obecnie NATO wkłada wiele wysiłku, aby zabezpieczyć swoje systemy i sieci oraz pomóc sojusznikom w zwiększeniu ich zdolności do skutecznej cyberobrony.

W marcu 2019 roku Jens Stoltenberg przedstawił raport roczny Sekretarza Generalnego NATO za rok 2018[67]. W tematyce cyberbezpieczeństwa priorytetowe działania dotyczyły ochrony wewnętrznych sieci Sojuszu oraz realizacji *Cyber Defence Pledge* – a więc wzmacniania tzw. cyberodporności sojuszników.

Inicjatywy podejmowane w 2019 roku przez NATO stanowiły w dużej mierze kontynuację tych działań. Skupiały się przede wszystkim na budowaniu współpracy poprzez wspólne ćwiczenia oraz szkolenia, a także na modernizacji systemów teleinformatycznych NATO. Najważniejsze wydarzenia 2019 roku to przyjęcie wymagań dotyczących odporności cywilnej infrastruktury telekomunikacyjnej, w tym 5G, oraz zainicjowanie centrum współpracy w zakresie cyberbezpieczeństwa dla sojuszników ***(Cyber Security Collaboration Hub).*** Poza tym, podczas szczytu w Londynie, NATO uznało przestrzeń kosmiczną za kolejną dziedzinę operacyjną. Aby wspierać rozwój potencjału technologicznego Sojusz zaplanował otwarte konkursy na kwotę **1,4 mld euro,** z czego blisko **220 mln euro** przeznaczono na projekty z obszaru cyberbezpieczeństwa.

Najważniejsze wydarzenia dotyczące cyberbezpieczeństwa NATO w 2019 roku:

- Przyjęcie przez ministrów obrony z państw NATO nowych **wymagań dotyczących odporności cywilnej infrastruktury telekomunikacyjnej, w tym 5G.**
- Zainicjowane centrum współpracy w zakresie cyberbezpieczeństwa dla sojuszników *(Cyber Security Collaboration Hub).*
- **Szczyt NATO w Londynie,** podczas którego przywódcy Sojuszu uznali przestrzeń kosmiczną za kolejną dziedzinę operacyjną NATO.
- **Rozwój potencjału technologicznego NATO** – zaplanowano **otwarte konkursy** na kwotę **1,4 mld euro,** z czego blisko **220 mln euro** na projekty z obszaru cyberbezpieczeństwa.

67 *Secretary General's Annual Report: „NATO: fit for the future"* (https://www.nato.int/cps/en/natohq/news_164519.htm)

Współpraca

12 lutego 2019 roku Agencja NATO ds. Komunikacji i Informacji (NCI) podłączyła do chronionej sieci NATO zespoły reagowania na incydenty cyberbezpieczeństwa z pięciu krajów: **Belgii, Francji, Holandii, Wielkiej Brytanii i Stanów Zjednoczonych.** Był to pierwszy krok zmierzający do utworzenia centrum współpracy w zakresie cyberbezpieczeństwa *(Cyber Security Collaboration Hub*[68]*)*. Docelowo do sieci podłączone mają zostać wszystkie kraje Sojuszu. Ma to umożliwić szybkie i bezpieczne dzielenie się informacjami.

23 maja 2019 roku w Londynie odbyła się druga konferencja podsumowująca realizację *Cyber Defence Pledge*[69]. Sekretarz generalny NATO Jens Stoltenberg wskazał, że ważną częścią strategii odstraszania może być **atrybucja ataków.** Kolejnym istotnym aspektem jest **wykorzystywanie możliwości ofensywnych w cyberprzestrzeni, zapewnianych przez sojuszników.** Każdy kto zaatakuje Sojusz w cyberprzestrzeni powinien spodziewać się odpowiedzi, za pomocą wszelkich adekwatnych narzędzi, którymi dysponuje NATO. Nie znaczy to jednak, że odpowiedź na atak w cyberprzestrzeni nastąpi z wykorzystaniem środków teleinformatycznych. Równie dobrze może to być odpowiedź kinetyczna.

Przykładem zacieśniającej się współpracy jest powiększenie **Centrum Doskonałości Cyberobrony NATO** *(NATO Cooperative Cyber Defence Centre of Excellence, CCDCOE),* o czterech nowych członków. 14 czerwca 2019 roku do CCDCOE dołączyły **Bułgaria, Dania, Norwegia i Rumunia**[70]**.** Obecnie Centrum ma 25 członków i jest największym spośród akredytowanych przez Sojusz centrów doskonalenia. Co więcej, w październiku proces przystąpienia do CCDCOE zainicjowała Republika Irlandii. Wśród projektów zrealizowanych przez CCDCOE w 2019 roku warto wymienić:

Dokument badawczy ***Huawei, 5G, and China as a Security Threat,*** który wskazuje, że wdrożenie sieci 5G powinno być w pierwszej kolejności wyborem strategicznym, a dopiero w dalszej – wyborem technologicznym[71]

Cyber Law Toolkit[72] czyli zestaw narzędzi dla prawników, składający się z kilkunastu scenariuszy. Każdy zawiera opis cyberincydentów inspirowanych prawdziwymi przykładami oraz szczegółową analizę prawną

Swoistym podsumowaniem roku był **Szczyt NATO w Londynie**[73]**,** który odbył się 3-4 grudnia. W deklaracji londyńskiej znalazło się kilka punktów nawiązujących do cyberbezpieczeństwa, sieci 5G oraz rozwijania nowoczesnych technologii:

- Uznanie roli nowoczesnych technologii i podkreślenie, że ważne jest utrzymanie przewagi technologicznej, przy zachowaniu zachodnich wartości i norm.
- Zobowiązanie do zapewnienia bezpieczeństwa komunikacji, w tym sieci 5G (w oparciu o bezpieczne i odporne systemy).

68 *New NATO hub will gather the Alliance's cyber defenders* (https://www.nato.int/cps/en/natolive/news_163358.htm)
69 Dokument przyjęty na szczycie w Warszawie w 2016 roku jest wynikiem dążenia Sojuszu do zwiększenia nacisku na cyberodporność na poziomie krajowym. Sojusznicy zobowiązali się do podniesienia swojego poziomu cyberbezpieczeństwa. Więcej w publikacji „*Cyberbezpieczeństwo A.D. 2018"* (https://cyberpolicy.nask.pl/cyberbezpieczenstwo-a-d-2018/)
70 *NATO Cooperative Cyber Defence Centre of Excellence grows to 25 members* (https://ccdcoe.org/news/2019/nato-cooperative-cyber-defence-centre-of-excellence-grows-to-25-members/)
71 *Huawei, 5G, and China as a Security Threat* (https://ccdcoe.org/library/publications/huawei-5g-and-china-as-a-security-threat/)
72 *Cyber Law Toolkit* (https://cyberlaw.ccdcoe.org/wiki/Main_Page)
73 *Secretary General: as the world changes, NATO will continue to change* (https://www.nato.int/cps/en/natohq/news_171581.htm)

- Podkreślenie, że Sojusz stoi w obliczu zagrożeń teleinformatycznych i hybrydowych.
- Uznanie przestrzeni kosmicznej za dziedzinę operacyjną NATO.

Ćwiczenia, szkolenia, konferencje

NATO podkreśla, że budowanie efektywnej współpracy musi być oparte o wymianę wiedzy między Sojusznikami, a także ćwiczone w warunkach zbliżonych jak najbardziej do realnych scenariuszy. Dlatego organizuje wiele ćwiczeń cyberbezpieczeństwa i podejmuje liczne inicjatywy związane z budowaniem kompetencji sojuszniczych w tym zakresie.

9 kwietnia – *Locked Shields* w Tallinie. W tym roku zadaniem uczestników była obrona fikcyjnej wyspy Berylii, która przygotowywała się do wyborów. Najlepsza okazała się drużyna z Francji, a drugie i trzecie miejsca zajęli odpowiednio – Czesi i Szwedzi.

25 kwietnia – warsztaty przed wyborami do Parlamentu Europejskiego. Podczas wydarzenia zorganizowanego przez Agencję ds. Komunikacji i Informacji NATO oraz CERT-EU, eksperci omawiali środki przeciwdziałania na cyberzagrożenia oraz dezinformację.

28 maja – konferencja ***Cyber Conflict*** *(CyCon2019).* Tematem przewodnim było *Silent Battle.*

Wrzesień – uruchomiono najnowsze **centrum treningowe *NCI Academy* w Portugalii.** Każdego roku będzie szkolić 4 tys. studentów. Projekt warty 20 mln euro ma zapewnić Sojuszowi wiodącą pozycję w dziedzinie nowoczesnych technologii. W październiku w nowym centrum odbyła się czwarta edycja *Education and Training Conference.*

25 września – konferencja **NATO *Information and Communication Conference*** w Polsce, dotycząca komunikacji strategicznej.

4 października – ćwiczenia systemu zarządzania incydentami NATO w Czarnogórze w ramach *NATO Science for Peace and Security Program.* W ich trakcie przetestowano *Next Generation Incident Command System,* czyli oprogramowanie, które ułatwia współpracę na wszystkich poziomach planowania oraz reagowania.

15 października – największa konferencja NATO dotycząca cyberbezpieczeństwa – **NIAS 2019,** w której udział wzięło ponad 1800 delegatów z 46 krajów. Konferencja odbyła się pod hasłem *Cloud-Data-Security.*

2 grudnia – ćwiczenia ***Cyber Coalition 2019*** w Tartu. Wzięło w nich udział ok. 900 uczestników z 28 państw członkowskich NATO oraz krajów partnerskich.

Modernizacja

W maju Agencja ds. Komunikacji i informacji NATO *(NATO Communication and Information Agency, NCI)* poinformowała o planowanych **otwartych konkursach** skierowanych do organizacji i przedsiębiorstw rozwijających potencjał technologiczny NATO. Budżet 18-miesięcznego programu to **1,4 mld euro,** z czego blisko 220 mln euro przeznaczono na projekty z obszaru cyberbezpieczeństwa[74].

Warto również wspomnieć o planach NCI dotyczących **modernizacji wewnętrznych systemów cyberbezpieczeństwa NATO.** Agencja wysłała w październiku zapytanie ofertowe opiewające na 20 mln euro – realizacja zamówienia ma wesprzeć wdrożenie Pakietu Zdolności 120 *(Capability Package 120)*, który w sposób etapowy odświeży wszystkie systemy bezpieczeństwa komunikacji i informacji[75].

Sieć 5G – wyzwanie strategiczne i technologiczne

Jednym z istotniejszych tematów, podejmowanych przez Sojusz w 2019 roku, była kwestia sieci 5G.[76] W kwietniu 2019 roku Centrum Doskonałości ds. Cyberobrony NATO (CCDCOE) przygotowało publikację badawczą: *Huawei, 5G, and China as a Security Threat.* Jej autorzy wskazali, że wiele krajów wyraziło zaniepokojenie powiązaniami chińskich firm, zajmujących się technologiami komunikacyjnymi, ze służbami wywiadowczymi. W związku z tym, **NATO powinno traktować wdrożenie 5G jako wybór przede wszystkim strategiczny, a dopiero w drugiej kolejności jako wybór technologiczny.**

Aby działania NATO i UE w tym zakresie były skoordynowane, w październiku 2019 roku odbyło się spotkanie zastępcy sekretarza generalnego NATO Rose Gottemoeller z komisarzem ds. Bezpieczeństwa Unii Sir Julianem Kingiem. Omawiano na nim wyzwania związane z cyberbezpieczeństwem. Komisarz King poinformował m.in. **o skoordynowanej unijnej ocenie ryzyka cyberbezpieczeństwa sieci 5G.**

W październiku Ministrowie Obrony NATO przyjęli **nowe wymagania dotyczące odporności cywilnej infrastruktury telekomunikacyjnej, w tym 5G.** Zgodzili się, że powinny one obejmować dokładną ocenę ryzyka i podatności na zagrożenia (identyfikacja zagrożeń teleinformatycznych czy konsekwencje własności zagranicznej). Zobowiązanie do zapewnienia bezpieczeństwa komunikacji, w tym sieci 5G, znalazło się w deklaracji ze Szczytu NATO w Londynie.

Dezinformacja

Sojusz zajmował się także zagadnieniami związanymi z zagrożeniami hybrydowymi, w tym kampaniami dezinformacyjnymi (również w odniesieniu do wyborów do Parlamentu Europejskiego). W maju w kwaterze głównej NATO odbyło się pierwsze spotkanie doradców ds. bezpieczeństwa narodowego poświęcone zagrożeniom hybrydowym. Sekretarz generalny Jens Stoltenberg podkreślił, że NATO musi być przygotowane zarówno na zagrożenia konwencjonalne i hybrydowe[77].

Komunikacja strategiczna była także tematem konferencji **NATO *Information and Communication Conference,*** która odbyła się 25 września w Polsce. Wzięło w niej udział blisko

74 *Review NATO's 1.4 billion EUR in upcoming business opportunities* (https://www.ncia.nato.int/NewsRoom/Pages/20190521_NITEC19_Day2.aspx)
75 *NATO Agency releases Request for Quotation to refresh cyber security technology* (https://www.ncia.nato.int/NewsRoom/Pages/20191104-NATO-Agency-releases-Request-for-Quotation-to-refresh-cyber-security-technology.aspx)
76 Należy jednak pamiętać, że stanowisko CCDCOE nie jest stanowiskiem NATO.
77 *National Security Advisers meet at NATO Headquarters* (https://www.nato.int/cps/en/natohq/news_166394.htm)

400 ekspertów reprezentujących dowództwo NATO, kraje wchodzące w skład Sojuszu oraz kraje partnerskie. Uczestnicy brali udział w warsztatach, pracach grup roboczych oraz sesjach plenarnych o komunikacji strategicznej Sojuszu.

Szczególnie aktywne w zakresie przeciwdziałania dezinformacji było **NATO StratCom COE,** które przygotowało wiele raportów oraz dokumentów dotyczących kampanii dezinformacyjnych. Wśród nich wymienić warto m.in.:

- ***Czarny rynek manipulacji mediami społecznościowymi***[78] – dokument opisuje dynamiczny rynek manipulacji w social mediach. Przeprowadzone badania pokazały, że wciąż można łatwo i tanio prowadzić dezinformację online – pomimo zobowiązań firm, które podpisały *Kodeks postępowania w zakresie zwalczania dezinformacji.* Rynek manipulacji dominują rosyjscy dostawcy tego typu usług.
- ***Rola Deepfakes w kampaniach o szkodliwym wpływie***[79] – autorzy raportu wskazują, że już niedługo tego typu algorytmy uczenia maszynowego, będą wykorzystywane na porządku dziennym. Skutkiem ubocznym będzie osłabienie zaufania w sferze online. W kontekście komunikacji strategicznej i cyberzagrożeń, *deepfakes* z czasem staną się kluczowe dla kampanii dezinformacyjnych wykorzystywanych w konflikcie hybrydowym.

78 *The Black Market for Social Media Manipulation* (https://www.stratcomcoe.org/black-market-social-media-manipulation)
79 *The Role of Deepfakes in Malign Influence Campaigns* (https://www.stratcomcoe.org/role-deepfakes-malign-influence-campaigns)

O TYM SIĘ MÓWIŁO

Najważniejsze tematy 2019 roku


5G
fake

CYBERBEZPIECZEŃSTWO 2019

ZMIANA DOTYCHCZASOWYCH PARADYGMATÓW?

– dr Magdalena Wrzosek –

Pod wieloma względami, dla polityczno-strategicznego dyskursu w zakresie cyberbezpieczeństwa, rok 2019 był przełomowy. Doszło do pewnej zmiany paradygmatu, na którym do tej pory opierano politykę w zakresie bezpieczeństwa teleinformatycznego. Przy dyskusjach o suwerenności cyfrowej coraz częściej i coraz głośniej wybrzmiewają kwestie technologiczne, a dane nieco straciły na znaczeniu. Podkreślana jest przede wszystkim konieczność zapewnienia bezpieczeństwa łańcucha dostaw oraz zaufania do nowych rozwiązań technologicznych i ich dostawców. Dane, dominacja GAFA[80], oraz kwestia bałkanizacji Internetu[81], które do tej pory dominowały w dyskusjach strategiczno – politycznych, w pewien sposób odeszły na dalszy plan.

W 2019 roku Europie przyjęto ***Akt o cyberbezpieczeństwie,*** który znacznie wzmocnił rolę Europejskiej Agencji ds. Cyberbezpieczeństwa (ENISA) oraz zainicjował europejską certyfikację produktów i usług ICT. Prowadzono także działania zmierzające do uruchomienia sieci 5G w sposób jak najbardziej skoordynowany, przy równoczesnym zapewnianiu właściwego poziomu bezpieczeństwa. Odbyła się również szeroko zakrojona dyskusja dotycząca dostawców technologii, zwłaszcza w kontekście mobilnych sieci nowej generacji (5G).

Dane, które często określane są ropą naftową XXI wieku, a także związana z nimi narracja budowy gospodarki opartej na danych, to oczywiście ważny element narracji strategiczno – politycznej w kontekście cyfrowej suwerenności. Ale 2019 rok udowodnił, że być może jej fundamentem jest, niedawno nieco zapomniana, technologia. Potrzeba dyskusji nad kwestią technologii była bardzo wyraźnie widoczna w narracji USA w stosunku do firmy Huawei. Stany Zjednoczone włożyły wiele wysiłku w przekonanie sojuszników do rezygnacji z rozwiązań chińskiej firmy. To technologia, a nie jak dotąd dane, znalazła się w centrum działań dyplomatycznych i ekonomicznych. Jest to istotna zmiana paradygmatu w stosunku do ubiegłych lat i podejścia do tematyki cyberbezpieczeństwa w dyskursie politycznym. Zmiana ta odbywa się w cieniu napięcia pomiędzy globalną gospodarką cyfrową, a obowiązkiem zapewnienia właściwego poziomu cyberbezpieczeństwa, ciążącym na wszystkich rządach i państwach. Szybki rozwój technologii sprawia, że państwa narodowe stają przed ważnym dylematem: czy uczestniczyć w dynamicznej transformacji cyfrowej i budowie cyfrowej gospodarki, nawet kosztem rezygnacji z kontroli nad bezpieczeństwem wykorzystywanej technologii? Jest to o tyle istotne, że podjęte wybory mogą mieć przełożenie na poziom cyberbezpieczeństwa samego państwa i obywateli.

Na początku 2020 roku[82] Komisja Europejska ogłosiła nową Europejską strategię transformacji cyfrowej UE *(Shaping Europe's digital future).* Znamienne, że Komisja położyła silny nacisk na cyfrową suwerenność w kontekście zapewnienia integralności i odporności sieci teleinformatycznych. Zdaniem KE wymaga to stworzenia odpowiednich warunków, umożliwiających rozwój i wdrożenie własnych zdolności w tym zakresie tak, aby Europa mogła się uniezależnić od technologii tworzonej w innych częściach świata[83]. Jednym z działań zapowiedzianych w *Strategii* jest przegląd Dyrektywy NIS.

80 Skrót odnoszący się do czterech technologicznych gigantów: Google, Apple, Facebook, Amazon.
81 Bałkanizacja Internetu jest rozumiana jako stopniowe odchodzenie od światowej sieci na rzecz internetów krajowych, w których to państwa narodowe będą kontrolować sieć, w zależności od własnej polityki i zgodnie z własną technologią.
82 Komisja Europejska opublikowała komunikat *Shaping Europe's digital future* 19 lutego 2020 roku
83 Komunikat KE *Shaping Europe's digital future*, s. 3.

Koncepcja cyfrowej suwerenności

Pojęcia „suwerenność" użył po raz pierwszy francuski prawnik i teoretyk państwa Jean Bodin, którego *Sześć ksiąg o Rzeczypospolitej* stało się podstawą francuskiej monarchii absolutnej, wprowadzonej za panowania Ludwika XIV. Zdaniem Bodin suwerenność to absolutna, trwała, wieczna i niepodzielna władza nad ludźmi, która spaja państwo i pozwala na zachowanie niezależności wewnętrznej i zewnętrznej. Koncepcja ta jest często określana „władzą skutecznie działającą"[84].

W najprostszym znaczeniu suwerenność jest więc zasadą absolutnej i niepodważalnej władzy. W nauce o polityce pojęcie suwerenności ma cztery wymiary: prawny, polityczny, wewnętrzny i zewnętrzny.

Cztery wymiary pojęcia suwerenności[85]

Suwerenność prawna	Niepodważalne prawo do zachowania zgodnego z przepisami
Suwerenność polityczna	Nieograniczona władza polityczna oraz wymaganie posłuszeństwa (monopol państwa na użycie siły)
Suwerenność wewnętrzna	Największa władza w państwie, która podejmuje decyzje wiążące wszystkich obywateli, grupy i instytucje w granicach terytorialnych państwa
Suwerenność zewnętrzna	Miejsce państwa w porządku międzynarodowym, a także jego zdolność do działania w sposób autonomiczny

W stosunkach międzynarodowych, suwerenność oznacza formalny status państwa, pozwalający na samodzielny i nieograniczony udział w życiu międzynarodowym[86]. Tylko państwo suwerenne może, bez zgody i upoważnienia kogokolwiek, podejmować wszelką aktywność międzynarodową, we własnym imieniu, w wiążący sposób, oraz ponosić pełną odpowiedzialność za swoje działania.

> Suwerenność państwa jest związana ze zdolnością do samodzielnego, niezależnego od innych podmiotów, sprawowania władzy politycznej nad określonym terytorium lub grupą. Niezależność odnosi się zarówno do działań wewnętrznych, jak i zewnętrznych.

W stosunkach międzynarodowych prawna definicja suwerenności została użyta po raz pierwszy w 1928 roku w sprawie *Island of Palmas*[87]. Definicja ta zakłada, że: „suwerenność w relacji pomiędzy państwami oznacza niezależność. Polega ona na egzekwowaniu funkcji państwa, niezależnie od części świata, w której znajduje się dane terytorium"[88].

Pierwsza dekada XXI wieku przyniosła bardzo silne i szybie nasycenie tzw. cybersfery, poprzez tworzenie wzajemnych połączeń między krajami, instytucjami, ludźmi, urządzeniami i aplikacjami. Szerokie wdrożenie technologii takich jak smartfony, Wi-Fi i media społecznościowe, stworzyło nowe rynki i nowe wzorce zachowań społecznych, które wpłynęły na życie milionów ludzi na całym świecie. Wiele aktywności zostało przeniesionych do sieci. Krytyczne dla państwa sektory, takie jak energetyka, finanse czy transport, również stały się zależne od systemów teleinforma-

84 S. Filipowicz, *Historia myśli polityczno – prawnej*, Arche, Gdańsk, 2007.
85 Opracowane na podstawie: A. Heywood, *Politologia*, PWN, Warszawa 2006.
86 S.D. Krasner, *Power, the State, and Sovereignty, Routledge*, London – New York, 2009.
87 *Island of Palmas case* dotyczyła sporu pomiędzy USA a Holandią na temat przynależności wysp do tych państw. Stały Trybunał Arbitrażow przyznał rację argumentacji Holandii.
88 *Island of Palmas arbitral award*, s. 838, (https://legal.un.org/riaa/cases/vol_II/829-871.pdf)

tycznych. Rewolucja cyfrowa przyczyniła się do powstania nowej domeny aktywności państw – cyberprzestrzeni, która stopniowo zaczęła być adresowana jako domena, w której konieczne jest zapewnienie bezpieczeństwa (cyberbezpieczeństwa).

W 2016 roku została przyjęta Dyrektywa NIS – pierwsze europejskie prawo w zakresie cyberbezpieczeństwa, a Sojusz Północnoatlantycki uznał cyberprzestrzeń za domenę operacji wojskowych[89]**.** Następstwem tych działań były rozważania nad tzw. suwerennością cyfrową. Jest to wciąż nowa koncepcja, która nie doczekała się jeszcze pełnej definicji, ale od pewnego czasu prowokuje coraz szerszą dyskusję na arenie międzynarodowej.

Jako pierwsi zwrotu „cyfrowa suwerenność" użyli Francuzi. W 2011 roku Pierre Bellnger[90] zdefiniował cyfrową suwerenność jako „kontrolę nad naszą teraźniejszością i przyszłością związaną z wykorzystaniem technologii i sieci komputerowych"[91]. Ta krótka definicja bardzo dobrze oddaje esencję całej dyskusji. Chodzi o zapewnienie niezależności działań państwa w nowej sferze aktywności – cyberprzestrzeni. Na poziomie Unii Europejskiej dyskusja na ten temat toczy się już od dłuższego czasu, przy czym zagadnienie to nazywane jest suwerennością cyfrową dopiero od niedawna. W obliczu budowy w Europie tzw. Jednolitego Rynku Cyfrowego, wielokrotnie powracał temat wzrastającej dominacji ekonomicznej i politycznej GAFA, czyli największych technologicznych gigantów (Google, Apple, Facebook, Amazon). Szczególnie zwracano uwagę m.in. na algorytmy kontrolujące dostęp do wiedzy, prowadzenie kampanii wyborczych w mediach społecznościowych, a także na kontrolę nad danymi użytkowników sieci. To wszystko sprawia, że wiedza tych firm o internautach jest niejednokrotnie większa, niż wiedza poszczególnych państw o ich własnych obywatelach. Dlatego w ogólnym dyskursie polityczno – strategicznym silnie akcentowała była kwestia danych osobowych oraz konieczności ich ochrony.

Strategia Jednolitego Rynku Cyfrowego dla Europy – Strategia DSM

6 maja 2015 roku Komisja Europejska opublikowała *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Strategia jednolitego rynku cyfrowego dla Europy.*

Dokument zakłada zniesienie ograniczeń regulacyjnych w kwestiach cyfrowych w taki sposób, aby możliwe było zbudowanie Wspólnego Europejskiego Rynku Cyfrowego. Ma to pomóc w szybszym rozwoju usług cyfrowych, a tym samym budować konkurencyjność europejskich firm. Jednym z działań związanych z DSM jest cyberbezpieczeństwo. Komisja podkreśla, że tylko bezpieczne usługi cyfrowe będą wykorzystywane przez obywateli.

Założenia strategii są oparte na trzech podstawowych filarach, do których została przydzielona lista konkretnych działań. Ich realizacja ma zapewnić wypracowanie jednolitych ram prawnych dla wspólnego rynku cyfrowego UE:

1. Lepszy dostęp konsumentów i przedsiębiorców do towarów sprzedawanych przez Internet;
2. Środowisko, w którym sieci i usługi cyfrowe mogą się rozwijać;
3. Cyfrowość jako siła napędowa wzrostu.

89 Podczas Szczytu NATO w Warszawie, w 2016 roku przyjęto także *Cyber Defence Pledge* – dokument w którym sojusznicy zobowiązali się do podniesienia swojego poziomu cyberbezpieczeństwa. Najważniejsze postanowienia dotyczyły przede wszystkim: konieczności wzmocnienia cyberbezpieczeństwa krajowych sieci oraz infrastruktury; rozwój kompetencji państw NATO w taki sposób aby możliwa była skuteczna obrona przed zagrożeniami w cyberprzestrzeni; stosowanie prawa międzynarodowego w cyberprzestrzeni oraz współpraca z UE; międzynarodowa współpraca w zakresie edukacji, szkoleń i wymiany informacji.

90 Założyciel i CEO francuskiej stacji radiowej Skyrock oraz sieci społecznościowej skyrock.com.

91 F. Gueham, *Digital Sovereignty*, Foundation Pour L'Innovation Politique, Styczeń 2017.

Kolejnym ważnym elementem tej dyskusji jest **zastosowanie prawa w cyberprzestrzeni i kwestia zarządzania Internetem.**

W 2007 roku, w wyniku ataku DDoS, zablokowane zostały strony estońskich banków, gazet, ministerstw oraz parlamentu. Jasne stało się, że poprzez działanie w cyberprzestrzeni, można skutecznie sparaliżować funkcjonowanie całego państwa i przyczynić się do znacznych strat ekonomicznych. Mimo, że nie udowodniono bezpośrednich związków pomiędzy odpowiedzialną za te ataki grupą *Nasi*, a Federacją Rosyjską, wielu ekspertów wyraziło przekonanie, że był to atak spełniający przesłanki tzw. cyberwojny. Na początku, Estonia powoływała się nawet na art. 5 Paktu Północnoatlantyckiego. Jednak później, w obliczu braku odzewu ze strony społeczności międzynarodowej, zrezygnowała. Wydarzenia te jednak zintensyfikowały działania zmierzające do określenia zasad funkcjonowania prawa międzynarodowego w cyberprzestrzeni.

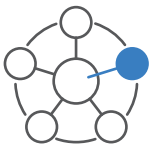
W 2013 roku *Cambridge University Press* wydała *Tallinn Manual 1.0*. Jest to akademicki podręcznik analizujący sposób implementacji prawa międzynarodowego w cyberprzestrzeni[92]. Cztery lata później opublikowane zostało drugie wydanie ***Tallinn Manual 2.0***, które poszerza niektóre kwestie. Cały pierwszy rozdział tej publikacji odnosi się właśnie do suwerenności cyfrowej. Autorzy opisują **pięć zasad cyfrowej suwerenności[93].**

Pięć zasad cyfrowej suwerenności według *Tallinn Manual 2.0*

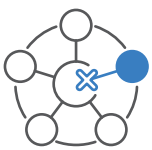
Zasada suwerenności państwa obowiązuje w cyberprzestrzeni

Suwerenność wewnętrzna w cyberprzestrzeni jest związana z infrastrukturą teleinformatyczną, osobami oraz aktywnością mającą miejsce na terytorium państwa, z zastrzeżeniem międzynarodowych zobowiązań prawnych

Suwerenność zewnętrzna w cyberprzestrzeni jest związana z wolnością do podejmowania działań w cyberprzestrzeni w relacjach międzynarodowych, z zastrzeżeniem międzynarodowych zobowiązań prawnych



Immunitet suwerenności i nienaruszalności oznacza, że jakakolwiek ingerencja państwa w infrastrukturę teleinformatyczną należącą do innego państwa, niezależnie od tego gdzie się znajduje, stanowi naruszenie suwerenności



Naruszenie suwerenności w cyberprzestrzeni odnosi się do zakazu podejmowania operacji w cyberprzestrzeni, naruszających suwerenność innego państwa

Na podstawie tych zasad państwo ma m.in. prawo odłączenia od sieci każdej infrastruktury teleinformatycznej, która znajduje się na jego

92 Wydawnictwo jest owocem prac międzynarodowej grupy ekspertów, powołanej przy *Cooperative Cyber Defence Centre of Excellence w Tallinie*, która pracowała w latach 2009-2012. Grupa prowadzona była przez prof. Michaela N. Schmitta, przewodniczącego departamentu prawa międzynarodowego w *United States Naval War College*.

93 Tallinn Manual 2.0 on the International Law application to Cyber Operations; Międzynarodowa Grupa Ekspertów, Cambridge University Press, Cambridge 2017.

terytorium, i której działanie może stanowić naruszenie suwerenności państwa[94]. Dodatkowo, suwerenność wewnętrzna oznacza, że państwo może, częściowo lub w całości, ograniczyć dostęp do sieci osobom znajdującym się na jego terytorium, w szczególności do określonych treści online[95]. Istnieje także zasada powstrzymywania się od wrogich działań w cyberprzestrzeni[96]. Suwerenność zewnętrzna oznacza natomiast, że państwa mogą angażować się w działalność w cyberprzestrzeni w stosunkach międzynarodowych, zgodnie z własnymi decyzjami, o ile nie naruszają norm prawa międzynarodowego[97]. Naruszeniem suwerenności jest każda ingerencja w granicach terytorium państwa, związana z działaniami w cyberprzestrzeni. Jako przykład eksperci podają użycie przez dane państwo nośnika USB ze złośliwym oprogramowaniem, żeby zakłócić działalność systemów na terytorium innego państwa[98]. W tym celu konieczne jest jednak dokonanie atrybucji, a więc przedstawienie dowodów, że za działanie to odpowiada inne państwo.

Rozważania podejmowane przez autorów *Tallinn Manual*, mają szeroki kontekst międzynarodowy. Od 2003 roku, przy ONZ działa GGE *(Grupa ekspertów rządowych ds. rozwoju w dziedzinie informacji i telekomunikacji w kontekście bezpieczeństwa międzynarodowego)*[99], której kolejne „edycje" analizują kwestie zastosowania prawa międzynarodowego w cyberprzestrzeni. Największe osiągnięcia miała trzecia grupa GGE, obradująca w latach 2012-2013, która uznała że prawo międzynarodowe ma zastosowanie w cyberprzestrzeni. Nie brzmi to być może zbyt odkrywczo, ale w stosunkach międzynarodowych było prawdziwym przełomem. Grupa zgodziła się[100], że działalność państw w Internecie, również działalność infrastruktury informacyjno-komunikacyjnej na terytorium danego państwa, podlega *Karcie Narodów Zjednoczonych,* normom i zobowiązaniom dotyczącym suwerenności państwowej oraz pozostałym przepisom prawa. Po tych ustaleniach w pracach grupy doszło niestety do impasu. Obrady grupy piątej zakończyły się brakiem konsensusu, a obecnie nad wyzwaniami pracuje grupa szósta, która ma przedstawić swój raport pod koniec 2021 roku[101].

Równolegle z powołaniem szóstej grupy GGE, ONZ utworzyła nowy format dyskusji: Otwartą grupę roboczą ds. Rozwoju technologii teleinformatycznych w kontekście bezpieczeństwa międzynarodowego *(Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security* ***– OEWG****)*[102]. Jest to szersze gremium, niż w przypadku grupy GGE. Do udziału w obradach dopuszczone są wszystkie państwa członkowskie, a nie tylko 25 z nich. Konsultacje prac OEWG mają być natomiast przeprowadzone w formule dopuszczającej udział przedstawicieli biznesu, trzeciego sektora oraz ośrodków akademickich. Powołanie tego formatu jest próbą przełamania dotychczasowego impasu, ponieważ na forum grupy GGE ścierają się interesy polityczne państw, o odmiennym podejściu do kwestii zarządzania Internetem. Z jednej strony państwa reprezentujące stanowisko poszanowania i ochrony wielostronnego modelu zarządzania Internetem (m.in. Europa i USA), a z drugiej strony te, które opowiadają się za zwiększeniem zakresu kontroli i wpływu rządów na Internet[103].

94 *Tallinn Manual 2.0 on the International Law application to Cyber Operations;* Międzynarodowa Grupa Ekspertów, Cambridge University Press, Cambridge 2017, s. 12-13.
95 Ibidem, s. 15.
96 Ibidem, s. 16.
97 Ibidem, s. 16.
98 Ibidem, s. 19
99 *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* Grupa została powołana po raz pierwszy w 2003 roku, a w latach 2003-2020 obradowało łącznie szczęść takich grup. Więcej informacji na temat grupy i jej pracy dostępnych jest na stronie: https://cyberpolicy.nask.pl/un-gge-prawo-miedzynarodowe-w-cyberprzestrzeni/
100 Warto zaznaczyć, że w grupie tej zasiadły państwa prezentujące zupełnie odmienną optykę w kwestii zarządzania Internetem. Dlatego wypracowany konsensus był wielkim przełomem.
101 Czytaj więcej o szóstej grupie GGE na s. 49
102 Czytaj więcej o grupie OEWG na s. 50
103 W 2019 roku Rosja wprowadziła ustawę o tzw. suwerennym Internecie w Rosji. Nowe prawo pozwala na izolowanie Runetu od globalnej sieci. Uzasadniane jest to zagrożeniem dla bezpieczeństwa cybernetycznego państwa, w tym ryzykiem odłączenia Rosji od zagranicznych serwerów ze strony państw trzecich, przede wszystkim USA; https://www.osw.waw.pl/pl/publikacje/analizy/2019-03-13/rosja-zaostrzanie-cenzury-w-internecie

Zarządzanie Internenetem

Zgodnie z definicją WSIS *(World Summit on the Information Society)* zaproponowaną w 2005 roku, zarzadzanie Internetem to **opracowywanie i stosowanie przez rządy, sektor prywatny i społeczeństwo obywatelskie, w ich odpowiednich rolach, wspólnych zasad, norm, procedur decyzyjnych i programów kształtujących rozwój i korzystanie z Internetu.**

Historycznie, za proces przyznawania domen internetowych oraz ogólny nadzór nad działaniem serwerów DNS na całym świecie odpowiadał rząd USA. W 1998 roku utworzony został ICANN (*The Internet Corporation for Assigned Names and Numbers* – Internetowa Korporacja ds. Nadanych Nazw i Numerów), prywatna organizacja non-profit, której rząd USA przekazał nadzór nad technicznymi aspektami Internetu. ICANN ma jednak status firmy zarejestrowanej w stanie Kalifornia, a więc podlega jurysdykcji rządu USA. Przejął rolę IANA *(Internet Assigned Numbers Authority)*, zajmującej się zarządzaniem globalnym systemem nazw domen[104]. Wraz ze wzrostem znaczenia Internetu, amerykańska dominacja w zakresie zarządzania Internetem była krytykowana przez wiele państw (m.in. Brazylia, Chiny, kraje arabskie)[105].

Dyskusja, która od wielu lat toczy się na poziomie ONZ i która powoduje impas w obradach grupy GGE, udowadnia, że zagadnienie cyfrowej suwerenności może być wykorzystywane do tzw. bałkanizacji Internetu[106]. W efekcie nie będziemy już mówić o Internecie – globalnej sieci łączącej wszystkich użytkowników, ale o „internetach", a więc sieciach funkcjonujących pod auspicjami poszczególnych rządów. Jest to już częściowo widoczne w polityce Chin i Rosji, jak również w przypadku dużych międzynarodowych platform, które udostępniają użytkownikom sieci różne treści, w zależności od adresu IP. Cyfrowa suwerenność stwarza więc wyzwanie dla funkcjonowania Internetu jako takiego. **Dla państw takich jak USA, Rosja czy Chiny wyzwania związane z zarządzaniem Internetem oraz implementacją międzynarodowego prawa w cyberprzestrzeni, stanowią element geopolityki.** Coraz większe uzależnienie państw od cyberprzestrzeni powoduje chęć zaznaczenia swojej dominacji w tym obszarze. Stanowi to zagrożenie dla neutralności sieci[107], a więc zasady, w myśl której ani dostawcy usług internetowych, ani rządy nie nakładają żadnych ograniczeń dostępu do sieci.

104 Historycznie rolę tą pełnił UCLA *(University of California at Los Angeles)*, pod nadzorem Departamentu Obrony USA. Jednak w 1998, po śmierci Jona Postela, który zajmował się zarządzaniem IANA, rola ta została przypisana ICANN.
105 *Internet Governance* [w:] J. Chipman, E. Tikk-Ringres, *Evolution of the cyber domain: the implication for National and Global Security,* The International Institute for Strategic Studies, 20015.
106 Bałkanizacja Internetu jest rozumiana jako stopniowe odchodzenie od światowej sieci na rzecz internetów krajowych, w których to państwa narodowe będą kontrolować sieć, w zależności od własnej polityki i zgodnie z własną technologią.
107 *Internet Governance* [w:] J. Chipman, E. Tikk-Ringres, *Evolution of the cyber domain: the implication for National and Global Security,* The International Institute for Strategic Studies, 20015.

Dane, czyli ropa XXI wieku

Od czasów tzw. afery *WikiLeaks*[108] i Edwarda Snowdena[109] dane traktowane były z coraz większą uważnością. Nie tylko przez pojedyncze państwa, ale także przez społeczność międzynarodową. W 2017 roku „The Economist" opublikował artykuł zatytułowany: Najcenniejszym surowcem świata nie jest już ropa, ale dane *(The world's most valuable resource is no longer oil, but data)*[110]. Dane określono w nim mianem „ropy naftowej ery cyfrowej" *(the oil of the digital era)*. Zapanowało przekonanie, że dane są podstawą władzy i wiedzy w XXI wieku. Gospodarka oparta na danych miała stanowić przyszłość, a w dobie społeczeństwa informacyjnego[111], to właśnie dane miały decydować o sile politycznej poszczególnych państw.

Afery *WikiLeaks* i Snowdena zdawały się to potwierdzać. Okazało się, że pewnego rodzaju „kolekcjonowanie" informacji na temat obywateli, sojuszników i oponentów, to domena mocarstw, które dzięki wykorzystaniu nowoczesnej technologii są w tym niezwykle skuteczne. Na odpowiedź Europy nie trzeba było długo czekać. Unia Europejska wprowadziła nowe regulacje w dwóch wymiarach: **ochrony danych osobnych i nieosobowych.** Było to połączone z dyskusją na temat roli GAFA w przetwarzaniu danych osobowych i nieosobowych Europejczyków. Danych, które w tym przypadku stały się walutą służącą do opłacania darmowych usług.

108 W 2010 roku portal WikiLeaks opublikował dokumenty wojskowe dotyczące wojny w Afganistanie i Iraku, pokazujące fakty nie znane dotąd opinii publicznej i realne straty po stronie cywilnej, a także depesze dyplomatyczne z amerykańskich ambasad na całym świecie. Po tych publikacjach strona WikiLeaks została zablokowana za pomocą ataku DoS.

109 W 2013 roku, na łamach prasy brytyjskiej („The Guardian") Edward Joseph Snowden ujawnił m.in. inwigilację obywateli USA przez Agencję Bezpieczeństwa Krajowego (NSA) oraz instytucji Unii Europejskiej i ponad 30 czołowych polityków na świecie.

110 Artykuł został opublikowany 6 maja 2017. Autorem stwierdzenia wykorzystanego przez „The Economist" jest matematyk Clive Humbly, który w 2006 roku, stwierdził, że „dane to nowa ropa", ponieważ „nieratyfikowane nie mogą być używane". Konieczna jest analiza, tak aby były użyteczne, podobnie jak w przypadku ropy, z której powstaje np. benzyna, i która jest użyteczna dla gospodarki.

111 Społeczeństwo, dla którego nadrzędną wartością jest informacja.

W kwietniu 2016 roku przyjęto **RODO** *(Rozporządzenie Ogólne o Ochronie Danych Osobowych)*, które obowiązuje od 25 maja 2018 roku[112]. Rozporządzenie jest pewnego rodzaju rewolucją w podejściu do ochrony danych osobowych w Europie i na świecie, ponieważ do jego stosowania są zobowiązane także podmioty spoza UE, świadczące usługi na terytorium państw członkowskich. Najważniejsze zmiany dotyczą:

- Wprowadzenia nowych uprawnień dla osób, których dane dotyczą (prawo do przenoszenia danych oraz prawo do bycia zapomnianym).
- Rozszerzenia obowiązku informacyjnego (administrator danych ma obwiązek informować o ich przetwarzaniu osoby, których dane te dotyczą).
- Uregulowania kwestii profilowania (decyzje nie są już opierane tylko na algorytmie, ale osoba, której dane dotyczą może żądać ludzkiej interwencji).
- Wprowadzenia podejścia polegającego na ochronie danych osobowych już w fazie projektowania *(privacy dy design)* i jako ustawienie domyślne *(privacy by default)*.

RODO wzmacnia kontrolę nad przetwarzaniem danych osobowych obywateli UE i zapewnia wyższy poziom bezpieczeństwa. Także poprzez wprowadzenie administracyjnych kar finansowych za nieprzestrzeganie przepisów (od 10 do 20 mln euro lub 2-4 % całkowitego rocznego światowego obrotu firmy).

Drugim aktem prawnym w zakresie ochrony danych osobowych jest, wciąż procedowane na forum UE[113], ePrivacy *(Rozporządzenie w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej)*. Projekt rozporządzenia przedstawiono w styczniu 2017 roku. Regulacja miała wejść w życie razem z RODO i została zaprojektowana jako *lex specialis* w zakresie prywatności w Internecie. Rozporządzenie ePrivacy obejmuje dostawców usług telekomunikacyjnych, dostawców Internetu oraz podmioty typu: Facebook, Messenger, Skype, Gmail, WhatsApp czy Viber. Ma także zastosowanie do komunikatów przesyłanych w trybie maszyna-maszyna (Internet Rzeczy) i danych pochodzących z publicznych i półprywatnych sieci łączności (hotspoty).

Najważniejszą zmianą wprowadzoną przez ePrivacy jest rozszerzenie definicji danych pochodzących z łączności elektronicznej. Włączono do niej nie tyko przesyłane treści, ale także informacje o użytkownikach końcowych, dane służące do śledzenia i identyfikowania źródła, miejsca łączności, lokalizacja geograficzna, data, godzina, czas trwania i rodzaj łączności. Zgodnie z projektem dane te mają być traktowane jako poufne, a ingerencja przez osoby inne niż użytkownicy końcowi została zakazana. Bezpośrednim skutkiem takiego podejścia jest uznanie plików *cookie*[114] za sferę prywatną, podlegającą ochronie, a także wprowadzenie prawa do kontrolowania łączności elektronicznej przez użytkowników, poprzez możliwość decydowania o identyfikacji rozmów przychodzących i wychodzących. Ochroną objęte zostały również metadane, dostarczające informacji na temat lokalizacji, historii przeglądarki czy godziny połączenia i czasu wysłania wiadomości. Projekt ePrivacy znacznie wzmacnia więc pozycję użytkowników w Internecie, poprzez możliwość decydowania o zakresie i celu gromadzenia danych na ich temat.

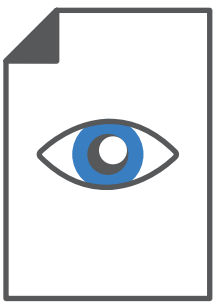
112 Rozporządzenie zastąpiło Dyrektywę 95/46/WE z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.
113 Impas w negocjacjach spowodowany jest dużą liczbą uwag o podłożu legislacyjnym zgłaszanych przez prawa członkowskie, a także silnym lobby przedstawicieli biznesu, którzy obawiają się, że ograniczenia w przetwarzaniu i wykorzystywaniu danych negatywnie wpłyną na rozwój innowacyjnych produktów i usług w UE.
114 Informacje przechowywane na urządzeniu końcowym użytkownika.

Obie regulacje wprowadzają **silną ochronę prywatności,** niespotykaną w żadnym innym reżimie prawnym, poza UE. W założeniu KE regulacje te miały zbudować zaufanie obywateli do nowoczesnych technologii i szerszego wykorzystywania Internetu. Jest to jeden z filarów Jednolitego Rynku Cyfrowego w Europie. U jego podstaw leży przekonanie, że Europejczycy muszą mieć gwarancję ochrony prywatności, tak aby bez obaw korzystali z Internetu, a tym samym przyczyniali się do budowy silnej gospodarki cyfrowej.

Równocześnie, w związku z rozwojem gospodarki cyfrowej, Komisja Europejska wprowadziła szereg regulacji w zakresie danych nieosobowych. KE określiła innowacje oparte na danych jako kluczowe dla wzrostu gospodarczego UE oraz powstawania nowych miejsc pracy. Komisja założyła, że wykorzystanie danych pozwoli uzyskać Unii Europejskiej przewagę konkurencyjną na globalnym rynku[115]. Jest to drugi z filarów Jednolitego Rynku Cyfrowego.

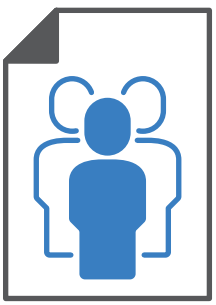
Pierwszym dokumentem strategicznym w tym zakresie był zaprezentowany w kwietniu 2018 roku Komunikat KE zatytułowany ***W kierunku wspólnej, europejskiej przestrzeni danych*** *(Towards a common European data space)*. W dokumencie tym dane zostały określone jako „surowiec Jednolitego Rynku Cyfrowego", który ma potencjał zrewolucjonizować życie i stworzyć możliwości rozwoju dla średnich przedsiębiorstw, których w UE jest najwięcej. Zoptymalizowanie wykorzystania danych zostało uznane jako kluczowe dla rozwoju Europy, także w kontekście nowych technologii takich jak Sztuczna Inteligencja i Internet Rzeczy. Komunikat definiuje trzy kategorie danych nieosobowych, w stosunku do których KE podjęła działania: **dane sektora publicznego** których ponowne wykorzystanie powinno być dozwolone; **dane naukowe,** które powinny być udostępniane szerzej, tak aby przyspieszać badania w konkretnych obszarach; **dane sektora prywatnego,** które stanowią o konkurencyjności europejskiej gospodarki i są udostępniane sektorowi publicznemu, co pozwala na ulepszanie usług publicznych.

Trzy kategorie danych nieosobowych zdefiniowane w Komunikacie *W kierunku wspólnej, europejskiej przestrzeni danych*



Dane publiczne

Dane naukowe

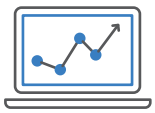


Dane sektora publicznego

115 Communication Towards a common European data space, Bruksela, 25.04.2018, s. 2

Razem z komunikatem KE przedstawiła jeszcze dwa dokumenty: *Wytyczne na temat dzielenia się danymi z sektora prywatnego* oraz *Zalecenia dotyczące dostępu do informacji naukowych i ich ochrony.* Dokumenty te dotyczą **dzielenia się danymi miedzy firmami** z poszanowaniem 4 zasad:

Przejrzystość: wyznaczenie osób i podmiotów, które będą miały dostęp do danych generowanych przez produkt lub usługę; określenie rodzaju danych, poziomu ich szczegółowości oraz celów, do których dane zostaną wykorzystane



Wspólnie tworzona wartość: uwzględnienie faktu, że czasem dane powstają jako efekt uboczny korzystania z urządzenia, a do ich powstania przyczynia się kilka stron

Szacunek dla interesów innych firm: odpowiednia ochrona interesów i tajemnic handlowych wszystkich firm zaangażowanych we współpracę

Ochrona konkurencji: uwzględnienie prawa do prowadzenia uczciwej konkurencji przez wszystkie zaangażowane podmioty

Dokumenty opisują również **wymianę danych w formule B2B** *(business to business)*, która może odbywać się w trzech formatach: otwartej wymiany danych; udostępnienia danych za wynagrodzeniem oraz na tzw. rynku danych, czyli platformie, która pozwala firmom anonimowo wymieniać potrzebne informacje.

W zakresie **dostępu do danych naukowych,** KE zaznaczyła, że jest on konieczny do stworzenia wspólnej przestrzeni do wymiany danych w Europie i szybszego rozwoju badań. Określono cztery zalecenia dostępu do informacji naukowych i ich ochrony:

- **Otwarty dostęp do publikacji naukowych i wyników badań naukowych –** Państwa członkowskie powinny zapewnić otwarty dostęp do publikacji i badań naukowych finansowanych ze środków publicznych. KE zakłada, że dane te powinny być ogólnodostępne najpóźniej do końca 2020 roku.
- **Współpraca z instytucjami naukowymi –** Wdrażanie rekomendacji przez państwa członkowskie powinno się odbyć przy współpracy z instytucjami badawczymi, odpowiadającymi za zarządzanie środkami publicznymi, a także z instytucjami akademickimi, które otrzymują te środki.
- **Umiejętności i kompetencje –** Niezbędne jest zapewnienie szkoleń z otwartego dostępu do danych, zarządzania nimi, ich ochrony i obsługi. Szkolenia powinny być dostępne na każdym szczeblu kariery naukowej i w szkolnictwie wyższym, a także wszędzie tam, gdzie taka praktyka może być niezbędna.

- **Dialog międzynarodowy –** Państwa członkowskie powinny być zaangażowane w dialog międzynarodowy dotyczący otwartego dostępu do nauki na poziomie krajowym, europejskim i globalnym.

W listopadzie 2018 roku przyjęte zostało także ***Rozporządzenie w sprawie ram swobodnego przepływu danych nieosobowych.*** Założeniem leżącym u podstaw tego dokumentu było przekonanie, że aby w pełni wykorzystać zalety gospodarki opartej na danych, konieczne jest zapewnienie swobodnego ich przepływu. Dzięki temu zarówno firmy, jak i organy administracji publicznej, będą miały możliwość przechowywania i przetwarzanie danych nieosobowych w dowolnym miejscu w UE. Rozporządzenie zakłada:

Swobodny przepływ danych nieosobowych przez granice: każda organizacja powinna mieć możliwość przechowywania i przetwarzania danych w dowolnym miejscu w Unii Europejskiej

Dostępność danych do celów kontroli regulacyjnej: organy publiczne zachowają dostęp do danych, także gdy są one zlokalizowane w innym państwie członkowskim lub są przechowywane lub przetwarzane w chmurze

Kolejny etap stanowiło wydanie w maju 2019 roku ***Wytycznych na temat przepływu danych osobowych i nieosobowych w UE.*** Celem dokumentu było ułatwienie małym i średnim przedsiębiorstwom zrozumienia powiązań pomiędzy *Rozporządzeniem o ochronie danych osobowych*, a *Rozporządzeniem w sprawie swobodnego przepływu danych nieosobowych.*

Bardzo ważnym krokiem w budowaniu europejskiej polityki w zakresie danych nieosobowych było przyjęcie w czerwcu 2019 roku ***Dyrektywy w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego*** zastępującej tzw. Dyrektywę reuse *(Dyrektywa w sprawie ponownego wykorzystania informacji sektora publicznego z 2003 roku).* Dyrektywa koncentruje się na ekonomicznych aspektach ponownego wykorzystywania informacji. Zachęca państwa członkowskie do udostępniania jak największej ilości informacji do ponownego wykorzystania. Przepisy odnoszą się do materiałów przechowywanych przez organy sektora publicznego w państwach członkowskich na szczeblu krajowym, regionalnym i lokalnym (ministerstwa, agencje państwowe i gminy, a także organizacje finansowane głównie przez organy publiczne lub będące pod ich kontrolą (np. Instytuty meteorologiczne)).

Dane osobowe i nieosobowe w UE - strategia i regulacje

Dane osobowe

27 kwietnia 2016

Przyjęcie RODO

10 stycznia 2017

Propozycja ePrivacy

28 maja 2018

Wejście w życie RODO

Dane nieosobowe

25 kwietnia 2018

- Komunikat KE *W kierunku wspólnej, europejskiej przestrzeni danych*
- *Wytyczne na temat dzielenia się danymi z sektora prywatnego*
- *Zalecenia dotyczące dostępu do informacji naukowych*

14 listopada 2018

Rozporządzenie w sprawie ram swobodnego przepływu danych nieosobowych

29 maja 2019 roku

Wytyczne na temat przepływu danych osobowych i nieosobowych w UE

20 czerwca 2019

Dyrektywa w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego

Na przestrzeni ostatnich lat Unia Europejska podejmowała więc bardzo wiele działań, w których centrum znajdowały się dane – zarówno osobowe, jak i nieosobowe. Przekonanie o tym, że europejskie dane należy chronić, a przy tym wykorzystać je do rozwoju nowoczesnych technologii (m.in. Sztuczna Inteligencja, Internet Rzeczy), podyktowane było chęcią konkurowania z takimi państwami jak USA czy Chiny, oraz przeciwstawienia się dominacji GAFA. Równocześnie rosła jednak rola technologii, która ostatecznie, w kontekście cyfrowej suwerenności, stała się wiodącym tematem w 2019 roku.

A jednak technologia? – zmiana paradygmatu

Kiedy w 2013 roku Komisja Europejska opublikowała pierwszą *Strategię Cyberbezpieczeństwa,* polityka cyberbezpieczeństwa w Europie kontentowała się na aspektach cywilnych. Cyberbezpieczeństwo rozumiane było jako ważny element rewolucji cyfrowej. KE argumentowała, że zarówno wolność, jak i dobrobyt obywateli UE, zależy od technologii informacyjno – komunikacyjnych, które stanowią „fundament wzrostu gospodarczego i są zasobem o krytycznym znaczeniu, na których opierają się wszystkie sektory gospodarki”[116]. Jako cele działań KE zdefiniowała:

Osiągnięcie odporności na zagrożenia cybernetyczne

Radykalne ograniczenie cyberprzestępczości

Opracowanie polityki obronnej i rozbudowa zdolności bezpieczeństwa cybernetycznego w powiązaniu ze Wspólną Polityką Bezpieczeństwa i Obrony UE

Rozbudowa zasobów przemysłowych i technologicznych na potrzeby bezpieczeństwa cyberprzestrzeni

Ustanowienie spójnej międzynarodowej polityki w zakresie cyberprzestrzeni dla Unii Europejskiej i promowanie podstawowych wartości UE

Mimo tego, że główną oś dokumentu stanowią kwestie współpracy transgranicznej, współpracy międzysektorowej, wymiany informacji o zagrożeniach oraz dobrych praktyk, a także koordynacji działań na poziomie UE, to jednak wyraźnie zaznaczone zostały też kwestie technologiczne. W części dotyczącej **rozbudowy zasobów przemysłowych,** KE wyraźnie zaznaczyła, że **„istnieje ryzyko, że Europa staje się nadmiernie uzależniona nie tylko od ICT pochodzących z zewnątrz, ale również rozwiązań w zakresie cyberbezpieczeństwa, opracowanych poza jej granicami. Należy zagwarantować, aby elementy sprzętu i oprogramowania produkowane w UE oraz w państwach trzecich, które są stosowane w kluczowych usługach i w kluczowej infrastrukturze oraz w coraz większym stopniu**

116 *Strategia bezpieczeństwa cybernetycznego UE: otwarta, bezpieczna i chroniona cyberprzestrzeń,* 7 lutego 2013, s. 1.

w urządzeniach przenośnych, były wiarygodne i bezpieczne oraz aby gwarantowały ochronę danych osobowych"[117]**.**

Razem ze *Strategią,* KE przedstawiła propozycję pierwszego ogólnoeuropejskiego prawa w zakresie cyberbezpieczeństwa w UE **– Dyrektywy NIS.** Po trzech latach negocjacji, w lipcu 2016 roku, dyrektywa została przyjęta. Nowe prawo wprowadziło obowiązkowe zgłaszanie incydentów dla operatorów usług kluczowych (podmioty sektora prywatnego lub publicznego, dostarczające usług kluczowych w sektorach energetyki, transportu, bankowości i infrastruktury rynków finansowych, zdrowia, zaopatrzenia w wodę oraz infrastruktury cyfrowej), a także uzależnienie poziomu zabezpieczeń od szacowania ryzyka oraz wprowadzenia narodowej strategii cyberbezpieczeństwa. Wart odnotowania jest fakt, że **dyrektywa NIS reguluje bezpieczeństwo sieci i systemów teleinformatycznych, a więc kwestie technologiczne.** Weszła w życie 25 maja 2018, czyli prawie równocześnie z RODO. Ogólny dyskurs zdominowały jednak przepisy związane z ochroną danych osobowych. Rozporządzenie spotkało się z dużo większym zainteresowaniem, zarówno ze strony sektora prywatnego, jak i opinii publicznej[118]. Niemniej jednak **oba akty prawne zaczęły obowiązywać właściwie jednocześnie i w pewien sposób są regulacjami komplementarnymi – ich zadaniem jest budowa bezpieczeństwa na Jednolitym Rynku Cyfrowym.**

Niedługo przed przyjęciem dyrektywy NIS, w lipcu 2016 roku, Komisja przedstawiła **Komunikat *Wzmacnianie europejskiego systemu odporności cybernetycznej oraz wspieranie konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego,*** stanowiący aktualizacje *Strategii* z 2013 roku. Dokument koncentrował się na współpracy pomiędzy państwami członkowskimi w przypadku incydentów na dużą skalę, oraz zapowiedział wprowadzenie europejskiej certyfikacji produktów i usług. Ważnym wyzwaniem zaadresowanym w *Komunikacie* była także **konieczność budowy europejskiego sektora cyberbezpieczeństwa.** W tym celu, powołano kontraktowe partnerstwo publiczno – prywatne, którego celem była integracja sektora i wspieranie jego działań. Projekt ten nie odniósł jednak sukcesu, ponieważ w skład partnerstwa weszły firmy pozaeuropejskie[119]. Warto podkreślić, że *Komunikat* zbliżał także kwestie cywilnego i wojskowego cyberbezpieczeństwa, postulując synergię działań.

Operacjonalizacją działań zapowiedzianych w *Komunikacie*, było przedstawienie przez KE, tzw. **Pakietu cyberbezpieczeństwa,** we wrześniu 2017 roku. W skład pakietu weszły następujące dokumenty:

- Komunikat *Odporność, Odstraszanie, Obrona: Budując silne cyberbezpieczeństwo dla Unii Europejskiej* – kolejna aktualizacja strategii KE[120].
- Propozycja Aktu Cyberbezpieczeństwa dot. mandatu ENISA i certyfikacji na poziomie europejskim.
- Zalecenia Komisji w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę (tzw. *Blueprint*)[121] Komunikat Komisji dot. implementacji Dyrektywy NIS

Pakiet o wiele silniej, niż dotychczasowe dokumenty i regulacje UE **akcentował kwestie związane z bezpieczeństwem technologicznym.** W Komunikacie ***Odporność, Odstraszanie,***

117 *Strategia bezpieczeństwa cybernetycznego UE: otwarta, bezpieczna i chroniona cyberprzestrzeń,* 7 lutego 2013, s. 27.
118 W dużej mierze, była to zasługa wysokich kar, wyprowadzonych w RODO, których brak w Dyrektywie NIS
119 Więcej informacji na stronie ECSO (European Cyber Security Organization) https://ecs-org.eu/
120 Czytaj więcej na stronie: https://cyberpolicy.nask.pl/odpornosc-prewencja-i-obrona-budowa-solidnego-bezpieczenstwa-cybernetycznego-unii-europejskiej/

Obrona: Budując silne cyberbezpieczeństwo dla Unii Europejskiej jest mowa o **zwiększeniu zdolności technologicznych Europy w zakresie cyberbezpieczeństwa.** *Akt o Cyberbezpieczeństwa (Cybersecurity Act – CA)* wprowadza natomiast certyfikację produktów i usług ICT[122].

Przyjęcie *Aktu o Cyberbezpieczeństwie*, w kwietniu 2019, sprawiło że kwestie technologiczne, do tej pory „przyćmiewane" w ogólnym dyskursie na temat cyberbezpieczeństwa przez tematykę związaną z danymi, znalazły się na pierwszym planie. CA to pierwsze prawo dotyczące rynku wewnętrznego, które odpowiada na potrzebę podniesienia poziomu bezpieczeństwa produktów, usług i procesów ICT. Zgodnie z założeniami przyświecającymi tym rozwiązaniom prawnym, konsument będzie mógł wybierać takie urządzenia i rozwiązania, które są przetestowane i spełniają odpowiednie normy bezpieczeństwa. Firmy natomiast będą musiały ubiegać się o certyfikat tylko w jednym kraju członkowskim i będzie on honowany na obszarze całej UE. Ma to oczywiście wspierać rozwój Jednolitego Runku Cyfrowego i sprzyjać podnoszeniu poziomu bezpieczeństwa, a także budowie przewagi technologicznej firm europejskich. Jednak przyjęciu *Aktu* towarzyszyły liczne kontrowersje. Przede wszystkim, niewiele krajów budowało dotąd kompetencje w zakresie certyfikacji (m.in. Francja, Niemcy, Hiszpania). Dla wielu, zbudowanie struktur pozwalających na realizowanie nowego prawa[123] stanowi duże wyzwanie. Jest to kosztowne i długotrwałe. W pierwszym etapie, wiele państw z pewnością będzie musiało korzystać z laboratoriów znajdujących się poza granicami kraju. Dodatkowo, kraje które już osiągnęły pewien poziom w certyfikacji, obawiają się że nowopowstałe instytucje ds. certyfikacji w innych państwach nie będą spełniały właściwych standardów, a jednak konieczne będzie honorowanie wydawanych przez nie certyfikatów. W dyskusji na poziomie UE, coraz silniej artykułowane są także kwestie suwerenności i konieczności zapewnienia właściwego poziomu cyberbezpieczeństwa produktów ICT. Założenie, że aby móc być dopuszczonymi do użytku, produkty i usługi spoza UE, będą musiały mieć europejski certyfikat, ma być elementem budującym europejską suwerenność cyfrową. Nawet jeśli poszczególne państwa wciąż mają wątpliwości w kwestii poziomu usług certyfikacyjnych, wydawanych w innych państwach, to przynajmniej będą to certyfikaty europejskie. Przy okazji tej dyskusji jasne stało się, że w porównaniu do roku 2017, czy 2018, temat bezpieczeństwa danych nie jest już najistotniejszy. **W 2019, w dyskursie politycznym dominowało bezpieczeństwo technologii.**

121 Czytaj więcej na stronie: https://cyberpolicy.nask.pl/blueprint-zarzadzanie-kryzysowe-w-obliczu-incydentow-cybernetycznych-na-duza-skale/
122 Czytaj więcej na temat CA na stronie: https://cyberpolicy.nask.pl/akt-o-cyberbepzieczenstwie-certyfikacja-cyberbezpieczenstwa/
123 Aby przeprowadzić proces certyfikacji konieczne jest funkcjonowanie w PCz Krajowego organu ds. certyfikacji cyberbezpieczeństwa (KOCC), Krajowej jednostki akredytującej oraz Jednostek oceniających zgodność.

Strategia i regulacje w zakresie cyberbezpieczeństwa w UE

7 lutego 2013

Strategia bezpieczeństwa cybernetycznego UE: otwarta, bezpieczna i chroniona cyberprzestrzeń

5 lipca 2016

Komunikat *Wzmacnianie europejskiego systemu odporności cybernetycznej oraz wspieranie konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego*

6 lipca 2016

Przyjęcie Dyrektywy NIS

13 września 2017

Pakiet Cyberbezpieczeństwa:

- Komunikat *Odporność, Odstraszanie, Obrona: Budując silne cyberbezpieczeństwo dla Unii Europejskiej* – kolejna aktualizacja strategii KE
- Propozycja Aktu Cyberbezpieczeństwa dot. mandatu ENISA i certyfikacji na poziomie europejskim.
- Zalecenia Komisji w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę (tzw. *Blueprint*)
- Komunikat Komisji dot. implementacji Dyrektywy NIS

17 kwietnia 2019

Przyjęcie *Aktu o Cyberbezpieczeństwie*

Jeszcze jeden temat 2019 roku bardzo silnie wpłynął na dyskusję o cyfrowej suwerenności i uwypuklił zmianę paradygmatu: **bezpieczeństwo sieci 5G.** UE koncentrowała się na zapewnieniu właściwego poziomu bezpieczeństwa sieci nowej generacji. W marcu KE przedstawiła rekomendacje dotyczące cyberbezpieczeństwa sieci 5G, a w październiku unijną skoordynowaną ocenę ryzyka związanego z cyberbezpieczeństwem w sieciach piątej generacji[124]. Działania te przebiegały równolegle z ogólnoświatową dyskusją na temat dostawców usług. USA oskarżyło chińską firmę Huawei o niejawne związki z chińskim rządem. Najpierw, w sierpniu 2018 roku, administracja amerykańska zakazała wykorzystywania sprzętu Huawei pracownikom rządu federalnego. Potem, w maju 2019 roku, Departament Handlu wprowadził chińską firmę na listę firm podlegających *Export Administration Regulation,* w wyniku czego amerykańskie firmy nie mogą prowadzić interesów z Huawei bez licencji rządowej. USA prowadziło także bardzo silną międzynarodową kampanię zmierzającą do tego, żeby urządzenia chińskiej firmy nie były wykorzystywane we wdrażaniu technologii 5G.

W tej dyskusji chodzi jednak przede wszystkim o potężne interesy ekonomiczne. Okazało się, że w najbliższych latach to nie kontrola nad danymi będzie przynosić znaczne zyski finansowe. Będzie to dostarczanie sprzętu, który zostanie wykorzystany w sieciach nowej generacji. Spór toczy się więc o to, skąd będzie pochodzić ta technologia i kto na tym zarobi.

Podsumowanie

Przez wiele lat dyskurs na temat bezpieczeństwa w Europie był zdominowany przez kwestie ochrony i bezpieczeństwa danych. Było to związane z wydarzeniami geopolitycznymi takimi tak afera *WikiLeaks* i publikacje Edwarda Snowdena. Panowało szerokie przekonanie, że to dane, zwane „ropą XXI wieku", są największym dobrem o które konkurują między sobą nie tylko poszczególne państwa, ale także organizacje międzynarodowe. UE zapewniła szczególne regulacje w zakresie danych osobowych i nieosobowych, zmuszając firmy spoza Europy do implementacji tych zapisów. Najbardziej znamiennym przykładem jest tutaj RODO i światowa wręcz dyskusja nad tą regulacją. Równolegle prowadzona była polityka w zakresie bezpieczeństwa technologii, która nie znajdowała tak dużego zrozumienia w szerszym dyskursie geopolitycznym. Wystarczy wspomnieć, że dyrektywa NIS weszła w życie właściwie równolegle z RODO, co zostało odnotowane z dużo mniejszymi emocjami i zainteresowaniem. Sytuacja uległa zmianie w 2019 roku. Po przyjęciu *Aktu o Cyberbezpieczeństwa* i dyskusji na temat wdrażania technologii 5G, kwestie technologiczne wysunęły się na pierwszy plan, w pewien sposób detronizując tematykę związaną z bezpieczeństwem danych. Ta zmiana paradygmatu jest silnie powiązana z dyskusją na temat cyfrowej suwerenności. Coraz wyraźniej wybrzmiewają argumenty na temat konieczności tworzenia rozwiązań technologicznych w Europie i uniezależnienia się od firm pozaeuropejskich. Temat ten został silnie zaakcentowany przez przewodniczącą Komisji Europejskiej, Ursulę von der Leyen, kiedy na początku 2020 roku prezentowała *Europejską strategię transformacji cyfrowej UE*.

Wydaje się, przy tym że suwerenność cyfrowa jest obecnie rozumiana na trzech różnych poziomach: strategicznym, prawnym oraz technologicznym. W wymiarze strategicznym jest bezpośrednio związana z toczącą się od lat międzynarodową dyskusją na temat zarządzania Internetem, oraz dopuszczaniem dostawców do tworzenia rozwiązań w zakresie 5G. W wymiarze prawnym, dotyczy zastosowania prawa międzynarodowego w cyberprzestrzeni, a w wymiarze technologicznym – bezpieczeństwa i zaufania do tworzonych rozwiązań.

5G

SIEĆ NOWEJ GENERACJI JAKO WYZWANIE TECHNOLOGICZNE I POLITYCZNE

– Rafał Babraj –

Trwająca rewolucja cyfrowa zmienia sposób w jaki funkcjonujemy. Nasze mieszkania powoli stają się *smart home*: odkurzacze uczą się rozkładów pomieszczeń, roboty kuchenne pobierają z sieci nowe przepisy, lodówki same mogą robić zakupy, a pralki prowadzą samodzielną diagnozę pod kątem ewentualnych usterek. Smartfony, które do niedawna były w domu jednym z niewielu urządzeń podłączonych do Internetu, teraz przejmują rolę pilota, którym kontrolować można cały szereg innych inteligentnych urządzeń. A tych, według różnych szacunków, w 2020 roku do sieci podłączonych może być nawet ponad 20 mld[125].

Smartfon często zastępuje nam również telewizję czy radio. Po filmy, muzykę lub książki sięgamy za pośrednictwem platform internetowych. Zakupy przez Internet? To już codzienność. Rozwój rynku gier komputerowych doprowadził do narodzin e-sportu, który stał się niezwykle dochodowym biznesem[126]. Ogromne zmiany przechodzi cały przemysł. Postępująca robotyzacja, automatyzacja procesów produkcyjnych, wykorzystywanie algorytmów uczenia maszynowego do usprawnienia zarządzania – to tylko niektóre aspekty Przemysłu 4.0[127].

To wszystko sprawia, że ilość transmitowanych danych wzrasta w ogromnym tempie. Instytut Łączności PIB przewiduje, że w ciągu najbliższych 2-3 lat obecna konfiguracja sieci nie będzie w stanie obsłużyć prognozowanego ruchu[128]. Również wyniki badań firm Ericsson (2018) i Cisco (2017), wskazują, że co roku ilość danych transmitowanych przez sieci komórkowe wzrasta o 50-60 proc[129].

Nie może więc dziwić, że sieć 5G była jednym z najważniejszych tematów w 2019 roku. Będzie ona miała kluczowe znaczenie dla cyfrowej transformacji gospodarki i społeczeństwa, a z jej rozwojem wiązane są ogromne nadzieje.

Dlaczego potrzebujemy sieci 5G?

Wzrastający transfer danych

Coraz więcej urządzeń online

Nowe usługi multimedialne

Powszechna cyfryzacja usług

125 *Gartner Insights on How to Lead in a Connected World (Leading the IoT)* (https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf)
126 Według raportu *Global Esports Market Report 2020*, przychody z e-sportu na całym świecie wzrosną w 2020 roku do 1,1 mld dolarów, czyli o blisko 16% w porównaniu do 2019 roku.
127 Więcej informacji m.in. o Przemyśle 4.0 w raporcie *Krótka opowieść o społeczeństwie 5.0, czyli jak żyć i funkcjonować w dobie gospodarki 4.0 i sieci 5G* (https://www.digitalpoland.org/assets/publications/krotka-opowiesc-50/krotka-opowiesc-s50.pdf)
128 Analiza wykonalności wdrożenia usług w technologii 5G przy obecnych oraz zwiększonych normach dopuszczalnych poziomów promieniowania elektromagnetycznego (https://www.il-pib.pl/images/stories/raporty/pdf/PIIT/Raport-IL_-Zadanie-A-Analiza-wykonalnosci-wdrozenia-uslug-w-technologii-5G.pdf)
129 Oddziaływanie elektromagnetycznych fal milimetrowych na zdrowie pracowników projektowanych sieci 5G i populacji generalnej (http://www.imp.lodz.pl/upload/npz/raport_5g.pdf)

Jednak, aby można było w pełni wykorzystać potencjał 5G, należy zadbać m.in. o wysoki poziom cyberbezpieczeństwa sieci telekomunikacyjnych. Dlatego w Unii Europejskiej w 2019 roku trwały intensywne prace w tym zakresie, a państwa członkowskie, w tym Polska, prowadziły prace, mające umożliwić częściowe wdrożenie 5G już w 2020 roku.

Równocześnie sektor prywatny, gdy tylko pojawiły się odpowiednie standardy, rozpoczął testy, a w niektórych krajach – pierwsze wdrożenia komercyjne. Poniższa oś czasu przedstawia przegląd najważniejszych wydarzeń w 2019 roku związanych z tematyką 5G.

Marzec 2019

Komisja Europejska wydaje **rekomendacje dotyczące cyberbezpieczeństwa sieci 5G.**

Czerwiec 2019

Ministerstwo Cyfryzacji przygotowuje serwis internetowy o 5G oraz Białą Księgę *Pole elektromagnetyczne a człowiek*.

Lipiec 2019

Aktualizacja *Krajowego Planu Działań zmiany przeznaczenia pasma 700 MHz w Polsce*.

Sierpień 2019

ITU publikuje nowy standard, który stwarza podstawę efektywnej integracji uczenia maszynowego z siecią 5G.

Październik 2019

Przygotowanie **unijnej skoordynowanej oceny ryzyka** związanego z cyberbezpieczeństwem w sieciach 5G.

Październik 2019

NATO przyjmuje nowe wymagania dotyczące odporności cywilnej infrastruktury telekomunikacyjnej, w tym 5G.

Październik 2019

Wejście w życie *ustawy o zmianie ustawy o wspieraniu rozwoju usług i sieci telekomunikacyjnych oraz niektórych innych ustaw* (tzw. ***megaustawa***).

Październik 2019

Podpisanie memorandum w sprawie analizy modelu biznesowego dla spółki **#Polskie5G.**

Październik 2019

Wejście w życie nowelizacji *Rozporządzenia Rady Ministrów w sprawie Krajowej Tablicy Przeznaczeń Częstotliwości.*

Listopad 2019

World Radio Conference **(WRC-19)** – identyfikacja dodatkowych pasm częstotliwości powyżej 6 GHz dla usług 5G.

Listopad 2019

Publikacja ***ENISA threat landscape for 5G.***

Grudzień 2019

Minister Zdrowia publikuje ***Rozporządzenie w sprawie dopuszczalnych poziomów pól elektromagnetycznych w środowisku (PEM).***

Grudzień 2019

Urząd Komunikacji Elektronicznej rozpoczyna konsultacje w sprawie **rozdysponowania częstotliwości z pasma 3,6 GHz.**

Czym jest 5G – (r)ewolucja sieci

Z roku na rok podłączamy do sieci coraz więcej urządzeń. Tymczasem zasoby częstotliwości radiowych są ograniczone. Dlatego, aby efektywniej je wykorzystywać, należy rozwijać nowe technologie i szukać sposobów na zwiększenie pojemności sieci.

5G to już piąta, a zarazem najnowsza, generacja technologii mobilnej. Komisja Europejska zdefiniowała ją jako zbiór elementów infrastruktury sieciowej służących do mobilnej oraz bezprzewodowej komunikacji[130]. Będzie wykorzystywana w połączeniach i usługach, które wymagają:

- bardzo dużej szybkości transmisji danych i przepustowości,
- komunikacji o niskich opóźnieniach,
- bardzo wysokiej niezawodności,
- obsługi dużej liczby podłączonych urządzeń.

Ostatnie 40 lat, które minęły od wdrożenia telefonii komórkowej, przyniosły ogromny postęp. Pierwsza generacja telefonów komórkowych, czyli tzw. sieć 1G, umożliwiała jedynie połączenia głosowe z wykorzystaniem sygnału analogowego. Wdrożona w latach dziewięćdziesiątych ubiegłego wieku sieć 2G wprowadziła łączność cyfrową, a przy tym możliwość wysyłania np. wiadomości tekstowych. Sieć 3G pozwalała już na połączenia z Internetem, choć nie zapewniała jeszcze wystarczającej transmi-

130 *Commission Recommendation of 26 March 2019 on Cybersecurity of 5G networks* (https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks)

sji danych, aby móc w pełni wykorzystać jego możliwości[131]. Dopiero sieć 4G umożliwiła swobodne korzystanie z multimediów oraz usług online, takich jak streaming wideo, nawigacja czy *smart home*. Obecnie jesteśmy u progu wprowadzenia sieci 5G, która przyniesienie fundamentalną zmianę – z ery smartfonów przejdziemy do ery Internetu Rzeczy[132].

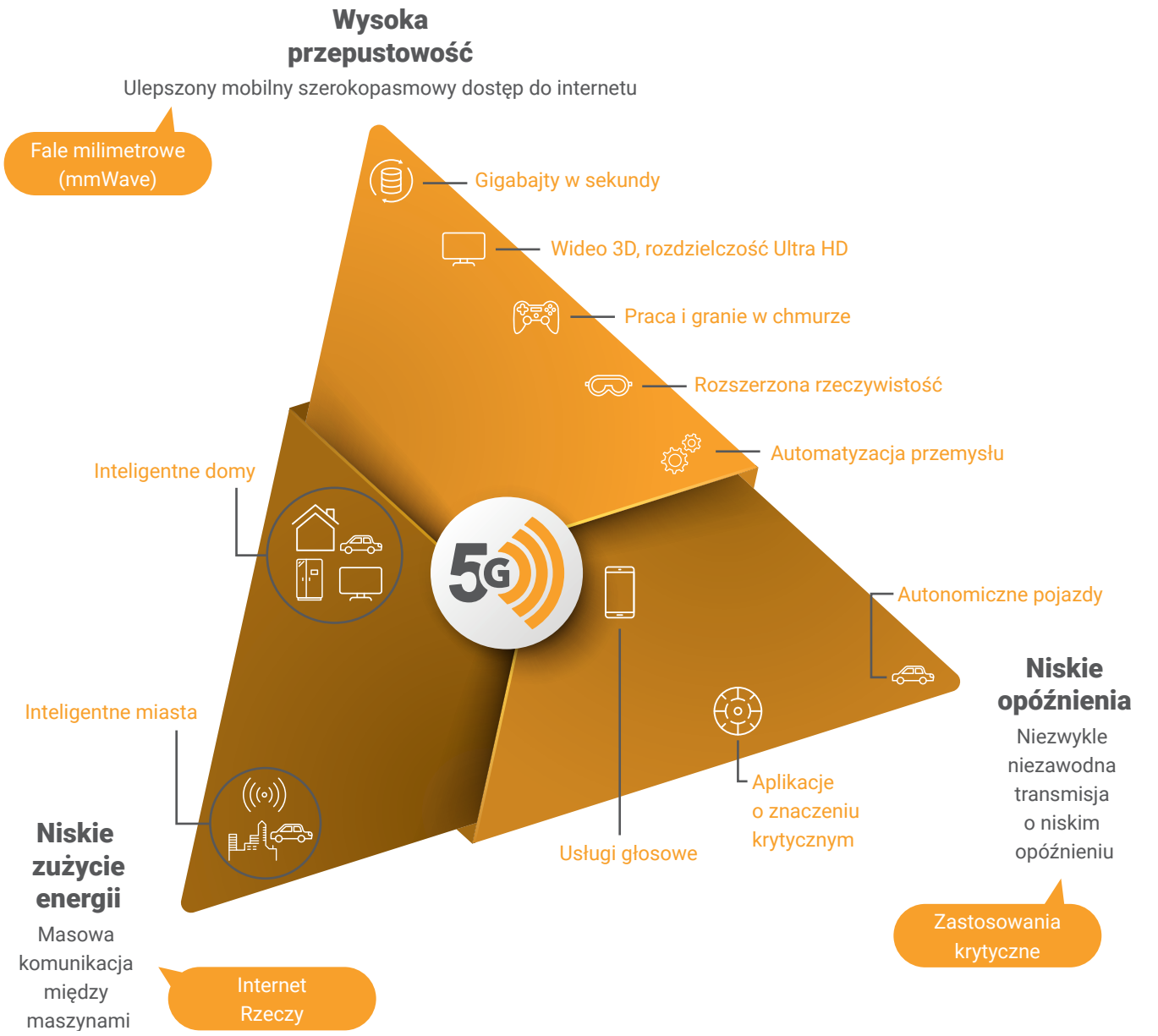
Porównanie standardów sieci komórkowej[133]:

Trzy filary 5G

Do czego będziemy wykorzystywać sieć nowej generacji? Trzy główne rodzaje usług, czyli tzw. scenariusze zastosowań dla 5G, określił Międzynarodowy Związek Telekomunikacyjny (ITU) w standardzie IMT-2020[134]. Będą to:

- **Ulepszony mobilny szerokopasmowy dostęp do internetu *(eMBB, enhanced Mobile Broadband)* –** bardzo szybka transmisja danych i przetwarzanie informacji w czasie niemal rzeczywistym. Wysokie szybkości transmisji będą osiągalne nawet przy większej liczbie użytkowników.
- **Masowa komunikacja między maszynami *(mMTC, massive Machine Type Communications)* –** umożliwi podłączenie, przy minimalnych opóźnieniach, blisko stukrotnie większej liczby urządzeń niż obecnie. Będzie to niezbędne przy rozwoju inteligentnych miast oraz Internetu Rzeczy.
- **Niezwykle niezawodna transmisja o niskim opóźnieniu *(URLLC, Ultra-Reliable Low Latency Communications)* –** minimalne opóźnienia umożliwią połączenia w czasie rzeczywistym, również w zastosowaniach krytycznych. Niezbędna m.in. w kwestiach bezpieczeństwa publicznego, rozwoju autonomicznych samochodów, telemedycyny czy automatyzacji przemysłu.

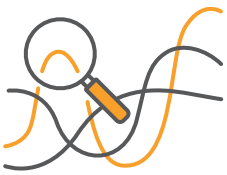
131 Przeglądanie stron www oraz wysyłanie e-maili było już możliwe od momentu pojawiania się 2,5G, czyli standardu GPRS/EDGE.
132 Internet Rzeczy *(Internet of Things)* to swoisty ekosystem, w którym urządzenia podłączone do sieci wymieniają dane, czyli komunikują się ze sobą – często bez udziału człowieka. Terminu „Internet Rzeczy" użył po raz pierwszy w 1999 roku brytyjski przedsiębiorca Kevin Ashton.
133 Przewodnik po 5G (https://www.gov.pl/web/5g/biala-ksiega1)
134 Standard IMT-2020 to wymagania przedstawione przez *ITU Radiocommunication Sector (ITU-R)* w 2015 r. dla sieci, urządzeń i usług 5G. Standard ma zostać ukończony w 2020 r. Częściowo został sfinalizowany wcześniej, na przykład w obszarze dotyczącym technologii dostępu radiowego *(5G New Radio)*. Czytaj więcej w nagłówku „Opracowanie standardów 5G".



(Źródło: Międzynarodowy Związek Telekomunikacyjny, ITU)

Czego potrzebujemy, aby wdrożyć sieć 5G?

Opracowania odpowiednich standardów



Identyfikacji nowych pasm częstotliwości

Zastosowania innowacyjnych rozwiązań technologicznych

Opracowanie standardów 5G

Standardy stanowią podstawę naszego funkcjonowania. Wsiadając do windy lub przejeżdżając przez most, ufamy że zostały one skonstruowane według określonych wytycznych, które zapewniają ich prawidłowe działanie. Standardy mogą się jednak różnić w zależności od kraju lub kontynentu. Widać to na przykładzie gniazdek elektrycznych. Inaczej będą wyglądać wtyczki w Polsce, inaczej w Stanach Zjednoczonych czy Australii. Co więcej, różne może być też napięcie w sieci elektrycznej.

Podobna sytuacja nie może mieć miejsca w przypadku sieci 5G. Smartfon powinien połączyć się bezprzewodowo z Internetem, bez względu na lokalizację i rodzaj urządzenia. Tymczasem dotychczas mogło się zdarzyć, że np. telefon importowany z innego kontynentu w prywatnej dystrybucji, nie obsługiwał częstotliwości, na której świadczone są usługi w UE.

Dlatego tak ważne jest opracowanie wspólnego standardu 5G. Pozwoli on m.in. zapewnić określony poziom wydajności nowej sieci (np. szybkość transmisji danych), a producenci na całym świecie będą mogli wytwarzać kompatybilny sprzęt oraz urządzenia.

Prace nad standardem IMT-2020

Już w 2012 roku Międzynarodowy Związek Telekomunikacyjny (ITU) rozpoczął pracę nad specyfikacją dla sieci 5G[135]. W czerwcu 2015 roku w Genewie ITU przedstawiło ogólną mapę drogową rozwoju sieci 5G i określiło nazwę standardu – IMT-2020. We wrześniu 2015 roku ITU opublikowało dokument ***Wizja IMT – Ramy i ogólne cele przyszłego rozwoju IMT***[136] ***na rok 2020 i kolejne lata*** (ITU-R M.2083[137]).

Kompletny standard ma być gotowy w 2020 roku. Jednak częściowe specyfikacje zostały opublikowane już w listopadzie 2017 roku. Były to *Minimalne wymagania dotyczące wydajności technicznej dla interfejsów radiowych IMT-2020* (ITU-R M.2410-0[138]).

Najważniejsze organizacje zajmujące się standaryzacją 5G

Międzynarodowy Związek Telekomunikacyjny *(ITU, International Telecommunication Union)* – standaryzuje oraz reguluje rynek telekomunikacyjny i radiokomunikacyjny na świecie. Jest jedną z organizacji wyspecjalizowanych ONZ. W ramach ITU działają trzy sektory: ITU-T (Sektor Normalizacji Telekomunikacji), ITU-R (Sektor Radiokomunikacji), ITU-D (Sektor Rozwoju Telekomunikacji).

3GPP *(3G Partnership Project)* zrzesza największe organizacje opracowujące standardy telekomunikacyjne na świecie. Projekt powstał w 1998 roku, żeby opracować normy dla systemów 3G. Obecnie tworzy również rozwiązania dla sieci nowej generacji.

5G PPP *(5G Infrastructure Public Private Partnership)* jest umową między Komisją Europejską oraz przemysłem. Komisja wspiera badania, a sektor prywatny odgrywa rolę lidera w określaniu strategii przemysłowej 5G.

135 *ITU towards IMT for 2020 and beyond* (https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx)
136 IMT *(International Mobile Telecommunications)* to termin używany przez społeczność ITU do oznaczania szerokopasmowych systemów mobilnych. Obejmuje łącznie IMT-2000, IMT-Advanced i IMT-2020. ITU-R opracowuje i przyjmuje międzynarodowe regulacje i standardy, które umożliwiają harmonizację i wdrożenie szerokopasmowych sieci komórkowych (3G, 4G, a teraz 5G) na całym świecie.
137 *IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond* (https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf)
138 *Minimum requirements related to technical performance for IMT-2020 radio interface(s)* (https://www.itu.int/pub/R-REP-M.2410-2017)

Oto kilka kluczowych aspektów określonych w dokumencie:

Kluczowe aspekty określone w standardzie IMT-2020

Wskaźnik	Specyfikacja
Maksymalna szybkość transmisji	• 20 Gb/s – łącze w dół *(downlink)* • 10 Gb/s – łącze w górę *(uplink)*
Doświadczana przez użytkownika szybkość transmisji danych	• 100 Mb/s w łączu w dół • 50 Mb/s w łączu w górę
Opóźnienie maksymalne	W warstwie użytkownika: • 1 ms (URLCC) • 4 ms (eMBB), W warstwie sterowania: 10-20 ms
Gęstość połączenia	1 mln urządzeń na km2
Mobilność	Zapewniona do 500 km/godz.

Po opublikowaniu wymagań przez ITU, twórcy technologii dostępu radiowego mogli zacząć opracowywać specyfikacje technologii 5G, które spełniałyby określone wytyczne. Proces ten rozpoczął się na początku 2016 roku w ramach prac 3GPP, czyli kluczowego organu normalizacyjnego dla globalnych systemów komunikacji mobilnej[139].

3GPP: pierwsza i druga faza standardu 5G

Podczas *Mobile World Congress 2017* w Barcelonie wielu wiodących operatorów telefonii komórkowej oraz dostawców sprzętu, wezwało do przyspieszenia procesu standaryzacji *5G New Radio* (w ramach tzw. *Release 15*). Celem było umożliwienie szerokich testów i pierwszych wdrożeń komercyjnych już w 2019 roku.

3GPP wyszło naprzeciw tym oczekiwaniom. Przygotowując specyfikacje uwzględniło zarówno model sieci niesamodzielnej, czyli w dużej mierze oparty o dotychczasową infrastrukturę, jak i samodzielną sieć 5G. Prace nad *Release 15* zakończyły się w czerwcu 2018 roku[140], a tym samym zakończyła się pierwsza faza standaryzacji 5G. W 2020 roku gotowy ma być *Release 16*.

- ***Release 15* – pierwsza faza standardu 5G (2018)**

  Grudzień 2017: standard dla sieci niesamodzielnych *(NSA, Non-Standalone)* – opiera się na istniejącej infrastrukturze, np. 4G. Uaktualniona do 5G zostaje tylko sieć dostępu radiowego. Zwiększy to wydajność mobilnego internetu.

139 *5G Research & Standards* (https://ec.europa.eu/digital-single-market/en/research-standards)
140 *Rel-15 success spans 3GPP groups* (https://www.3gpp.org/news-events/3gpp-news/1965-rel-15_news)

Czerwiec 2018: standard dla sieci samodzielnych *(SA, Standalone)* – umożliwi wdrożenie funkcji sieci rdzeniowej 5G oraz wprowadzenie nowych funkcjonalności. Wymaga znacznie większych zmian w architekturze sieci.

- ***Release 16*** **– druga faza standardu 5G (2020)**

Jakie aspekty uwzględniają standardy 5G

Release 15	*Release* 16
• System 5G – Faza 1	• System 5G – Faza 2
• Nowe Radio	• Przemysłowy Internet Rzeczy
• Masowa komunikacja pomiędzy maszynami oraz Internet Rzeczy	• Zwiększenie efektywności 5G
• Architektura oparta na usługach	• Ulepszenie niezwykle niezawodnej łączności o niskim opóźnieniu
• Komunikacja między pojazdem a wszystkim – faza 2 (V2X)	• Komunikacja między pojazdem a wszystkim – faza 3 (V2X)
• System komunikacji mobilnej dla kolei – faza 1 (FRMCS)	• System komunikacji mobilnej dla kolei – faza 2
• Segmentacja sieci na całej linii (*slicing – logical end-2-end networks*)	

Widmo elektromagnetyczne: fale radiowe i mikrofale

Widmo elektromagnetyczne składa się z różnego rodzaju fal[141]. Wszystkie one mają inne właściwości, które wpływają na to, jak można je wykorzystać. Na przykład w paśmie promieniowania podczerwonego prowadzone są obserwacje astronomiczne, promieniowanie ultrafioletowe jest wykorzystywane w kryminalistyce, promieniowanie rentgenowskie w diagnostyce medycznej, a promieniowanie gamma do zwalczania nowotworów w radioterapii.

Systemy telefonii komórkowej wykorzystują **fale radiowe oraz mikrofale.** Przyjmuje się, że mają one częstotliwość od 3 KHz do 300 GHz i są używane również m.in. na potrzeby transmisji radiowych (AM i FM), telewizji cyfrowej oraz satelitarnej, Wi-Fi czy Bluetooth.

Pasma na niskich częstotliwościach, to tzw. **pasma pokryciowe,** stosowane poza miastami. Zapewniają dobrą propagację, czyli rozchodzenie się fal, a więc – duży zasięg. Wyższe częstotliwości to tzw. **pasma pojemnościowe,** wykorzystywane np. tam, gdzie jest duże zagęszczenie urządzeń. Fale w tych pasmach

141 Wyróżniamy: fale radiowe, mikrofalowe, promieniowanie podczerwone, światło widzialne, promieniowanie ultrafioletowe, promieniowanie rentgenowski oraz promieniowanie gamma.

są znacznie krótsze, a przez to bardziej podatne na tłumienie czy odbicie. Mniejszy zasięg wymusza zatem większe zagęszczenie nadajników.

W przypadku 5G nowością będzie wykorzystanie częstotliwości milimetrowych (np. pasmo 26 GHz), których dotychczas nie używano w sieciach komórkowych.

Identyfikacja nowych pasm częstotliwości dla 5G

Aby móc obsłużyć zwiększający się z każdym rokiem ruch w sieciach komórkowych, konieczne było przydzielenie nowych częstotliwości na potrzeby 5G. Ich identyfikacja rozpoczęła się podczas Światowej Konferencji Radiokomunikacyjnej 2015 w Genewie **(WRC-15).** Eksperci zidentyfikowali częstotliwości w paśmie 1427-1518 MHz oraz 3,4-3,6 GHz. Zwiększyli również przepustowość mobilnego internetu szerokopasmowego w paśmie 694–790 MHz[142].

Kolejna edycja konferencji **WRC-19** odbyła się w 2019 roku w Sharm el-Sheik. W zatwierdzonych rezolucjach podkreślono, że usługi wymagające bardzo niskiego opóźnienia i dużej przepływności, będą też wymagały większych bloków widma. Dlatego zidentyfikowano pasma wyższych częstotliwości: 24,25-27,5 GHz; 37-43,5 GHz; 45,5-47 GHz; 47,2-48,2 i 66-71 GHz[143].

Spośród wskazanych pasm, doradzająca Komisji Europejskiej Grupa ds. Polityki Widma Radiowego[144] już w 2016 roku wytypowała trzy, które w pierwszej kolejności mogłyby zostać wykorzystane do uruchomienia sieci 5G :

- Pasmo niskie: **700 MHz**[146]**,** czyli tzw. pokryciowe, zapewniające dostęp na dużym obszarze przy stosunkowo małych nakładach na infrastrukturę. Fale na tych częstotliwościach rozchodzą się równomiernie i nie są aż tak pochłaniane przez przeszkody. Dzięki temu pasmo może być użyte np. do komunikacji między maszynami, a zatem wdrożenia Internetu Rzeczy.
- Pasmo średnie: **3,4–3,8 GHz,** czyli tzw. pojemnościowe, stanowi dobrą równowagę zasięgu i pojemności. Może być wykorzystywane w miastach o dużej gęstości zabudowy (eMBB), a także do wprowadzenia usług wymagających niezawodnej transmisji i szczególnie niskich opóźnień (URLLC).
- Pasmo wysokie: **26 GHz**[147]**,** może być używane do zapewnienia płynnej obsługi użytkowników w bardzo zatłoczonych miejscach (dworce, stadiony). Pasmo to wykorzystywać mogą urządzenia wymagające niskiego opóźnienia (np. Przemysł 4.0).

Nowe rozwiązania technologiczne

Aby jak najlepiej wykorzystać dostępne częstotliwości, konieczne będą nowe rozwiązania technologiczne, zarówno w obszarze sieci szkieletowej *(Core Network)*, jak i radiowej sieci dostępowej *(RAN, Radio Access Network)*.

W pierwszej fazie wdrażania 5G (*Non-Standalone*) sieci będą opierać się o już istniejącą infrastrukturę, np. 3G i 4G. Jednak pełne wdrożenie planowanych funkcjonalności będzie wymagało odejścia od tradycyjnej architektury.

142 *World Radiocommunication Conference allocates spectrum for future innovation* (https://www.itu.int/net/pressoffice/press_releases/2015/56.aspx)
143 *WRC-19 identifies additional frequency bands for 5G* (https://news.itu.int/wrc-19-agrees-to-identify-new-frequency-bands-for-5g/)
144 Grupa doradcza wysokiego szczebla, która pomaga Komisji Europejskiej w opracowaniu polityki dotyczącej widma radiowego.
145 *Radio Spectrum Policy Group Strategic Roadmap towards 5G for Europe. Opinion on spectrum related aspects for next-generation wireless systems (5G)* (https://rspg-spectrum.eu/wp-content/uploads/2013/05/RPSG16-032-Opinion_5G.pdf)
146 17 maja 2017 r. Parlament Europejski i Rada wydały Decyzję w sprawie wykorzystania zakresu częstotliwości 470-790 MHz w Unii Europejskiej. Państwa członkowskie zostały zobowiązane do udostępnienia pasma 700 MHz na potrzeby usług szerokopasmowych do 30 czerwca 2020 r. lub w uzasadnionych przypadkach najpóźniej do 30 czerwca 2022 r.
147 Decyzja wykonawcza Komisji UE z dnia 14 maja 2019 r. w sprawie harmonizacji zakresu częstotliwości 24,25-27,5 GHz na potrzeby systemów naziemnych umożliwiających świadczenie usług bezprzewodowej szerokopasmowej łączności elektronicznej w Unii. Państwa członkowskie muszą do 30 marca 2020 r. wyznaczyć oraz udostępnić zakres częstotliwości 24,25–27,5 GHz.

Niezwykle ważne stanie się oprogramowanie, ponieważ sieć będzie musiała być odpowiednio elastyczna, aby zapewnić realizację różnorodnych usług. Na przykład dla pojazdów autonomicznych najistotniejsze będzie niskie opóźnienie, dla Internetu Rzeczy – duża pojemność sieci, a dla wielbicieli kina oglądających filmy na swoich smartfonach – odpowiednia przepustowość.

Sieć szkieletowa

Jedną z najważniejszych innowacji 5G jest wirtualizacja sieci rdzeniowej[148], czyli centralnej części infrastruktury 5G zarządzającej np. usługami głosowymi, transmisją danych i połączeniami internetowymi. Wśród nowych rozwiązań technologicznych, warte podkreślenia są przede wszystkim:

- **Wirtualizacja funkcji sieciowych** *(NFV, Network Functions Virtualization)* pozwoli oddzielić sprzęt od oprogramowania sieciowego. Konkretne funkcje oraz usługi nie będą wymagać dedykowanego sprzętu, a będą mogły być zainstalowane na standardowych serwerach typu COTS (*commercial off-the-shelf*, czyli komercyjne produkty dostępne w sprzedaży), co znacznie obniży koszty.
- **Programowalne sieci/sieci definiowane programowo** *(SDN, Software Defined Network)* pozwolą oddzielić płaszczyzny sterowania i przekazywania danych. W klasycznych sieciach za te dwie funkcje odpowiadają urządzenia sieci. W SDN urządzenie sieciowe odpowiadać będzie tylko za przesyłanie danych. Zarządzanie siecią trafi do scentralizowanej warstwy kontrolnej i odbywać się będzie przy użyciu oprogramowania sterującego.
- **Dzielenie/segmentacja sieci** *(NS, Network Slicing)* – podział jednej sieci fizycznej, bazującej na wspólnej infrastrukturze, na wiele odizolowanych sieci wirtualnych, a także ich konfiguracja zgodnie z konkretnymi potrzebami. W rezultacie operatorzy mogą wdrożyć w zarządzanym przez siebie segmencie tylko niezbędne funkcjonalności, np. jeden segment zostanie przypisany dla pojazdów autonomicznych (URLLC, czyli małe opóźnienia), a inny dla rozszerzonej rzeczywistości (eMBB, bardzo duża prędkość transferu).

Radiowa sieć dostępowa

Zauważalne modyfikacje czekają również radiową sieć dostępową. Najbardziej widoczną zmianą będzie znacznie **większa liczba stacji bazowych** – zwłaszcza w miastach. Urządzenia 5G po raz pierwszy będą wykorzystywać fale o częstotliwości 26 GHz, które mają bardzo ograniczony zasięg. Dlatego stacje bazowe będą musiały znajdować się bliżej siebie.

Telefonia komórkowa – jak to działa?

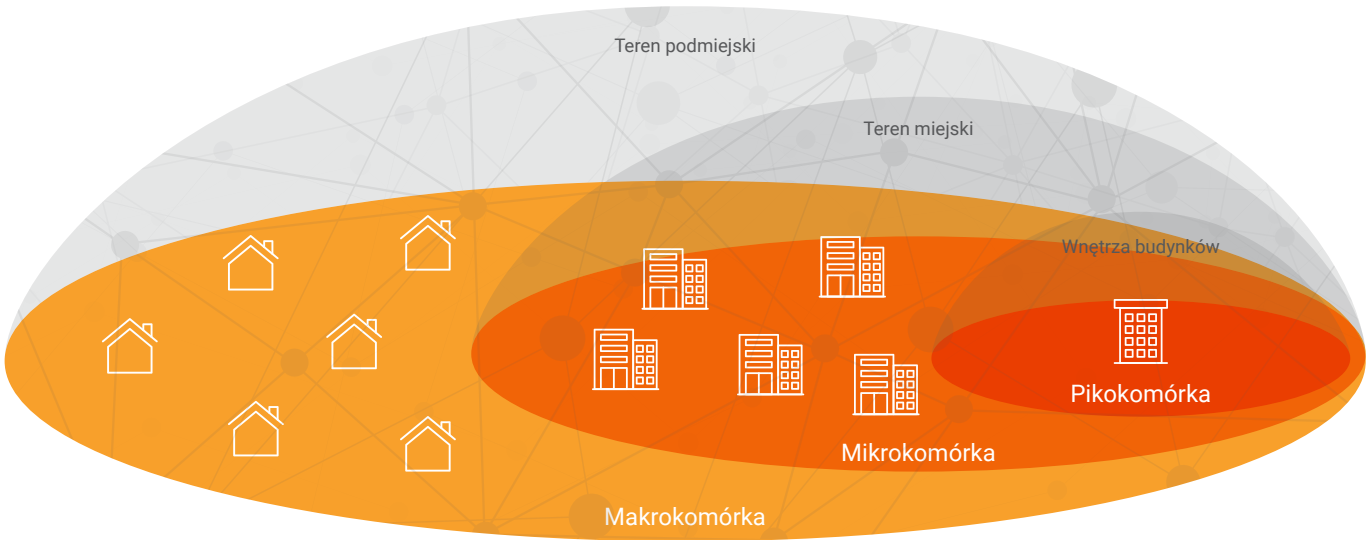
Idea systemu komórkowego polega na podzieleniu dużego obszaru na mniejsze komórki. Zamiast jednej stacji bazowej pracującej z dużą mocą i obsługującej cały system, wykorzystywanych jest wiele urządzeń o mniejszej mocy. Telefon łączy się z najbliższą stacją bazową, zapewniającą zasięg w danej komórce. Taki sposób projektowania systemu pozwala na dużą elastyczność. Duże komórki można wykorzystywać dla obszarów wiejskich, gdzie nie ma wielu użytkowników. Małe komórki sprawdzą się np. w centrum miasta.

148 W skład sieci rdzeniowej wchodzą m.in. centrala odpowiadająca za przesyłanie połączeń i pakietów danych, rejestr urządzeń na podstawie numerów IMEI, rejestr abonentów (na podstawie karty SIM), a także elementy umożliwiające np. współpracę z innymi systemami.

5G w dużej mierze wykorzystywać będzie małe komórki o zasięgu do dwóch kilometrów, a najczęściej kilkuset metrów. Nowością będą pikokomórki oraz femtokomórki, których zasięg nie przekracza kilkudziesięciu metrów. Poniżej rodzaje stacji bazowych w sieci piątej generacji.

Rodzaj stacji bazowej	Makrokomórka	Mikrokomórka	Pikokomórka[149]
Zasięg	Do kilkunastu kilometrów	Do dwóch kilometrów, najczęściej kilkaset metrów	Nie przekraczający kilkudziesięciu metrów
Częstotliwość	700 MHz	3,6 GHz	26 GHz
Zastosowanie	Usługi głosowe, Smart home, Smart city	Smart city, e-zdrowie, autonomiczne pojazdy	Przemysł 4.0, VR, AR

Rodzaje stacji bazowych



Innowacją sieci 5G będzie to, że stacje bazowe będą mogły przetwarzać oraz przechowywać dane aplikacji użytkownika. Jest to tak zwane **wielodostępowe przetwarzanie brzegowe** *(MEC, Multi-access Edge Computing)*, które odciąży sieć szkieletową i zapewni możliwość lokalnego przetwarzania danych na brzegu sieci. A zatem zasoby obliczeniowe, dotychczas dostępne w chmurze, znajdą się znacznie bliżej użytkownika końcowego. Oznacza to dużo niższe opóźnienia w przekazie danych, nawet 1 ms.

149 Jeszcze mniejsze femtokomórki, zwykle obejmują zasięg mniejszy niż 10 m.

Następna ważna innowacja dotyczy anten, które znajdują się w stacjach bazowych. Sieć 5G będzie wykorzystywać technologię **Massive MIMO** *(Massive Multiple Input Multiple Output)*, która dzięki zastosowaniu wielu anten, umożliwi jednoczesną transmisję i odbiór więcej niż jednego sygnału przez ten sam kanał radiowy. MIMO jest już stosowane w sieci LTE-Adanced, lecz w wersji *Massive* zapewni znacznie większą liczbę anten[150]. Technologia Massive MIMO umożliwi z kolei kształtowanie wiązki sygnału w określonym kierunku. Będzie to tzw. ***beamforming***, który znacznie poprawi wydajność transmisji.

Biorąc pod uwagę, że sieć 5G będzie oparta, przynajmniej w pierwszej fazie, także na infrastrukturze starszej generacji, warto wspomnieć o technologii **Multi-RAT** *(Radio Access Technology)*. Zapewni ona integrację np. z 3G, 4G czy Wi-Fi. Dzięki temu użytkownicy będą mogli automatycznie łączyć się z optymalną w danym momencie siecią.

Unia Europejska – z szansą na lidera w wyścigu 5G?

Luty 2014

Uruchomienie inicjatywy 5G PPP *(Public Private Partnership)*.

Marzec 2015

Opublikowanie dokumentu ***EU vision on 5G.***

Lipiec 2015

Pierwsza faza projektów 5G fundowanych przez UE.

Wrzesień 2016

Publikacja ***5G for Europe Action Plan.***

Czerwiec 2017

Druga faza projektów 5G fundowanych przez UE.

Lipiec 2018

Trzecia faza projektów 5G fundowanych przez UE.

150 Dzisiejsze stacje bazowe 4G mają kilkanaście portów dla anten obsługujących cały ruch komórkowy. Stacje bazowe 5G będą mogły obsługiwać około stu portów (źródło: *Everything You Need to Know About 5G*, https://spectrum.ieee.org/video/telecom/wireless/everything-you-need-to-know-about-5g)

Wrzesień 2018

Uruchomienie ***European 5G Observatory.***

Marzec 2019

Komisja Europejska wydaje **rekomendacje dotyczące cyberbezpieczeństwa** sieci 5G.

Październik 2019

Przygotowanie unijnej **skoordynowanej oceny ryzyka** związanego z cyberbezpieczeństwem w sieciach piątej generacji (5G).

Listopad 2019

Publikacja raportu ***ENISA threat landscape for 5G.***

Komisja Europejska już w 2013 roku ustanowiła partnerstwo publiczno-prywatne dotyczące 5G. Inicjatywa **5G PPP**[151] zaczęła w pełni funkcjonować w lutym 2014 roku i miała przyspieszyć rozwój tej technologii. KE przeznaczyła na wsparcie inicjatywy 700 mln euro w ramach programu *Horyzont 2020*[152]. Oczekiwano przy tym, że przemysł odpowie na to finansowanie kwotą szacowaną na ponad 3 mld euro[153].

Ważnym czynnikiem, warunkującym rozwój sieci 5G, jest współpraca międzynarodowa. Bez niej niemożliwe byłoby osiągnięcie globalnego porozumienia dotyczącego wizji 5G, standardów oraz widma radiowego. Komisja Europejska podpisała dotychczas deklaracje współpracy z Brazylią (2017), Chinami (2015), Japonią (2015) i Koreą Południową (2014). Dotyczą one m.in. wymiany informacji, wspólnych projektów badawczych, określenia usług, które będą dostarczane jako pierwsze czy też promowania globalnych standardów dla 5G. Oprócz tego prowadzona jest współpraca z Indiami, Stanami Zjednoczonymi oraz Tajwanem[154].

Globalna wizja 5G została uzgodniona na poziomie Międzynarodowego Związku Telekomunikacyjnego (ITU), a 5G PPP zapewniło europejski wkład w ten proces. W ramach partnerstwa utworzono grupy robocze m.in. do spraw architektury, widma, standardów, testów czy bezpieczeństwa.

Inwestycje w rozwój sieci 5G

Europejski plan badań nad siecią 5G został sfinansowany w ramach programu *Horyzont 2020*. Składa się z trzech etapów omówionych poniżej:

- **Faza 1: Przyszła architektura sieci 5G (2015-2017)**

  1 lipca 2015 roku Komisja Europejska uruchomiła 19 projektów badawczych o budżecie 129 mln euro. Efekty badań pozwoliły

151 *5G Infrastructure Public Private Partnership* jest umową między Komisją Europejską a przemysłem. Komisja odgrywa rolę, głównie poprzez wspieranie badań, a sektor prywatny odgrywa rolę lidera w określaniu strategii przemysłowej 5G. (https://5g-ppp.eu/)
152 *Towards 5G* (https://ec.europa.eu/digital-single-market/en/towards-5g)
153 *Europe launches a 3.5 Billion investment in 5G* (https://5g-ppp.eu/the-5g-ppp-has-started/)
154 *International Cooperation on 5G* (https://ec.europa.eu/digital-single-market/en/5G-international-cooperation)

wypracować technologiczne fundamenty dla przyszłych sieci 5G i przyczyniły się do procesu standaryzacji.

- **Faza 2: Przejście do praktycznych zastosowań i eksperymentów z udziałem branży (2017-2019)**

  1 czerwca 2017 roku Komisja Europejska uruchomiła 21 projektów o budżecie 150 mln euro. Ich celem była weryfikacja opracowanych wcześniej koncepcji. Przeprowadzono eksperymenty w kontekście bliższym przyszłemu użytkownikowi sieci (np. pojazdy autonomiczne, robotyzacja, Internet Rzeczy).

- **Faza 3: Kompleksowe platformy 5G, połączone i autonomiczne pojazdy, testy w branżach i długoterminowa ewolucja (2018-2020)**

  Pierwsza fala – konsolidacja wyników poprzednich faz. 1 lipca 2018 roku uruchomiono 3 projekty w celu zbudowania kompleksowych platform, mających połączyć 15 placów testowych w 10 różnych krajach UE.

  Druga fala – wsparcie autonomicznych pojazdów *(CAM, Connected and Automated Mobility)*. Komisja Europejska uruchomiła 1 listopada 2018 roku trzy projekty badawczo-innowacyjne, obejmujące korytarze transgraniczne uzgodnione przez sąsiadujące państwa członkowskie. Głównym celem jest stworzenie pełnego ekosystemu pojazdów autonomicznych.

  Trzecia fala – wsparcie testów i programów pilotażowych, poświęconych zademonstrowaniu możliwości 5G w branżach takich jak media i rozrywka, przemysł, zdrowie, transport czy energia. W połowie 2019 roku uruchomiono siedem nowych projektów na łączną kwotę 100 mln euro.

  Czwarta fala – ma rozpocząć się w 2020 roku. Dotyczyć będzie długoterminowej ewolucji systemów komunikacyjnych oraz technologii, które nie zostały jeszcze uwzględnione lub nie w pełni uwzględnione przez 5G PPP.

Wizja 5G dla Europy

W marcu 2015 roku podczas Światowego Kongresu Mobilnego, Komisja Europejska przedstawiła ***EU vision on 5G***[155]. Dokument został opracowany w ramach 5G PPP i podkreślał[156]:

- Kluczowe czynniki rozwoju – sieci nowej generacji zapewnią m.in. nieprzerwany dostęp do sieci w trudnych warunkach (podróże, odludne miejsca), będą wspierać krytyczne usługi wymagające niezawodności i niskich opóźnień, umożliwią rozwój Internetu Rzeczy, a także biznesu oraz całego ekosystemu innowacji technicznych.
- Przełomowe funkcje 5G – zwiększona niezawodność, przepustowość i dostępność przy mniejszych opóźnieniach. Jednoczesne podłączenie dużo większej liczby urządzeń. Bardziej wydajny sprzęt pozwoli lepiej zarządzać energią i obniżyć koszty.
- Zasady projektowania – wysoka elastyczność, skalowalność oraz podejście usługowe. Sieć powinna szybko i elastycznie dostosowywać się do szerokiego zakresu wymagań oraz zastosowań.
- Kluczowe komponenty technologiczne – aby osiągnąć wymaganą wydajność, skalowalność i elastyczność, infrastruktura 5G w dużej mierze opierać się będzie na nowych technologiach, m.in. *Software Defined Network (SDN)*, wirtualizacja funkcji sieciowych (NFV) czy *Mobile Edge Computing (MEC)*.

155 *The 5G Infrastructure Public Private Partnership: the next generation of communication networks and services* (https://5g-ppp.eu/wp-content/uploads/2015/02/5G-Vision-Brochure-v1.pdf)
156 *Mobile World Congress 2015: EU unveils its vision for 5G* (https://ec.europa.eu/digital-single-market/en/news/5g-european-research-and-vision-showcased-blueprint-showcased-mobile-world-congress-2015)

- Uwagi dotyczące widma – identyfikując nowe pasma dla 5G, należy uwzględnić tzw. fale milimetrowe, czyli częstotliwości powyżej 6 GHz. Inwestycje w nową sieć będą mieć charakter długoterminowy, dlatego kluczowe jest zapewnienie stabilnych i dobrze przemyślanych ram prawnych regulujących widmo radiowe.
- Oś czasu – komercyjne wdrożenia systemów 5G planowane po 2020 roku.

Plan działania 5G dla Europy

Aby zapewnić wczesne wdrożenie infrastruktury 5G w Europie, 14 września 2016 roku Komisja Europejska przyjęła plan działania 5G dla Europy[157]. Jego celem było rozpoczęcie świadczenia usług 5G we wszystkich państwach członkowskich do końca 2020 roku, a następnie zapewnienie nieprzerwanego zasięgu 5G na obszarach miejskich i wzdłuż głównych szlaków transportowych do 2025 roku[158]. Komisja zaproponowała działania w pięciu obszarach: Wspólny unijny harmonogram wprowadzenia 5G, udostępnienie widma radiowego 5G, stworzenie gęstej sieci punktów dostępowych, zapewnienie globalnej interoperacyjności (standaryzacja), innowacje wspierające wzrost.

Krok 1: Współpraca z państwami członkowskimi i interesariuszami z branży, w celu ustanowienia wspólnego harmonogramu wprowadzenia usług 5G.

Krok 2: Ustalenie listy pasm widma na potrzeby uruchomienia usług 5G. Lista powinna obejmować częstotliwości w co najmniej trzech zakresach widma: poniżej 1 GHz, między 1 GHz a 6 GHz oraz powyżej 6 GHz.

Krok 3: Uzgodnienie do końca 2017 roku pełnego zestawu pasm widma, w celu wdrożenia komercyjnych sieci 5G w Europie.

Krok 4: Opracowanie krajowych planów działania 5G, ustanowienie celów w zakresie wdrażania i monitorowania postępów oraz określenie najlepszych praktyk.

Krok 5: Zobowiązanie do zapewnienia początkowych standardów 5G najpóźniej do końca 2019 roku. Promowanie całościowego podejścia do standaryzacji, a także budowanie partnerstw w tym zakresie.

Krok 6: Zaplanowanie kluczowych badań technologicznych w 2017 roku, a także przedstawienie do marca 2017 roku planów wdrożenia zaawansowanych testów przedkomercyjnych.

Krok 7: Uwzględnienie w krajowych planach działania 5G możliwości wykorzystania przyszłej infrastruktury 5G, do poprawy wydajności usług komunikacyjnych zapewniających bezpieczeństwo publiczne.

157 *Communication – 5G for Europe: An Action Plan and accompanying Staff Working Document* https://ec.europa.eu/digital-single-market/en/news/communication-5g-europe-action-plan-and-accompanying-staff-working-document

158 *5G for Europe Action Plan* (https://ec.europa.eu/digital-single-market/en/5g-europe-action-plan)

Krok 8: Określenie celów i warunków dla instrumentów finansowania przedsięwzięć związanych z 5G, tak aby wesprzeć innowacyjne strat-upy, które rozwijają tę technologię. Możliwość zwiększenia finansowania prywatnego poprzez źródła publiczne, takie jak *Europejski Fundusz na rzecz Inwestycji Strategicznych (EFIS).*

Europejskie Obserwatorium 5G

W 2018 roku Komisja uruchomiła **Europejskie Obserwatorium 5G,** aby monitorować postępy wdrażania planu działania 5G dla Europy[159]. Jest to narzędzie, które opisuje zmiany na rynku oraz przygotowania podejmowane przez biznes i państwa członkowskie. Na portalu znaleźć można informacje o prowadzonych testach sieci 5G, przyjmowanych dokumentach strategicznych w poszczególnych krajach oraz częstotliwościach przydzielanych dla usług szerokopasmowych.

Z danych udostępnionych przez obserwatorium w grudniu 2019 roku[160] wynikało, że:

- 11 państw członkowskich opublikowało krajowe plany oraz mapy drogowe dotyczące wdrożenia sieci 5G.
- W 28 państwach członkowskich prowadzono łącznie 181 testów sieci nowej generacji.
- W Europie trwają prace nad 11 transgranicznymi korytarzami 5G[161]. Wśród państw, które chcą utworzyć taki korytarz są Polska i Litwa. Oba kraje podpisały list intencyjny we wrześniu 2018 roku, zobowiązując się do współpracy przy realizacji transgranicznego korytarza via Baltica (Warszawa, Kowno, Wilno)[162].

Według obserwatorium na koniec 2019 roku w sumie 15 operatorów uruchomiło komercyjne usługi 5G w 9 państwach członkowskich[163]. W gronie tych krajów nie ma Polski, choć prowadzono szeroko zakrojone testy, o których więcej informacji w dalszej części raportu[164].

Rok 2019

pod znakiem cyberbezpieczeństwa sieci 5G

W 2019 roku szczególnie duży nacisk położono na kwestię cyberbezpieczeństwa sieci 5G, która będzie miała kluczowe znaczenie dla cyfrowej transformacji gospodarki i społeczeństwa Unii Europejskiej. Szacuje się, że przychody związane z 5G osiągną w 2025 roku 225 miliardów euro[165], dlatego w Europie konieczne jest podjęcie takich kroków, aby można było konkurować na globalnym rynku. Zapewnienie właściwego poziomu bezpieczeństwa sieci nowej generacji jest niezbędne, żeby móc w pełni wykorzystać jej potencjał.

Rekomendacje dotyczące cyberbezpieczeństwa sieci 5G

26 marca 2019 roku Komisja Europejska wydała **rekomendacje cyberbezpieczeństwa sieci 5G**[166]**.** Dokument określił środki operacyjne, które miały pomóc zrealizować trzy główne cele:

- Ocena zagrożeń teleinformatycznych sieci 5G na poziomie krajowym.
- Skoordynowana unijna ocena ryzyka sieci 5G, bazująca na ocenach krajowych.

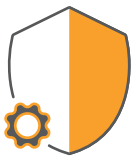
159 *European 5G Observatory* (https://ec.europa.eu/digital-single-market/en/european-5g-observatory)
160 *5G scoreboard* (September 2019) (http://5gobservatory.eu/observatory-overview/5g-scoreboards/)
161 Korytarz 5G oznacza szlak transportowy, np. autostradę lub linię kolejową, który będzie posiadał infrastrukturę umożliwiającą korzystanie z sieci 5G. Dzięki temu możliwe będą np. podróżne autonomicznych pojazdów między poszczególnymi krajami. Dodatkowo droga może być np. wyposażona w czujniki, które będą zbierać dane, pozwalające usprawnić zarządzanie ruchem.
162 *Cross-border corridors for Connected and Automated Mobility (CAM)* (https://ec.europa.eu/digital-single-market/en/cross-border-corridors-connected-and-automated-mobility-cam)
163 *5G is really ON in Europe* (http://5gobservatory.eu/5g-is-really-on-in-europe/)
164 Więcej informacji w nagłówku: Testy i wdrożenia 5G w polskich miastach.
165 *ABI Research projection:* https://www.abiresearch.com/press/abi-research-projects-5g-worldwide-servicerevenue
166 *Commission Recommendation of 26 March 2019 on Cybersecurity of 5G networks C(2019) 2335 final* (https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks)

- Przygotowanie przez Grupę Współpracy NIS zestawu środków (*toolbox*[167]), które ograniczą zagrożenia sieci 5G.

Komisja przygotowała rekomendacje na dwóch poziomach: europejskim oraz krajowym[168].

Poziom krajowy	Poziom europejski
Ocena ryzyka infrastruktury sieci 5G Do 30 czerwca 2019 roku państwa członkowskie przeprowadzą ocenę, określając wrażliwe elementy, których naruszenie miałoby negatywny wpływ na bezpieczeństwo.	**Unijny przegląd podatności związanych z infrastrukturą** Do 15 lipca 2019 roku państwa członkowskie przekażą ENISA krajowe oceny ryzyka sieci 5G. Do 1 października Komisja i ENISA przedstawi wspólny unijny przegląd podatności związanych z infrastrukturą 5G. Dodatkowo ENISA przygotuje *Krajobraz zagrożeń sieci piątej generacji.*
Przegląd krajowych wymogów bezpieczeństwa i metod zarządzania ryzykiem Do 30 czerwca 2019 roku państwa członkowskie zrobią przegląd oraz uaktualnią obowiązki nałożone na przedsiębiorstwa udostępniające usługi łączności elektronicznej.	***Toolbox* – spis zagrożeń i środki zaradcze** Do 31 grudnia 2019 roku Grupa Współpracy NIS stworzy *toolbox*, który wskaże rodzaje zagrożeń, wpływających na bezpieczeństwo sieci 5G (m.in. łańcuch dostaw, podatności oprogramowania), a także zestaw możliwych środków zaradczych dla każdego z nich (np. certyfikacja).

Rekomendacje Komisji Europejskiej dotyczyły również dwóch innych ważnych aspektów:



Certyfikacja cyberbezpieczeństwa – po opracowaniu istotnych dla 5G programów certyfikacji cyberbezpieczeństwa, państwa członkowskie powinny przyjąć krajowe przepisy wprowadzające obowiązkową certyfikację produktów, usług lub systemów technologii informacyjnych i komunikacyjnych

Zamówienia publiczne – państwa członkowskie powinny współpracować z Komisją, żeby stworzyć wymogi bezpieczeństwa, które mogłyby mieć zastosowanie przy zamówieniach publicznych dotyczących sieci 5G

167 Toolbox został opublikowany przez Grupę Współpracy NIS 29 stycznia 2020 roku. Jest to zestaw narzędzi, który określa szereg środków i działań, mających pozwolić skutecznie ograniczyć ryzyko i zapewnić wdrożenie bezpiecznych sieci 5G w całej Europie. Czytaj więcej na portalu CyberPolicy (https://cyberpolicy.nask.pl/zestaw-narzedzi-toolbox-dla-bezpieczenstwa-sieci-5g/)

168 Czytaj więcej o rekomendacjach KE na portalu CyberPolicy (https://cyberpolicy.nask.pl/rekomendacje-komisji-europejskiej-w-sprawie-dzialan-i-srodkow-operacyjnych-bezpieczenstwa-sieci-5g-w-unii-europejskiej/)

Unijna skoordynowana ocena ryzyka związanego z cyberbezpieczeństwem sieci 5G

W lipcu 2019 roku, zgodnie z marcowymi rekomendacjami Komisji Europejskiej, państwa członkowskie przekazały wypracowane dokumenty dotyczące krajowych ocen ryzyka sieci 5G. Na tej podstawie w październiku 2019 roku powstała **unijna skoordynowana ocena ryzyka związanego z cyberbezpieczeństwem w sieciach piątej generacji**[169]**.**

Raport opisuje szczególnie wrażliwe aktywa i zasoby sieci, wskazuje na jej możliwe podatności i słabe punkty, a także przedstawia przykładowe scenariusze ryzyka. Autorzy zwracają uwagę, że wykorzystanie 5G oznacza odejście od tradycyjnej architektury sieci, a najważniejszą kwestią stanie się oprogramowanie. Może to spowodować zarówno korzyści (łatwiejsza aktualizacja, konfiguracja i łatanie luk), jak i zagrożenia (większa rola zewnętrznych dostawców, wymóg przemyślanych i skutecznych procedur zarządzania poprawkami)[170].

1. Odpowiedzialność

Duży nacisk położono na szczególnie istotną rolę, którą odgrywać będą operatorzy sieci komórkowych oraz producenci sprzętu telekomunikacyjnego. Konieczna jest więc **ocena profilu ryzyka poszczególnych dostawców,** co jest o tyle istotne, że na rynku jest zaledwie kilka firm, które mogą dostarczyć technologię niezbędną do wdrożenia sieci piątej generacji.

2. Zagrożenia

Na sieci 5G oprze się wiele aspektów gospodarki oraz życia społecznego. Kluczowe będą więc jej **integralność, dostępność** oraz **poufność.** Główne zagrożenia dotyczyć mogą np.:

- Zakłócenia lokalnej lub globalnej sieci 5G (dostępność).
- Szpiegowania ruchu lub kradzieży danych (poufność).
- Przekierowania ruchu/danych w sieci 5G (integralność/poufność).
- Zniszczenia lub modyfikacji innej infrastruktury cyfrowej lub systemów informatycznych za pośrednictwem sieci 5G (integralność/dostępność).

Podmioty zagrażające sieci 5G oceniono, uwzględniając dwa aspekty: możliwości (zasoby) oraz intencje (motywacje). **Jako najbardziej znaczące wskazano zagrożenia ze strony państw lub podmiotów wspieranych przez państwo.** Wymienia się również zagrożenia takie jak: wydarzenia losowe, hakerzy, *insider*, grupa haktywistów, zorganizowana grupa przestępcza.

3. Zasoby i aktywa

Raport przedstawia podział na główne kategorie aktywów, wraz z ich poziomem wrażliwości oraz wykazem kluczowych elementów. **Za krytycznie wrażliwe uznano funkcje bazowe sieci 5G, wirtualizację funkcji sieciowych (NFV) oraz organizację sieci (MANO).**

4. Podatności i luki w zabezpieczeniach

Autorzy raportu wskazują na trzy rodzaje możliwych podatności:

- **Związane ze sprzętem, oprogramowaniem i procedurami –** poważne wady bezpieczeństwa w sprzęcie dostarczonym przez dostawcę, wynikające np. ze złych procesów tworzenia oprogramowania, mogą ułatwić złośliwe działania.

169 *Member States publish a report on EU coordinated risk assessment of 5G networks security* (https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049)
170 Czytaj więcej na portalu CyberPolicy: Unijna skoordynowana ocena ryzyka związanego z cyberbezpieczeństwem w sieciach piątej generacji (5G) (https://cyberpolicy.nask.pl/unijna-ocena-ryzyka-cyberbezpieczenstwa-w-sieciach-5g/)

- **Specyficzne dla dostawców –** np. prawdopodobieństwo, że dostawca będzie podlegać ingerencji ze strony państwa spoza UE, poprzez silny związek między dostawcą a rządem tego kraju.
- **Wynikające z zależności od poszczególnych dostawców –** zależność od jednego dostawcy wpływa na brak różnorodności używanych urządzeń i rozwiązań. To zwiększa ryzyko, ponieważ taki dostawca może np. znaleźć się pod presją handlową, ponieść komercyjną porażkę lub zostać objęty sankcjami.

Krajobraz zagrożeń dla sieci 5G

W listopadzie 2019 roku unijna skoordynowana ocena ryzyka została uzupełniona o raport ***ENISA threat landscape for 5G networks***[171]**.** Przygotowany przez Agencję UE ds. Cyberbezpieczeństwa dokument obejmuje:

- Szczegółową architekturę oraz najważniejsze elementy infrastruktury 5G.
- Ocenę zagrożeń dla 5G z uwzględnieniem zidentyfikowanych wrażliwych aktywów.
- Wstępną ocenę motywów i możliwości aktorów zagrożeń.
- Listę interesariuszy związanych z 5G.

Ponieważ wciąż brakuje wiedzy o incydentach czy ujawnionych podatnościach, zidentyfikowanie zagrożeń stanowi pewne wyzwanie. Dlatego krajobraz zagrożeń dla sieci 5G jest punktem wyjścia dla przyszłych ocen ryzyka. Autorzy raportu przewidują, że specyfika nowej generacji sieci mobilnych wpłynie na zmianę profilu zagrożeń. Należy wziąć pod uwagę:

171 *ENISA threat landscape for 5G Networks* (https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks)

- Wiele nowych podatności, co zwiększy powierzchnię ataku, ekspozycję i liczbę krytycznych zasobów.
- Nowe narzędzia oraz metody wykorzystywania podatności.
- Nowe motywy oraz cele ataku.
- Nowe złośliwe cele działających już aktorów zagrożeń.

Zagrożenia sieci 5G

Raport kategoryzuje zagrożenia na podstawie taksonomii ENISA. Wymienia m.in. złośliwą aktywność i nadużycia, przechwycenie lub podsłuchanie komunikacji, ataki fizyczne, uszkodzenia, awarie, przestoje, katastrofy czy działania prawne.

Dokument kategoryzuje również zagrożenia w zależności od celu ataku. W oparciu o to kryterium zagrożenia można podzielić na:

- **Zagrożenia sieci bazowej,** np. nadużycia zdalnego dostępu i uwierzytelniania użytkownika czy funkcji sieciowych hostowanych przez strony trzecie; wykorzystanie źle zaprojektowanej architektury lub źle skonfigurowanych systemów i sieci.
- **Zagrożenia w sieci dostępu radiowego,** np. nadużycie zasobów widma, fałszywy węzeł sieci dostępowej, manipulowanie danymi konfiguracyjnymi sieci dostępu, przejęcie sesji.
- **Zagrożenia przetwarzania brzegowego,** np. przeciążenie węzła brzegowego, nadużycie interfejsów programowania aplikacji, fałszywa brama MEC.
- **Zagrożenia wirtualizacji,** np. nadużycie zasobów obliczeniowych w chmurze, zła segmentacja sieci, wykorzystanie podatności w protokołach DCI[172].
- **Zagrożenia dla infrastruktury fizycznej,** np. klęski żywiołowe, wandalizm lub fizyczny sabotaż, dostęp pracowników firm trzecich, uszkodzenie sprzętu użytkownika.
- **Zagrożenia ogólne,** np. odmowa usługi, wyciek lub zniszczenie danych, wykorzystanie luk w zabezpieczeniach oprogramowania i sprzętu, złośliwy kod lub oprogramowanie.

Raport zawiera również rekomendacje, które podkreślają konieczność dzielenia się wiedzą oraz informacjami na poziomie Unii Europejskiej i państw członkowskich. Dużą rolę do odegrania mają nie tylko instytucje unijne oraz krajowe, ale też właściwe organy w dziedzinie cyberbezpieczeństwa 5G oraz interesariusze, np. operatorzy sieci czy dostawcy usług i sprzętu.

Toolbox – zestaw narzędzi dla bezpieczeństwa sieci 5G

Do 31 grudnia 2019 roku przygotowany miał zostać zapowiadany w rekomendacjach Komisji Europejskiej *toolbox*, czyli zestaw narzędzi, wspierający w eliminowaniu zidentyfikowanych zagrożeń dla cyberbezpieczeństwa. Ostatecznie został opublikowany 29 stycznia 2020 roku.

172 Technologia *Data Center Interconnect* (DCI) jest wykorzystywana do łączenia dwóch lub więcej centrów danych, aby urządzenia mogły dzielić zasoby.

Polska droga do 5G

Czerwiec 2017

Porozumienie na rzecz strategii *5G dla Polski*.

Styczeń 2018

Konsultacje społeczne strategii *5G dla Polski*.

Czerwiec 2018

Krajowy Plan Działań zmiany przeznaczenia pasma 700 MHz w Polsce.

Wrzesień 2018

Pierwsze testy terenowe sieci 5G w Polsce.

Październik 2018

Zakończono konsultacje zaktualizowanego *Narodowego Planu Szerokopasmowego*.

Czerwiec 2019

Ministerstwo Cyfryzacji przygotowuje serwis internetowy o 5G oraz *Białą Księgę – Pole elektromagnetyczne a człowiek*.

Lipiec 2019

Aktualizacja *Krajowego Planu Działań zmiany przeznaczenia pasma 700 MHz w Polsce*.

Październik 2019

Wejście w życie *ustawy o zmianie ustawy o wspieraniu rozwoju usług i sieci telekomunikacyjnych oraz niektórych innych ustaw* (tzw. megaustawa).

Październik 2019

Podpisanie memorandum w sprawie analizy modelu biznesowego dla spółki #Polskie5G.

Październik 2019

Wejście w życie nowelizacji *rozporządzenia Rady Ministrów w sprawie Krajowej Tablicy Przeznaczeń Częstotliwości.*

Grudzień 2019

Minister Zdrowia publikuje *rozporządzenie w sprawie dopuszczalnych poziomów pól elektromagnetycznych w środowisku (PEM).*

Grudzień 2019

Urząd Komunikacji Elektronicznej rozpoczyna konsultacje w sprawie rozdysponowania częstotliwości z pasma 3,6 GHz.

Według opracowanego przez Komisję Europejską ***Planu Działania 5G dla Europy***, do końca 2017 roku państwa członkowskie powinny przygotować strategie wdrożenia 5G. W czerwcu 2017 roku zainicjowano **porozumienie na rzecz *Strategii 5G dla Polski***[173]**.** Dokument podpisali Ministerstwo Cyfryzacji, Urząd Komunikacji Elektronicznej i Instytut Łączności PIB, a także przedstawiciele operatorów, dostawców sprzętu, instytucji badawczo-rozwojowych, izb gospodarczych oraz uczelni technicznych.

W styczniu 2018 roku rozpoczęto konsultacje społeczne wypracowanej w ramach porozumienia strategii ***5G dla Polski***[174]**.** Dokument przedstawił m.in. architekturę i standardy 5G, a także opisał cel wdrożenia sieci nowej generacji oraz planowane działania. W czasie konsultacji, które trwały od 5 stycznia do 11 lutego 2018 roku, otrzymano 38 stanowisk. Później prace nad strategią wstrzymano, a do końca 2019 roku dokument nie został przyjęty.

Kolejnym istotnym krokiem było opublikowanie w czerwcu 2018 roku ***Krajowego Planu Działań zmiany przeznaczenia pasma 700 MHz w Polsce***[175]**.** Pasmo to jest obecnie zajmowane przez naziemną telewizję cyfrową. Możliwe jest jednak przeniesienie transmisji telewizyjnych w zakres 470-694 MHz, bez straty jakości. Pasmo 700 MHz[176] zostanie wtedy zwolnione dla 5G.

Publikacja planu była odpowiedzią na *Decyzję w sprawie wykorzystania zakresu częstotliwości 470-790 MHz w Unii Europejskiej,* wydaną 17 maja 2017 roku przez Parlament Europejski i Radę. Państwa członkowskie zostały zobowiązane do udostępnienia pasma 700 MHz na potrzeby usług szerokopasmowych do 30 czerwca 2020 roku[177]. *Krajowy Plan Działań* wskazał jednak, że dotychczas nie udało się osiągnąć porozumienia z Federacją Rosyjską, która użytkuje w paśmie 700 MHz systemy radiokomunikacyjne oraz telewizyjne[178].

W październiku 2018 roku zakończyły się ogłoszone przez Ministerstwo Cyfryzacji konsultacje aktualizowanego ***Narodowego Planu Szerokopasmowego***[179] *(NPS).* Wpłynęło łącznie 16 stanowisk. W aktualizacji z 2018 roku uwzględniono zapewnienie dostępu do sieci 5G dla lepszej łączności bezprzewodowej i nowych rozwiązań technologicznych.

173 Porozumienie na rzecz Strategii 5G dla Polski (https://www.gov.pl/web/cyfryzacja/minister-cyfryzacji-podpisala-porozumienie-na-rzecz-strategii-5g-dla-polski).
174 Strategia 5G dla Polski (https://www.gov.pl/web/cyfryzacja/strategia-5g-dla-polski).
175 Krajowy Plan Działań zmiany przeznaczenia pasma 700 MHz w Polsce (https://www.gov.pl/web/cyfryzacja/krajowy-plan-dzialan-zmiany-przeznaczenia-pasma-700-mhz-w-polsce).
176 Tzw. pasmo 700 Mhz obejmuje zakres 694-790 MHz.
177 W uzasadnionych przypadkach do 30 czerwca 2022 r. Decyzja uwzględnia również wyjątek na obszarach, na których nie udało się zakończyć koordynacji technicznej z krajami trzecimi (pozaunijnymi) – co ma znaczenie, biorąc pod uwagę nieefektywny dialog w tej sprawie ze stroną rosyjską.
178 Prezes UKE podpisał stosowne dwu- i wielostronne porozumienia ze: Słowacją, Czechami, Węgrami, Niemcami, Szwecją, Litwą, Łotwą, Danią oraz dwustronne umowy z Ukrainą oraz z Republiką Białorusi.
179 Narodowy Plan Szerokopasmowy został przyjęty przez Radę Ministrów 8 stycznia 2014 r. jako rządowy program rozwoju infrastruktury szerokopasmowej w ramach Strategii Sprawne Państwo 2020. Jego oddziaływanie zostało rozszerzone dzięki wskazaniu Narodowego Planu Szerokopasmowego jako projektu strategicznego w obszarze cyfryzacji w kierunku: Rozwój nowoczesnej sieci cyfrowej w Strategii na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.).

Wskazano dwa cele:

- Zapewnienie do 2020 roku łączności 5G jako w pełni rozwiniętej usługi komercyjnej w co najmniej jednym głównym mieście[180].
- Niezakłócony dostęp do sieci 5G na wszystkich obszarach miejskich i głównych szlakach komunikacyjnych do 2025 roku.

NPS podkreślał, że polski rząd rozumie wagę wdrożenia sieci 5G dla całego państwa i rozwoju gospodarczego kraju. Wskazał przy tym na ***Plan dla 5G w Polsce***, który ma adresować kwestię mobilnych sieci nowej generacji i uzupełniać się z NPS. Jednak do końca 2019 roku dokument nie został opublikowany[181].

Rok 2019 – intensywne prace nad wdrożeniem sieci 5G w Polsce

Druga połowa 2019 roku była niezwykle intensywna, jeśli chodzi o prace związane z siecią 5G w Polsce. W lipcu opublikowano aktualizację ***Krajowego Planu Działań zmiany przeznaczenia pasma 700 MHz w Polsce.*** Wprowadziła ona m.in. przesunięcie terminu udostępnienia pasma 700 MHz dla sieci 5G do 30 czerwca 2022 roku[182] – nie będzie to jednak miało negatywnego wpływu na pozostałe państwa członkowskie. Powodem były nierozwiązane problemy koordynacji transgranicznej – brak informacji ze strony Federacji Rosyjskiej, Republiki Białorusi oraz Ukrainy o wyłączeniu do 30 czerwca 2020 roku naziemnej telewizji, działającej w paśmie 700 MHz na terenie tych krajów.

W sierpniu 2019 roku Sejm RP przyjął ***ustawę o zmianie ustawy o wspieraniu rozwoju usług i sieci telekomunikacyjnych oraz niektórych innych ustaw***[183]**.** Nowe przepisy zaczęły obowiązywać od października i mają usunąć bariery administracyjno-prawne, przeszkadzające w budowie sieci szerokopasmowych. Zwłaszcza proces inwestycyjno-budowlany ma być krótszy i prostszy. Spadną koszty inwestycji, a operatorzy będą mogli w większym stopniu wykorzystywać infrastrukturę techniczną. Ustawa powołała także Fundusz Szerokopasmowy z rocznym budżetem 140 mln zł. Środki te posłużą m.in. na dofinansowanie budowy i rozwoju sieci telekomunikacyjnych.

W październiku 2019 roku Polski Fundusz Rozwoju, Exatel, a także przedstawiciele T-Mobile, Orange i Polkomtela podpisali w siedzibie Ministerstwa Cyfryzacji memorandum w sprawie analizy modelu biznesowego dla spółki **#Polskie5G**[184]. Spółka miałaby być hurtowym operatorem ogólnopolskiej bezprzewodowej sieci 5G w paśmie 700 MHz, która zapewniałaby dostęp do usług 5G w całej Polsce. Zaproponowany model zakłada, że to państwo, poprzez spółkę celową, byłoby właścicielem jednolitej infrastruktury dla pasma pokryciowego 700 MHz. A zatem państwo miałoby wiele do powiedzenia w kwestii tego, jakie firmy będą dopuszczone do tworzenia sieci 5G w Polsce. Takie rozwiązanie mogłoby pozwolić na obniżenie kosztów budowy infrastruktury telekomunikacyjnej, co przełożyłoby się na konkurencyjne ceny usług. Ważną częścią memorandum jest konieczność zapewnienia wysokiego poziomu cyberbezpieczeństwa. Wypracowaniem uzgodnień zajmą się grupy robocze, a efekty prac zostaną przekazane Prezesowi Rady Ministrów i Ministrowi Cyfryzacji.

Normy promieniowania PEM

Rozwój sieci 5G w Polsce wymagał zmiany polskich norm promieniowania elektromagnetycznego (PEM), które były znacznie bardziej

180 Poprzednia Minister Cyfryzacji Anna Streżyńska rekomendowała, by tym pierwszym miastem była Łódź. Obecnie sytuacja nie jest jednak przesądzona.
181 Media informowały w październiku 2019 roku, że Narodowy Plan Szerokopasmowy trafił pod obrady Komitetu Stałego Rady Ministrów.
182 Aktualizacja Krajowego Planu Działań zmiany przeznaczenia pasma 700 MHz w Polsce, https://www.gov.pl/web/cyfryzacja/aktualizacja-krajowego-planu-dzialan-zmiany-przeznaczenia-pasma-700-mhz-w-polsce
183 Ustawa z dnia 30 sierpnia 2019 r. o zmianie ustawy o wspieraniu rozwoju usług i sieci telekomunikacyjnych oraz niektórych innych ustaw (http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20190001815)
184 Polskie 5G nabiera kształtów (https://www.gov.pl/web/cyfryzacja/polskie-5g-nabiera-ksztaltow)

restrykcyjne[185], niż te przyjęte w UE oraz zalecane przez WHO. Dlatego w grudniu 2019 roku Minister Zdrowia opublikował ***rozporządzenie w sprawie dopuszczalnych poziomów pól elektromagnetycznych w środowisku*** *(PEM)*[186]. Od 1 stycznia 2020 roku dopuszczalne normy dla częstotliwości od 2 GHz do 300 GHz wynoszą 10 W/m2 (gęstość mocy) i 61 V/m (składowa elektryczna) i są analogiczne do tych, obowiązujących w większości państw Unii Europejskiej.

Krokiem w stronę uspokojenia społeczeństwa, którego część obawia się negatywnych skutków ekspozycji na pole elektromagnetyczne, są zapisy obowiązującej od października tzw. megaustawy. Operatorzy telekomunikacyjni mają teraz obowiązek raportowania o poziomach pól elektromagnetycznych w środowisku. Natomiast w 2020 roku uruchomiony ma zostać system **SI2PEM**, który pozwoli sprawdzić poziom pól w dowolnym miejscu w kraju[187].

5G a dezinformacja

W 2019 roku tematy związane z pracami nad 5G cieszyły się dużym zainteresowaniem mediów, ale stały się również celem kampanii dezinformacyjnych. W sieci pojawiło się wiele fałszywych informacji, które wskazywały na szkodliwość 5G (celowa depopulacja, porównania do holocaustu) lub sugerowały, że niektóre kraje wstrzymały się z wdrażaniem sieci piątej generacji – w przeciwieństwie do Polski, której mieszkańcy zostali „królikami doświadczalnymi".

Mitami dotyczącymi 5G zajmowały się organizacje fact-checkingowe , a w czerwcu 2019 roku do problemu odniosło się Ministerstwo Cyfryzacji. Resort przygotował serwis internetowy oraz Białą Księgę – Pole elektromagnetyczne a człowiek, które miały stanowić wiarygodne źródło wiedzy o 5G.

Aukcje

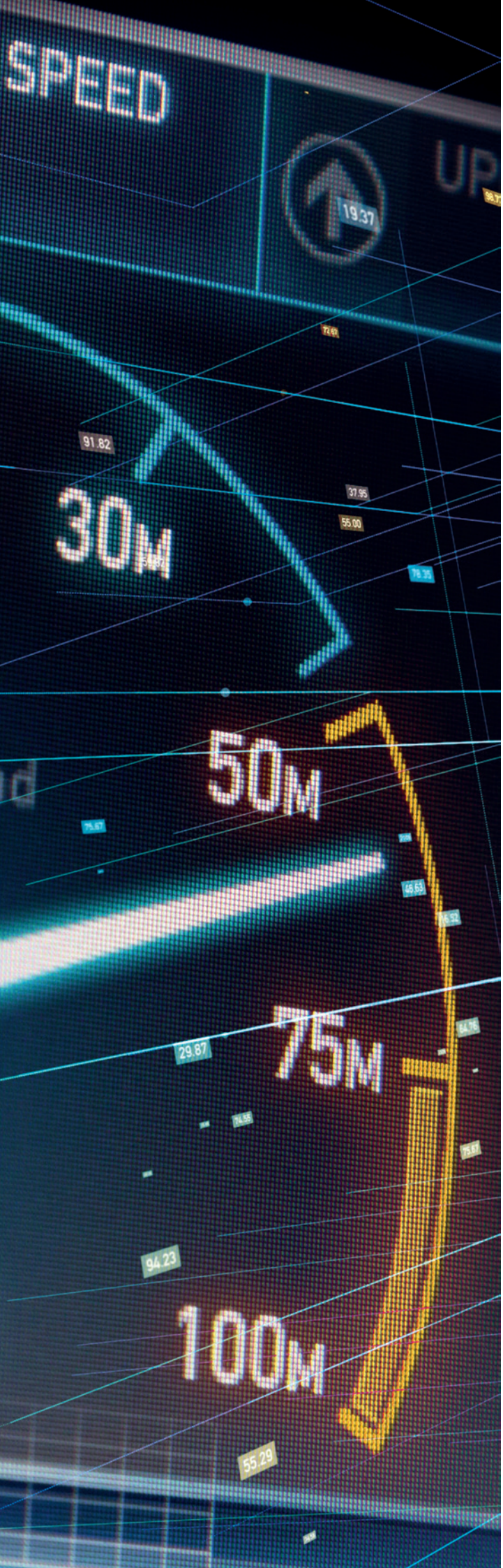
W kwietniu 2019 roku Urząd Komunikacji Elektronicznej opublikował ***Plan rozdysponowania częstotliwości z zakresu 3600-3800 MHz***[188]**.** Przewidywał on, że zakończenie procesu dystrybucji częstotliwości 3,6-3,8 GHz nastąpi na przełomie czerwca i lipca 2020 roku. Plan pierwotnie zakładał ogłoszenie przetargu, lecz w sierpniu 2019 roku UKE zdecydowało, że częstotliwości wykorzystywane w sieci 5G zostaną rozdysponowane w drodze aukcji.

9 grudnia 2019 roku rozpoczęło się postępowanie konsultacyjne w sprawie rozdysponowania **częstotliwości z pasma 3,6 GHz**[189]**.** W założeniach przewidziano 4 rezerwacje, każda po 80 MHz z pasma 3480-3800 MHz. Będą one ważne do czerwca 2035 roku. Proponowana cena wywoławcza każdego z bloków to 450 mln zł. Według założeń, zwycięzcy aukcji zostaną zobowiązani do rozwoju sieci poprzez budowę:

- Co najmniej 10 stacji bazowych na obszarze 1 miasta wojewódzkiego wybranego spośród wskazanych miast – w ciągu 6 miesięcy od otrzymania rezerwacji.
- Co najmniej 300 stacji bazowych na obszarze całego kraju, z zastrzeżeniem, że wybranych zostanie co najmniej 9 miast wojewódzkich – do 31 grudnia 2023 roku.
- Co najmniej 700 stacji bazowych na obszarze całego kraju, z zastrzeżeniem, że wybranych zostanie co najmniej 16 miast wojewódzkich – do 31 grudnia 2025 roku.

Rozszerzenie harmonogramu o aukcje w **paśmie 26 GHz** nie było możliwe przed wejściem w życie nowelizacji ***rozporządzenia Rady Ministrów w sprawie Krajowej Tablicy Przeznaczeń***

188 Plan rozdysponowania częstotliwości z zakresu 3600-3800 MHz (https://uke.gov.pl/akt/plan-rozdysponowania-czestotliwosci-z-zakresu-3600-3800-mhz,195.html)
189 27 stycznia 2020 roku rozpoczęła się druga runda postępowania konsultacyjnego w sprawie rozdysponowania częstotliwości pod 5G. Podane poniżej założenia zostały więc zaktualizowane.



Częstotliwości[190]**.** Zaktualizowane rozporządzenie obowiązuje od 3 października 2019 roku. Wprowadziło ono zmiany w przeznaczeniu częstotliwości w paśmie 26 GHz, znajdujących się wcześniej w użytkowaniu Ministerstwa Obrony Narodowej.

Testy i wdrożenia 5G w polskich miastach w 2019 roku

Według informacji ***European 5G Observatory,*** do końca 2019 roku usługi komercyjne uruchomiło łącznie 15 operatorów w dziewięciu państwach członkowskich UE[191]. Na tej liście nie znalazła się jednak Polska. Nie znaczy to jednak, że polscy operatorzy sieci mobilnych nie podejmowali działań, zmierzających do uruchomienia takich usług.

Orange

- Wrzesień 2018: stacja bazowa 5G w Gliwicach (częstotliwość 3,4-3,6 GHz, współpraca z Huawei).
- Luty 2019 roku: testy w **Zakopanem** (częstotliwość 26-28 GHz, współpraca z Ericsson).
- Wrzesień 2019: testy z udziałem klientów w **Warszawie** (9 stacji bazowych, częstotliwość 3400-3480 MHz, współpraca z Ericsson).
- Październik 2019: testy w **Lublinie** (10 stacji bazowych, częstotliwość 3500-3580 MHz, współpraca z Nokią).

Play

- Czerwiec 2019: pilotaż sieci 5G w Toruniu (częstotliwość 3,5-3,6 GHz, współpraca z Huawei). W październiku 2019 roku ruszyły testy konsumenckie.

190 Rozporządzenie Rady Ministrów z dnia 23 sierpnia 2019 r. zmieniające rozporządzenie w sprawie Krajowej Tablicy Przeznaczeń Częstotliwości (http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20190001777)
191 *5G is really ON in Europe* (http://5gobservatory.eu/5g-is-really-on-in-europe/)

- Czerwiec 2019: porozumienie w sprawie pilotażowego programu S5-Akcelerator Technologii 5G w Łodzi. Podpisane przez: Play, Ericsson, Politechnika Łódzka, UKE oraz Łódzka Specjalna Strefa Ekonomiczna.
- Lipiec 2019: list intencyjny z Ericssonem oraz Legią Warszawa w sprawie budowy sieci 5G na Stadionie Miejskim im. Marszałka Józefa Piłsudskiego.
- Listopad 2019: zgoda od UKE na testy komercyjne w Gdyni[192] w 2020 roku (100 nadajników, częstotliwość 2100 MHz, współpraca z Huawei).

T-mobile

- Grudzień 2018: testowa sieć w **Warszawie** (5 stacji bazowych, częstotliwość 3,5 GHz, współpraca z Huawei). Uruchomienie w stolicy #5G_LAB, które przedstawia korzyści płynące z wdrożenia sieci 5G.
- Październik 2019: uruchomienie wewnętrznej instalacji 5G w siedzibie hub:raum w Krakowie. Sieć zbudowana we współpracy z Nokią (pikokomórki) oraz Ericsson i Cisco (sieć rdzeniowa). Testowanie rozwiązań z zakresu *edge computing*.

Plus

- Plus nie informował szczegółowo o prowadzonych przez siebie testach. Dopiero 3 stycznia 2020 roku pojawił się ogólny komunikat, że w 2019 roku prowadzone były szerokie testy, zakończone w grudniu[193].

5G na świecie – przegląd wybranych inicjatyw w 2019 roku

Temat 5G zdominował w 2019 roku dyskusję na forum nie tylko UE, ale także innych organizacji międzynarodowych. ITU (Międzynarodowy Związek Telekomunikacyjny), NATO (Organizacja Traktatu Północnoatlantyckiego) oraz OECD (Organizacja Współpracy Gospodarczej i Rozwoju) także zajmowały się problematyką sieci piątej generacji, definiując ją jako jedno z większych wyzwań rewolucji cyfrowej.

Międzynarodowy Związek Telekomunikacyjny (ITU)

1. Światowa Konferencja Radiokomunikacyjna – WRC 19

Jednym z najważniejszych wydarzeń dla rozwoju sieci 5G w 2019 roku była konferencja zorganizowana przez ITU w listopadzie w Sharm El-Sheikh – *World Radiocommunication Conference*. Wśród postanowień końcowych *(Final Acts of the Radio Regulations)* znalazły się **zapisy dotyczące nowych pasm częstotliwości dla Międzynarodowej Telekomunikacji Mobilnej (IMT), które ułatwią rozwój sieci piątej generacji.**

Podczas konferencji ustalono, że do realizacji usług wymagających bardzo niskiego opóźnienia oraz bardzo dużej przepływności konieczne będą większe bloki widma niż dostępne w pasmach częstotliwości, które zostały zidentyfikowane wcześniej. Wobec tego zidentyfikowano dodatkowe pasma umożliwiające wdrożenie sieci 5G: 24,25-27,5 GHz, 37-43,5 GHz, 45,5-47 GHz, 47,2-48,2 i 66-71 GHz[194].W sumie podczas

192 W styczniu 2020 roku Play podpisał memorandum z Miastem Gdynia w sprawie uruchomienia sieci 5G. Świadczone usługi wykorzystują częstotliwości 2100 MHz, na których działa sieć 4G LTE.
193 Polkomtel planuje uruchomić sieć 5G w paśmie 2600 MHz TDD w pierwszym kwartale 2020 roku w 7 miastach Polski: Warszawie, Gdańsku, Katowicach, Łodzi, Poznaniu, Szczecinie i Wrocławiu. Ponad 100 stacji bazowych dostarczyć mają Nokia oraz Ericsson.
194 *WRC-19 identifies additional frequency bands for 5G* (https://news.itu.int/wrc-19-agrees-to-identify-new-frequency-bands-for-5g/)

WRC-19 zidentyfikowano 17,25 GHz widma dla IMT, przy czym 14,75 GHz widma zostało zharmonizowanych na całym świecie (85% globalnej harmonizacji).

2. **Nowy standard ITU wprowadzający uczenie maszynowe w sieciach 5G**

W sierpniu ITU opublikował nowy standard (ITU Y.3172[195]), który stworzył **podstawę dla wprowadzenia uczenia maszynowego w 5G.** Standard opisuje strukturę architektoniczną sieci, tak aby uwzględniała ona obecne oraz możliwe w przyszłości przypadki użycia uczenia maszynowego. Wykorzystanie Sztucznej Inteligencji przy zarządzaniu siecią może usprawnić jej działanie, zwiększyć efektywność energetyczną oraz obniżyć koszty eksploatacji.

3. **Spotkanie dyrektorów ds. technologii (CTO) w ramach *ITU Telecom World 2019***

We wrześniu 2019 roku w Budapeszcie odbyło się *ITU Telecom World 2019,* podczas którego doszło do spotkania dyrektorów ds. technologii z wiodących firm telekomunikacyjnych[196]. Dyrektorzy zgodzili się, że **współpraca w branży będzie kluczem do bezpieczeństwa w erze 5G.** Wskazali również, że jeśli operatorzy chcą szybko dostarczyć nowe usługi, przy jednoczesnym obniżeniu kosztów, powinni rozważyć współdzielenie infrastruktury sieciowej. Wśród kluczowych wniosków znalazły się także konieczność dalszych **inwestycji w sieci światłowodowe**, które stanowią kręgosłup społeczeństwa informacyjnego, oraz wykorzystanie uczenia maszynowego w sieciach nowej generacji. Ponadto dyrektorzy zaproponowali utworzenie obserwatorium 5G, w którym dzielono by się doświadczeniami z przeprowadzonych testów oraz wczesnych wdrożeń komercyjnych. Rozwiązanie to wsparłoby kraje rozwijające się, które mogłyby uzyskać większą wiedzę o możliwościach biznesowych 5G.

Prace nad efektywnością energetyczną sieci 5G – niedługo trzy nowe standardy

We wrześniu 2019 roku ITU poinformowało o trzech nowych standardach, które mają zwiększać efektywność energetyczną sieci 5G:

- Zrównoważone rozwiązania w zakresie zasilania energią dla sieci 5G (ITU – ITU L.1210)
- Inteligentne rozwiązanie energetyczne dla telekomunikacyjnych stacji bazowych (ITU – ITU L.1380)
- Specyfikacje systemu zarządzania infrastrukturą centrów danych (DCIM) w oparciu o technologię Big Data i Sztuczną Inteligencję (ITU – ITU L.1305)
- Zostały zatwierdzone na pierwszym etapie i mogą wejść w ostatnią fazę cyklu opracowania.

Organizacja Współpracy Gospodarczej i Rozwoju (OECD)

W lipcu OECD przygotowało publikację *The road to 5G networks. Experience to date and future developments*[197]. W raporcie przedstawiono jakich zmian można oczekiwać na rynku telekomunikacyjnym po wprowadzeniu sieci 5G. Skoncentrowano się na studiach przypadków konkretnych krajów z uwzględnieniem

195 *New ITU standard to introduce Machine Learning into 5G networks* (https://news.itu.int/new-itu-standard-machine-learning-5g-networks/)
196 *5G dominates debate at CTO meeting in Budapest* (https://news.itu.int/5g-dominates-debate-at-cto-meeting-in-budapest/)
197 *The road to 5G networks* (https://www.oecd-ilibrary.org/science-and-technology/the-road-to-5g-networks_2f880843-en)

strategii krajowych (nie ma wśród nich Polski). Raport podkreśla, że 5G to nie tylko następna technologia mobilna, ale zupełnie nowe podejście do systemów komunikacyjnych. **Jest to pierwszy standard opracowany z myślą o Internecie Rzeczy.** Wiele zależeć będzie od tego, jak szybko zostanie wdrożony, a żeby móc w pełni skorzystać z nowych możliwości, konieczne będzie opracowanie standardów, dostosowanie przepisów i regulacji, a także ewolucja modeli biznesowych. Raport zwraca szczególną uwagę na:

- **Zagęszczenie sieci –** 5G będzie wymagała budowy wielu mniejszych komórek.
- **Prawdopodobne wysokie koszty wdrożenia 5G,** na które składać się będzie m.in. rozwój sieci światłowodowej czy budowa wielu mikrokomórek. To wymusi nowe modele biznesowe 5G, partnerstwa, a być może również współdzielenie infrastruktury.
- **Nowe partnerstwa**, nie tylko w biznesie, ale także między krajami. W UE ciekawym przykładem są korytarze 5G, czyli np. autostrady, które w przyszłości umożliwią transgraniczne podróże pojazdom autonomicznym.
- **Nowe problemy regulacyjne,** dotyczące np. limitów pola elektromagnetycznego, zagęszczenia sieci czy jej segmentacji.

Sojusz Północnoatlantycki (NATO)

Sojusz również traktuje sieć 5G jako jeden z priorytetów. Podczas spotkania ministrów obrony NATO w październiku 2019 roku, przyjęto nowe wymagania dotyczące odporności cywilnej infrastruktury telekomunikacyjnej, w tym 5G[198]. Ministrowie zgodzili się, że powinny one obejmować:

Dokładną ocenę ryzyka i podatności na zagrożenia

Identyfikację i sposoby przeciwdziałania cyberzagrożeniom

Konsekwencje własności zagranicznej, kontroli lub inwestycji bezpośrednich

Zobowiązanie do zapewnienia bezpieczeństwa komunikacji, w tym sieci 5G, znalazło się też w deklaracji z grudniowego **Szczytu NATO w Londynie**[199]**.**

Interesującym wkładem w dyskusję o bezpieczeństwie sieci 5G była publikacja badawcza *Huawei, 5G, and China as a Security Threat*[200] zaprezentowana w kwietniu 2019 roku przez Centrum Doskonałości ds. Cyberobrony NATO (CCDCOE). Więcej informacji o działaniach NATO, również w zakresie 5G, w rozdziale dotyczącym Sojuszu Północnoatlantyckiego.

198 *Defence Ministers set the stage for meeting of NATO leaders in London* (https://www.nato.int/cps/en/natohq/news_169961.htm?selectedLocale=en)
199 *Secretary General: as the world changes, NATO will continue to change* (https://www.nato.int/cps/en/natohq/news_171581.htm)
200 Należy jednak pamiętać, że stanowisko CCDCOE nie jest stanowiskiem NATO.

Podsumowanie

Rok 2020 ma być przełomowy dla wdrożenia sieci 5G. Cel minimum, który powinny spełnić państwa członkowskie, to zapewnienie łączności 5G jako w pełni rozwiniętej usługi komercyjnej w co najmniej jednym głównym mieście. Dlatego w 2019 roku **działania w Polsce** skupiały się przede wszystkim na stworzeniu warunków, które umożliwią wdrożenie sieci piątej generacji. W tym celu zmieniono przepisy prawa, tak aby:

- Dostosować normy pól elektromagnetycznych do poziomu europejskiego.
- Uporządkować dostępne częstotliwości widma radiowego.
- Ułatwić budowę infrastruktury sieci 5G.

Podpisano również memorandum w sprawie analizy modelu biznesowego dla spółki #Polskie5G, która miałaby zarządzać częstotliwością 700 MHz. Z kolei UKE rozpoczęło konsultacje w sprawie rozdysponowania częstotliwości z pasma 3,6 GHz.

Na poziomie międzynarodowym główny nacisk położono na cyberbezpieczeństwo nowych sieci. **Komisja Europejska** wydała rekomendacje w tym zakresie. Przygotowano też unijną skoordynowaną ocenę ryzyka oraz uzupełniający ją raport, który przedstawił krajobraz zagrożeń dla 5G. Do końca roku pracowano także nad zestawem narzędzi, mającym skutecznie ograniczyć ryzyko i zapewnić wdrożenie bezpiecznych sieci 5G w całej Europie. Ostatecznie *toolbox* opublikowano w styczniu 2020 roku. Również **NATO** przyjęło nowe wymagania dotyczące odporności cywilnej infrastruktury telekomunikacyjnej, w tym 5G.

Z kolei organizacje, takie jak **ITU czy 3GPP,** odpowiadające za opracowanie wymagań oraz standardów dla sieci piątej generacji, wciąż prowadziły wytężone prace. ITU opublikowało na przykład nowy standard, który stwarza podstawę efektywnej integracji uczenia maszynowego z siecią 5G. Natomiast podczas ***World Radio Conference*** zidentyfikowano dodatkowe pasma częstotliwości powyżej 6 GHz dla usług 5G. Z kolei 3GPP planuje opublikować w 2020 roku tzw. drugą fazę standardu 5G (***Release* 16**).

UMIEJĘTNOŚCI CYFROWE

FUNDAMENT CYFROWEJ REWOLUCJI

– Justyna Balcewicz-Majewska –

Transformacja cyfrowa dotyka wszystkich sektorów gospodarki, w tym również edukacji i rynku pracy. Szybkie zmiany powodują wzrost niepewności, co do przyszłości zatrudnienia[201] Jednak obawa o to, że rozwój technologiczny przyczyni się do utraty pracy nie jest czymś nowym. Pojęcie **bezrobocia technologicznego** pojawiło się w latach 30. XX wieku, wprowadzone przez angielskiego ekonomistę Johna Maynarda Keynesa[202]. Wraz z rewolucją cyfrową, która charakteryzuje się ogromnym tempem przemian, powróciła obawa o przyszłość pracy. Z raportów instytucji międzynarodowych wynika, że utrzymanie zatrudnienia będzie wymagało od pracowników dostosowania się do nowych trendów na rynku pracy. Prognozowane przemiany stanowią również duże wyzwanie dla państw, ponieważ przyszłość pracy będzie w dużej mierze zależała od decyzji strategicznych[203].

Przyszłość rynku pracy będzie w dużej mierze zależała od decyzji na poziomie strategicznym

Szybki rozwój nowoczesnych technologii prowadzi do zmian strukturalnych całej gospodarki, również rynku pracy. Efekt tych przemian zależy od sposobu zarządzania transformacją, działań prewencyjnych przeciwko wykluczeniu, a także wsparcia w przekwalifikowaniu się pracowników. *World Economic Forum* przewiduje, że do 2022 roku 75 mln miejsc pracy zniknie, a na ich miejsce powstanie 133 mln nowych. Według szacunków OECD, w ciągu najbliższych 15-20 lat zautomatyzujemy 14% istniejących zawodów, a 32% ulegnie radykalnym przemianom. Zarządzenie tak dużymi zmianami w strukturze zatrudnienia, będzie wymagało przekrojowych działań z zakresu edukacji, szkoleń, prawa pracy, zabezpieczeń socjalnych i wielu innych. Dlatego organizacje międzynarodowe, takie jak ITU i OECD przygotowały zbiory rekomendacji i zestawy narzędzi (*toolboxy*), które pomagają zarządzić transformacją w obszarze kompetencji cyfrowych i edukacji. Na szczególną uwagę zasługuje przede wszystkim nowa *Strategia Umiejętności OECD*[204]. Strategia stanowi wsparcie dla państw, które na jej podstawie mogą tworzyć dokumenty krajowe, dostosowane do lokalnych realiów i potrzeb.

Rozwój kompetencji cyfrowych ma istotne znaczenie dla innowacji, wzrostu zatrudnienia i konkurencyjności europejskiej gospodarki cyfrowej. Komisja Europejska od wielu lat podejmuje systematyczne działania wspierające aktywność państw członkowskich w rozwoju kompetencji cyfrowych obywateli. Obecne podejście po raz pierwszy zostało zaprezentowane w *Europejskiej Agendzie Cyfrowej* w 2010 roku i jest kontynuowane w ramach *Strategii Jednolitego Rynku Cyfrowego dla Europy (2015), Nowego europejskiego programu na rzecz umiejętności (2016) i Planu działania w zakresie edukacji cyfrowej (2018)*. W 2018 roku kompetencje cyfrowe zostały włączone do zbioru kompetencji kluczowych, razem z kompetencjami matematycznymi, obywatelskimi, przedsiębiorczości i wielojęzyczności. Wyniki indeksu *DESI* 2019[205] wskazują, że dotychczasowe działania wciąż nie są wystarczające. W badaniu niechlubne 25 miejsce, na 28 państw europejskich, zajęła Polska, która mimo poprawy wskaźników z poprzednich lat, dalej

201 *Transformative Technologies and Jobs of the Future. Background report for the Canadian G7 Innovation Ministers' meeting 2018*, OECD Publishing, Montreal (https://www.oecd.org/innovation/transformative-technologies-and-jobs-of-the-future.pdf)
202 Bezrobocie technologiczne – bezrobocie wynikające z postępu technicznego, który powoduje zastępowanie pracy ludzi pracą maszyn i urządzeń (A. Klimczuk, M. Klimczuk-Kochańska, *Technological Unemployment*, [w:] M. Odekon (red.), *The SAGE Encyclopedia of World Poverty,* 2nd Edition, SAGE Publications, Los Angeles 2015, s. 1510-1511)
203 *OECD The Future of Work. OECD Employment Outlook 2019* (https://www.oecd-ilibrary.org/employment/oecd-employment-outlook-2019_9ee00155-en)
204 Pierwsza *Strategia Umiejętności OECD* została opublikowana w 2012 roku. W 2019 roku OECD wydało nową Strategię, uwzględniającą aktualne trendy.
205 Indeks *DESI (International Digital Economy and Society Index)* przedstawia aktualny stan gospodarki cyfrowej i społeczeństwa cyfrowego w krajach UE. Pierwszy raport DESI ukazał się w 2014 roku.

pozostaje na końcu rankingu. Polacy najgorzej wypadają w obszarze kapitału ludzkiego. 20% obywateli nie korzysta z sieci, a prawie połowie brakuje podstawowych umiejętności obsługi komputera. Konieczność podjęcia działań na rzecz rozwoju cyfrowych kompetencji w Polsce została uwzględniona w krajowej *Strategii na Rzecz Odpowiedzialnego Rozwoju*[206], a także w innych strategiach sektorowych.

W styczniu 2019 roku Rada Ministrów przyjęła *Zintegrowaną Strategię Umiejętności 2030* – część ogólną dokumentu strategicznego, którego nadrzędnym celem jest tworzenie możliwości i warunków rozwoju umiejętności niezbędnych do wzmocnienia kapitału społecznego, włączenia społecznego, wzrostu gospodarczego i poprawy jakości życia. Aktualnie polski rząd pracuje nad częścią szczegółową *Strategii*, która będzie zawierała konkretne programy, wraz ze wskazaniem podmiotów odpowiedzialnych za realizację i źródła finansowania.

Organizacje międzynarodowe

Edukacja w kontekście transformacji cyfrowej jest tematem szeroko poruszanym przez organizacje międzynarodowe: ONZ, ITU, OECD, *World Economic Forum*. Publikowane w 2018 i 2019 roku badania podejmują tą tematykę z różnych perspektyw: diagnoza trendów wpływających na edukację; opracowanie rekomendacji do strategii umiejętności; przemiany rynku pracy. Poniższa analiza przedstawia każdą z tych perspektyw na przykładzie wybranych publikacji organizacji międzynarodowych.

Organizacja	Tytuł raportu	Tematyka	Data
OECD	*Trends Shaping Education 2019*	Podsumowanie najważniejszych trendów, kształtujących oblicze edukacji i rynku pracy przyszłości.	Styczeń 2019
OECD	*Nowa Strategia Umiejętności OECD 2019*	Metody pomiaru umiejętności w państwach i wytyczne do opracowania krajowych strategii umiejętności.	Maj 2019
ITU	*Zestaw narzędzi umiejętności cyfrowych ITU*	Zestaw narzędzi wspierający utworzenie krajowych strategii umiejętności.	Maj 2018
WORLD ECONOMIC FORUM	*The Future of Jobs Report*	Perspektywa przemian rynku pracy w latach 2018-2022.	Wrzesień 2018
OECD	*The Future of Work. OECD Employment Outlook 2019*	Rekomendacje dotyczące zarządzania transformacją rynku pracy.	Kwiecień 2019

206 *Strategia na Rzecz Odpowiedzialnego Rozwoju* została przyjęta 14 lutego 2017 roku przez Radę Ministrów. Strategia określa priorytety działania Polski do 2020 roku z perspektywą do 2030 roku.

Najważniejsze trendy kształtujące oblicze edukacji w 2019 roku

21 stycznia 2019 roku Centrum Edukacji, Badań i Innowacji[207] OECD opublikowało raport zatytułowany ***Trends Shaping Education 2019***[208]. Dokument zawiera podsumowanie pięciu najważniejszych trendów ekonomicznych, politycznych, społecznych i technologicznych, które kształtują oblicze edukacji i rynku pracy przyszłości. Do tych trendów zaliczono **globalizację, kryzys demokracji, nowe zagrożenia bezpieczeństwa, starzenie się społeczeństw i zmianę wzorców społecznych.**

207 Centrum Edukacji, Badań i Innowacji OECD *(Centre for Educational Research and Innovation – CERI)* zajmuje się analizą trendów i przemian szeroko pojętej edukacji (formalnej i pozaformalnej) Celem badania *Trends Shaping Education* jest identyfikacja, na podstawie kluczowych ekonomicznych, społecznych, demograficznych i technologicznych trendów, zjawisk, które mają potencjalnie największy wpływ na edukację. Raport publikowany jest cyklicznie co 2-3 lata. Do analizy CERI wykorzystuje międzynarodowe źródła danych, źródła OECD, Banku Światowego i ONZ. Raport może służyć za źródło wiedzy decydentom, praktykom i politykom. Źródło: *Trends Shaping Education – Background* (http://www.oecd.org/education/ceri/trends-shaping-education-background.htm)

208 *OECD Trends Shaping Education 2019*, OECD Publishing, Paris (https://www.oecd-ilibrary.org/education/trends-shaping-education-2019_trends_edu-2019-en)

Pierwszym trendem jest **globalizacja** i przesunięcie ośrodka największego rozwoju gospodarczego w stronę Azji (Chiny i Indie). Globalizacja przyczynia się do wzrostu światowej konsumpcji, mobilności ludności, a także popularyzacji transgranicznego rynku towarów i usług. Szybki rozwój gospodarczy spowodował z jednej strony wzrost poziomu życia, a z drugiej rosnącą różnicę pomiędzy bogatymi i biednymi członkami społeczeństwa. Wraz z dysproporcją pojawia się problem wykluczenia osób, które z różnych powodów nie nadążają za zmianami technologicznymi. Z pogłębiających się różnic wynika zachodni **kryzys demokracji**, spowodowany nieustannymi niepokojami społecznymi i brakiem zaufania do instytucji rządzących[209]. Największe obawy budzą rosnące różnice zarobków pomiędzy najbiedniejszymi i najbogatszymi. Maleje liczba obywateli należących do klasy średniej, którzy stanowią podstawę ustroju demokracji. Rośnie poziom urbanizacji. Według przewidywań autorów raportu w 2050 roku już 70% światowej ludności będzie mieszkać w miastach, gdzie dostęp do towarów i usług, opieki zdrowotnej, edukacji, pracy, a także zarobków jest znacznie większy niż na wsi[210].

Wraz z rozwojem technologii pojawiają się dotychczas nieznane zagrożenia, związane z przenoszeniem przestępczości do cyberprzestrzeni. Wyzwaniem jest różnica w postępie technologicznym i podejściu państw do zarządzania ryzykiem w zakresie cyberbezpieczeństwa, ochrony prywatności i danych poufnych. Wciąż brakuje spójnych rozwiązań prawnych dostosowanych do wyzwań działalności w przestrzeni cyfrowej[211].

Kolejnym obserwowanym trendem jest **starzenie się społeczeństw.** W ciągu ostatnich 45 lat średnia długość życia w krajach OECD wzrosła z 70 do 80 lat, przy czym w takich krajach jak Hiszpania, Szwajcaria czy Japonia średnia sięga 83-84 lat. Jednocześnie zwiększyły się oczekiwania co do jakości życia na emeryturze. Postęp medycyny sprawił, że 80% tego czasu osoby starsze przeżywają w dobrym zdrowiu. Są też bogatsze i mają większe oczekiwania co do produktów i usług, które kupują na tzw. srebrym rynku *(silver market)*, skierowanym właśnie do osób starszych. Zmieniają się również wzorce konsumpcyjne i potrzeby osób młodych – tzw. cyfrowych tubylców[212]. Osoby te są przyzwyczajone do wykorzystywania sieci w codziennym życiu i używają Internetu do zaspokajania wszystkich potrzeb, włącznie z potrzebą przynależności do grupy, czy zakupami usług i produktów online. Umożliwia im to szeroko rozwinięty rynek cyfrowy. Wraz z tymi przemianami wzmocnieniu ulega kult indywidualizmu, czego przejawem jest zmiana wzorców społecznych, opóźnienie zawierania małżeństw, większa aktywność kobiet na rynku pracy i zaangażowanie mężczyzn w obowiązki związane z domem i wychowywaniem dzieci[213].

Strategia Umiejętności OECD 2019

OECD podkreśla, że w państwach, w których obywatele rozwijają umiejętności[214], uczą się przez całe życie i wykorzystują zdobytą wiedzę zarówno w pracy, jak i życiu społecznym, zauważalna jest większa innowacyjność, produktywność i szybsze podnoszenie poziomu dobrobytu. W kształtowaniu umiejętności niezwykle ważną rolę odgrywają regulacje. Wprowadzenie reform z zakresu umiejętności jest złożonym zagadnieniem, co wynika z rozproszenia odpowiedzialności pomiędzy instytucjami zarządzającymi edukacją, rynkiem

208 *OECD Trends Shaping Education 2019,* OECD Publishing, Paris (https://www.oecd-ilibrary.org/education/trends-shaping-education-2019_trends_edu-2019-en)
209 *OECD Trends Shaping Education 2019,* OECD Publishing, Paris, s. 35. (https://www.oecd-ilibrary.org/education/trends-shaping-education-2019_trends_edu-2019-en)
210 Bakhshi H., Downing J.M., Osborne M.A., Schneider P. (2017). *The Future of Skills: Employment in 2030.* London. Pearson and Nesta ; s. 12 (https://futureskills.pearson.com/research/assets/pdfs/technical-report.pdf)
211 *Transformative Technologies and Jobs of the Future. Background report for the Canadian G7 Innovation Ministers' meeting 2018,* OECD Publishing, Montreal (https://www.oecd.org/innovation/transformative-technologies-and-jobs-of-the-future.pdf)
212 Cyfrowi tubylcy, *digital natives* – osoby urodzone po roku 1980, dla których cyfrowe technologie są naturalnym elementem świata.
213 OECD Trends Shaping Education 2019, OECD Publishing, Paris, s. 90-99. (https://www.oecd-ilibrary.org/education/trends-shaping-education-2019_trends_edu-2019-en)
214 Umiejętności, zgodnie z definicją OECD, to pakiet wiedzy, właściwości i zdolności, których można się nauczyć i które umożliwiają jednostkom skuteczne oraz konsekwentne wykonywanie czynności lub zadań, a także mogą być budowane i rozszerzane przez uczenie się. Źródło: *Zintegrowana strategia Umiejętności 2030*; s. 19-20 (https://www.kwalifikacje.gov.pl/images/zsu.pdf)

pracy, przemysłem i prawem. Konieczna jest koordynacja działań i współpraca różnorodnych interesariuszy.

OECD dostrzegło wyzwania związane z rozwojem umiejętności już w 2012 roku. Powstała wtedy pierwsza *Strategia Umiejętności*[215]. Dokument zawierał narzędzia pomiaru lokalnych umiejętności, a także wytyczne do opracowania krajowych strategii, dostosowanych do potrzeb danego państwa. Od tego czasu, pod przewodnictwem OECD, 11 krajów opracowało własne dokumenty strategiczne[216]. 22 maja 2019 roku opublikowana została nowa ***Strategia Umiejętności OECD (OECD Skills Strategy 2019),*** dostosowana do oczekiwań zmieniającego się świata i uwzględniająca aktualne trendy, które w istotny sposób wpływają na umiejętności i wskazują które z nich będą kluczowe na rynku pracy i w życiu społecznym w przyszłości. Do trendów tych należą: globalizacja, cyfryzacja, migracje i starzenie się społeczeństwa.

Dokument wzbogacono również o przykłady dobrych praktyk z doświadczeń innych państw, a także wnioski i rekomendacje, podzielone na 3 obszary:

Rozwój umiejętności przez całe życie

Wzmocnienie systemu zarządzania umiejętnościami

Efektywne wykorzystywanie umiejętności zarówno w pracy, jak i w życiu społecznym

Wnioski i rekomendacje Strategii Umiejętności OECD 2019:

1. **Priorytetowe działania na rzecz rozwoju umiejętności przez całe życie:**

- Podnoszenie świadomości i zachęcanie do uczenia się przez całe życie.
- Zapewnienie dobrego startu do uczenia się przez całe życie.
- Zapewnienie, aby uczenie się przez całe życie było dostępne finansowo; odpowiednio doceniane i wynagradzane, a także odpowiadające wymaganiom i oczekiwaniom rynku.

2. **Priorytetowe działania na rzecz efektywnego wykorzystywania umiejętności w pracy i życiu społecznym:**

- Promowanie uczestnictwa przedstawicieli rynku pracy i społeczeństwa obywatelskiego w opracowywaniu strategii umiejętności.
- Zwiększanie puli talentów poprzez przyciąganie brakujących ekspertów z zagranicy.
- Zachęcanie pracodawców do lepszego wykorzystywania umiejętności pracowników;.
- Zredukowanie niedopasowania popytu i podaży na umiejętności.
- Stymulowanie zapotrzebowania na umiejętności wysokiego szczebla.

3. **Priorytetowe działania na rzecz wzmocnienia systemu zarządzania umiejętnościami:**

- Promowanie koordynacji działań i współpracy w ramach całego rządu.

215 *OECD Better Skills, Better Jobs, Better Lives. A Strategic Approach to Skills Policies* (2012). (https://www.oecd-ilibrary.org/education/better-skills-better-jobs-better-lives_9789264177338-en)

216 Od 2012 roku powstało łącznie 11 krajowych strategii umiejętności, z których 10 zostało ukończonych (Austria, Belgia, Włochy, Korea, Meksyk, Holandia, Norwegia, Portugalia, Słowenia i Hiszpania i Peru). W Portugalii i Słowenii wdrożono 2 strategie – druga była poprawiona o braki zidentyfikowane w pierwszym dokumencie.

- Zaangażowanie wszystkich interesariuszy.
- Budowanie integralnego systemu informacji o rozwoju umiejętności.
- Koordynacja finansowania.

Strategia Umiejętności OECD ma stanowić wsparcie dla państw przy opracowaniu strategii krajowych. W Polsce obecnie trwają prace nad częścią szczegółową Zintegrowanej Strategii Umiejętności. Część ogólną dokumentu rząd przyjął w styczniu 2019 roku (czytaj więcej na str. 142).

Zestaw narzędzi umiejętności cyfrowych ITU

Konieczność opracowania przez państwa strategii umiejętności dostrzega także ITU, które w maju 2018 roku przedstawiło ***Zestaw narzędzi umiejętności cyfrowych (ITU Digital Skills Toolkit***[217]***)***. Raport został przygotowany przez grupę ekspertów w ramach projektu *Decent Jobs for Youth*[218].

Celem *Zestawu narzędzi umiejętności cyfrowych* ITU jest zapewnienie, aby umiejętności cyfrowe były:

- Cenione i traktowane priorytetowo ze względu na swoją wiodącą rolę w świecie nowoczesnych technologii.
- Dołączone do zestawu umiejętności podstawowych (obok czytania, pisania i liczenia).
- Dostępne dla wszystkich obywateli i wykorzystywane zarówno w pracy, jak i w codziennym życiu społecznym.
- Powszechne, umożliwiające pełny rozwój technologiczny.

Zestaw narzędzi cyfrowych ITU ma być wsparciem w tworzeniu krajowych strategii umiejętności. *Toolkit* uwzględnia wiele zawiłości związanych z opracowywaniem i doskonaleniem regulacji z zakresu umiejętności cyfrowych. Wskazuje miejsce umiejętności cyfrowych w szerszych ramach umiejętności niezbędnych do funkcjonowania w przyszłości. Oferuje wskazówki jak zgromadzić interesariuszy w celu wypracowania jednej, spójnej i przekrojowej strategii. *Toolkit* opiera się na praktycznych doświadczeniach z całego świata, dostarcza realnych przykładów, inspiracji i inicjatyw, które odbywają się w innych krajach.

Państwa mogą korzystać z zestawu narzędzi w całości, do opracowania kompleksowej strategii umiejętności cyfrowych lub mogą skoncentrować się na konkretnym, priorytetowym obszarze – na przykład jak dotrzeć do grup niedostatecznie reprezentowanych. Narzędzia zostały stworzone w taki sposób, aby stymulować dyskusję i umożliwić różne ścieżki dojścia do strategii umiejętności, a nie jako sztywne wytyczne.

Przyszłość rynku pracy – Raport World Economic Forum

W 2018 roku Światowe Forum Ekonomiczne *(World Economic Forum)* zaprezentowało raport ***The Future of Jobs Report***[219]**.** W raporcie przedstawiono perspektywę krótkoterminowych przemian na rynku pracy w latach 2018-2022. Badania przeprowadzono już po raz drugi[220]. Autorzy przedstawili cztery czynniki, które będą k**ształtować zmiany na rynku pracy w najbliższej przyszłości:**

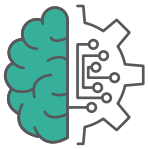
217 *ITU Digital Skills Toolkit* (2018) (https://www.itu.int/en/ITU-D/Digital-Inclusion/Documents/ITU%20Digital%20Skills%20Toolkit.pdf)

218 Projekt *Decent Jobs for Youth* jest jednym z projektów wpisujących się w realizację strategicznych celów zrównoważonego rozwoju ONZ *(2030 Agenda for Sustainable Development).* Głównym celem projektu jest działanie na rzecz zapewnienia godnego miejsca pracy dla ludzi młodych. Jest to również platforma współpracy i wymiany informacji, a także dzielenia się rekomendacjami na temat dobrych praktyk, m.in. z obszaru edukacji. (https://www.decentjobsforyouth.org/)

219 Insight Report : *The Future of Jobs Report 2018.* Centre for the New Economy and Society. World Economic Forum (http://www3.weforum.org/docs/WEF_Future_of_Jobs_2018.pdf)

220 W celu przygotowania raportu, przeprowadzane jest badanie rynku, w którym biorą udział firmy z 12 segmentów rynku i 20 branż. Próba dobierana jest proporcjonalnie również pod względem reprezentacji geograficznej i wielkości przedsiębiorstwa. Łącznie zebrano 313 odpowiedzi od firm, które razem zatrudniają ponad 150 milionów pracowników. Źródło: *WEF The Future of Jobs Report (2018);* Appendix A: Report Methodology, s. 27-30.

Wszechobecny mobilny Internet



Sztuczna Inteligencja

Big Data

Technologia chmury (Cloud)

Według danych z raportu, do 2022 roku aż 85% firm planuje wdrożyć analizę dużych zborów danych, uczenie maszynowe oraz rozszerzyć zastosowanie technologii w biznesie. Respondenci zapowiedzieli również chęć inwestowania w robotyzację (roboty stacjonarne, nie humanoidalne). Pracodawcy przewidują zmiany w sposobie produkcji i lokalizacji. Wybór lokalizacji będzie zależał przede wszystkim od dostępności wykwalifikowanej siły roboczej, a także wysokości kosztów pracy, elastyczności lokalnego prawa, a w niektórych branżach – bliskości surowców.

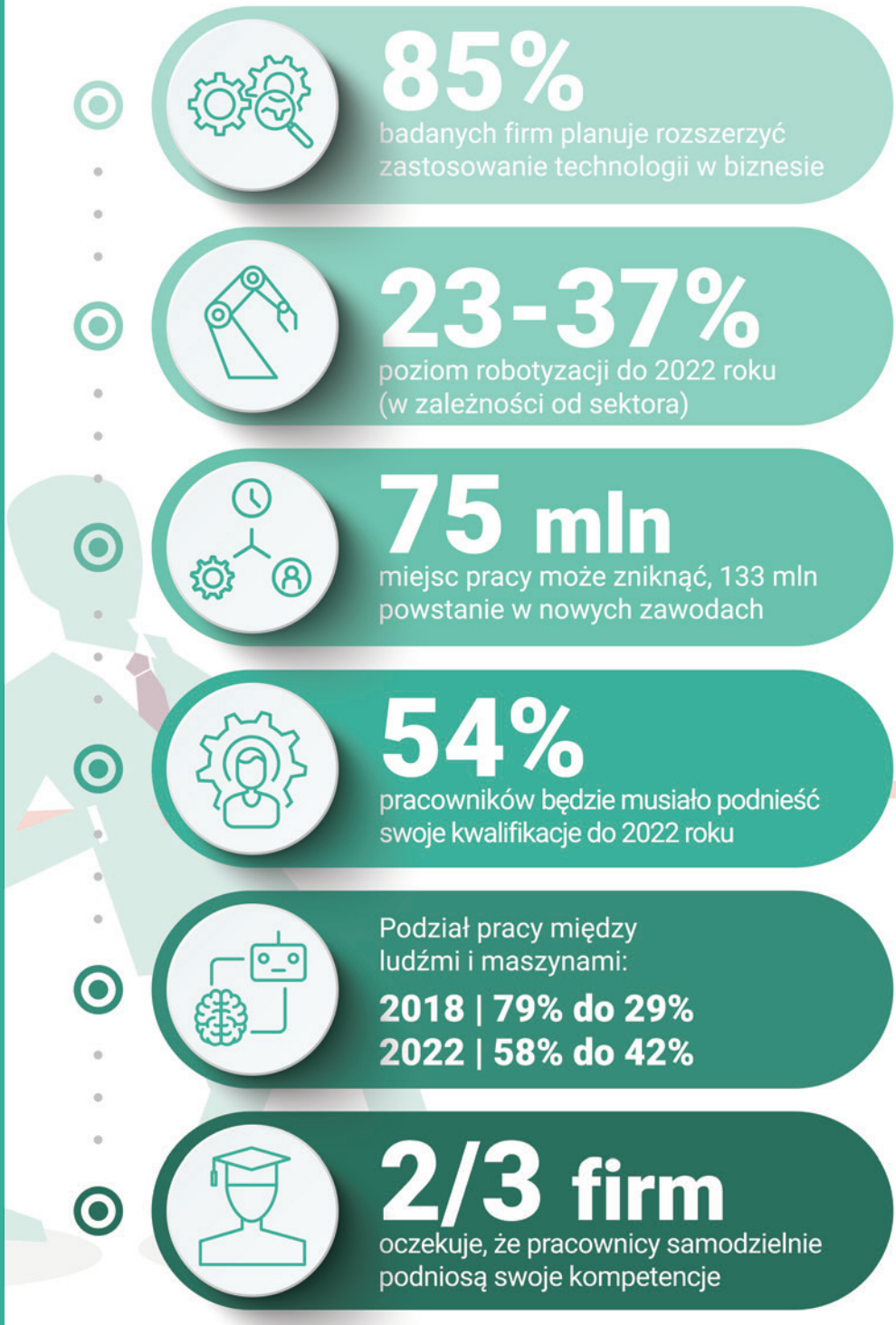
Prawie połowa firm oczekuje, że dzięki automatyzacji do 2022 roku **zmniejszy liczbę zatrudnienia pracowników w pełnym wymiarze godzin.** Równocześnie 38% spodziewa się zwiększenia liczby etatów w związku z podnoszeniem wydajności, pojawieniem się nowych ról w firmie i zatrudnieniem zdalnego personelu. Prawdopodobny jest wzrost liczby zadań wykonywanych przez maszyny z 29% zadań w 2018 roku do 42% w 2022. Do tego czasu niektóre zawody zostaną całkowicie zautomatyzowane.

Zgodnie z analizami, we wszystkich gałęziach przemysłu powstaną nowe miejsca pracy, których **będzie więcej niż tych, poddanych automatyzacji.** Oznacza to, że wyzwaniem nie jest sam brak pracy, ale konieczność wyuczenia nowych zawodów, przekwalifikowania pracowników i wyposażenia ich w nowe kompetencje. **Przewiduje się, że do 2022 roku, aż 54% wszystkich pracowników będzie musiało liczyć się z przeszkoleniem, trwającym od 6 do 12 miesięcy.** Niepokojący jest fakt, że w obliczu niedopasowania kwalifikacji personelu do zmieniających się warunków pracy, firmy deklarują chęć wymiany kadry na nową, lub oczekują, że pracownicy samodzielnie dostosują się do nowych warunków pracy. Prawie połowa firm w przypadku wystąpienia luki kompetencyjnej, zapowiada zatrudnienie pracowników tymczasowych lub zewnętrznych podwykonawców. Już teraz firmy kładą większy nacisk na zakup nowych technologii niż szkolenia pracowników, którzy będą potrafili z tej technologii korzystać. W kwestii szkoleń obserwujemy jeszcze jeden niepokojący trend. Zgodnie z danymi z raportu *World Economic Forum*, firmy planujące szkolenia, kierują je przede wszystkim do pracowników pełniących kluczowe role, a nie do tych najbardziej zagrożonych utratą pracy z powodu automatyzacji[221].

221 Insight Report : *The Future of Jobs Report 2018.* Centre for the New Economy and Society. Wrold Economic Forum, s. 7-9.

Rynek pracy Perspektywa do 2022 roku

Raport WEF – *The Future of Jobs (2018)*



Dostosowanie obowiązującego prawa do wymagań rynku pracy przyszłości – Raport OECD

Przygotowana przez ekspertów OECD diagnoza przemian rynku pracy, w przeciwieństwie do innych raportów, skupia się przede wszystkim na konieczności zarządzenia nadchodzącą transformacją. ***W raporcie The Future of Work. OECD Employment Outlook 2019***[222] autorzy zaznaczają, że w związku z szybkim rozwojem nowoczesnych technologii konieczne będą strukturalne zmiany. Efekt tych przemian w dużej mierze zależy od sposobu zarządzenia transformacją rynku pracy i decyzji na poziomie polityczno-strategicznym.

Przyszłość rynku pracy według raportu OECD:

- Transformacja cyfrowa to zarówno szanse jak i zagrożenia dla rynku pracy.
- Nowe zawody powstają szybciej niż zanikają te istniejące.
- OECD przewiduje, że 14% istniejących zawodów może zniknąć w ciągu 15-20 lat; 32% zawodów ulegnie radykalnym zmianom.
- Najbardziej zagrożeni automatyzacją są słabo wykształceni młodzi ludzie i kobiety.
- W efekcie transformacji wielu pracowników utknie na niepewnych stanowiskach, z niskim wynagrodzeniem, ograniczonym dostępem do ochrony socjalnej i blokadą dalszego rozwoju.
- Starzenie się społeczeństw może oznaczać konieczność zastępowania braków kadrowych pracą maszyn.

Działania prewencyjne

Według autorów raportu skutki transformacji rynku pracy i ryzyko związane z utratą zatrudnienia powinny zostać zneutralizowane za pomocą odpowiednio zaprojektowanego wsparcia socjalnego, które umożliwi pracownikom przekwalifikowanie się. W ramach działań prewencyjnych, warto również z wyprzedzeniem zatroszczyć się o regulacje w zakresie edukacji, również tej skierowanej do dorosłych, która przygotuje społeczeństwo do pracy w świecie nowoczesnych technologii. Efektywny system uczenia się dorosłych musi umożliwiać przekwalifikowanie się każdego rodzaju pracowników, w dowolnym momencie kariery zawodowej. Jednocześnie szkolenia powinny być zaprojektowane w sposób elastyczny, aby pracownicy mogli pogodzić dokształcanie z życiem prywatnym, obowiązkami zawodowymi i rodzinnymi.

W krajach OECD poziom szkoleń pracowników niskiego i średniego szczebla jest 40% mniejszy niż pracowników wyższego szczebla.

Pracownicy zagrożeni automatyzacją są o 30% mniej chętni na szkolenia niż pracownicy, którym automatyzacja nie grozi.

Pracodawcy chętniej szkolą pracowników na wyższych stanowiskach – czyli tych, którzy nie są zagrożeni automatyzacją.

222 Raport został przygotowany przez ekspertów do spraw zatrudnienia, pracy i polityki społecznej OECD i zawiera coroczną ocenę kluczowych przemian na rynku pracy w krajach OECD. Dokument wydano w ramach projektu *Przyszłość pracy OECD (OECD Future of Work Initiative)*, którego celem jest diagnoza przemian jakie globalizacja, postęp technologiczny i zmiana demograficzna wywierają na rynek pracy w krajach OECD, poziom umiejętności i politykę socjalną. Źródło: *Raport OECD Employment Outlook 2019, The Future of Work* (https://www.oecd-ilibrary.org/employment/oecd-employment-outlook-2019_9ee00155-en)

Równe prawa, bez względu na formę zatrudnienia

W krajach OECD wciąż **najbardziej popularnym modelem jest praca na etat,** w pełnym wymiarze godzin. Z perspektywy pracownika, etat zapewnia bezpieczeństwo pracy, daje pewność pracy na przyszłość, a także wsparcie i ochronę socjalną. Coraz większą popularnością cieszą się jednak niestandardowe formy zatrudnienia: telepraca, praca w ramach kontraktu B2B, praca tymczasowa, umowy o dzieło[223] itp. OECD zwraca uwagę, że takie umowy nie są w pełni chronione prawem pracy i mogą stanowić pole do nadużyć. Podkreśla, że **rolą rządzących jest zadbać, aby w czasach transformacji rynku pracy, każdy z pracowników miał równy dostęp do ochrony socjalnej, szkoleń i ochrony prawnej w przypadku utraty pracy.** Państwo powinno zapewnić:

- Równe traktowanie pracowników, bez względu na formę zatrudnienia.
- Zabezpieczenia socjalne nie tylko dla etatu, ale również dla innych form zatrudnienia.
- Przenoszenie uprawnień między różnymi programami zabezpieczenia społecznego.
- Wsparcie socjalne dostosowane do realnych potrzeb obywateli.
- Uzupełnienie pomocy socjalnej innymi formami wsparcia (wsparcie w szukaniu pracy, szkolenia itp.).
- Formalizację nowych sposobów zatrudnienia wynikających z rozwoju nowoczesnych technologii (np. praca za pośrednictwem platform cyfrowych).

OECD proponuje reformy w zakresie:

Lepszego egzekwowania przepisów prawa pracy

Wzmocnienia pozycji pracowników zatrudnionych na niestandardowych umowach

Uelastycznienia oferty szkoleniowej

223 Niestandardowe formy zatrudnienia pozwalają pracownikom na większą swobodę oraz łatwiejsze łączenie życia zawodowego z prywatnym. Dla firm oznaczają mniejsze koszty, swobodę w podziale pracy oraz możliwość dostosowania obsady do zapotrzebowania.

Kierunki regulacji OECD:

Zapewnienie takiego rozwoju rynku pracy, aby przyczynił się on do dobrobytu wszystkich, wymaga skoordynowanych działań politycznych w wielu obszarach, dostosowanych do charakterystyki, preferencji i zdolności każdego z państw.

Regulacje rynku pracy:

Wszyscy pracownicy, bez względu na formę zatrudnienia, posiadają takie same prawa i ochronę. W szczególności oznacza to:

- Zniesienie umów B2B tam, gdzie pracownikowi przysługuje etat.
- Zmniejszenie szarej strefy, która nie zabezpiecza praw pracownika.
- Objęcie prawami pracowników zatrudnionych w ramach niestandardowych umów.
- Promowanie na arenie międzynarodowej godnej pracy w czasach gospodarki cyfrowej, sprzeciw przeciwko nieuczciwym warunkom pracy oferowanym przez platformy cyfrowe.

Regulacje dotyczące dialogu społecznego, rokowań zbiorowych i stosunków pracy:

- Promowanie dialogu pomiędzy pracownikami i pracodawcami na poziomie krajowym.
- Pozostawienie pola do rokowań zbiorowych i samoregulacji.
- Zapewnienie szerokiego dostępu do szkoleń i wspieranie uczenia się przez całe życie dla osób dorosłych.
- Rozszerzenie definicji pracownika w prawie pracy o pracowników zatrudnionych w ramach niestandardowych form zatrudnienia.

Regulacje dotyczące uczenia dorosłych:

- Stworzenie kompleksowej strategii uczenia się dorosłych.
- Podniesienie świadomości na temat korzyści z uczenia się przez całe życie.
- Stworzenie elastycznych form szkoleniowych: poza godzinami pracy, w dostępnych miejscach, w przystępnej cenie i dla każdego typu pracowników, niezależnie od kwalifikacji.
- Zachęcanie pracodawców do przeszkolenia pracowników znajdujących się w grupach ryzyka bezrobocia technologicznego.
- Rozwój polityk uczenia się dorosłych w kierunku dotacji finansowych na szkolenia i usługi poradnictwa zawodowego.
- Zapewnienie równego dostępu do szkoleń dla wszystkich pracowników, bez względu na status.
- Zapewnienie dobrej jakości szkoleń, dostosowanych do wymogów rynku pracy.
- Opracowanie systemu współfinansowania działań przez rząd, pracodawców i osoby fizyczne.

Unia Europejska

Ponieważ silna gospodarka cyfrowa ma zasadnicze znaczenie dla innowacji, wzrostu, zatrudnienia i europejskiej konkurencyjności[224], Komisja Europejska od wielu lat podejmuje systematyczne działania na rzecz rozwoju kompetencji cyfrowych w krajach UE. W ramach indeksu *DESI (International Digital Economy and Society Index)* KE prowadzi regularny monitoring poziomu kompetencji obywateli. Wyniki z czerwca 2019 roku wskazują konieczność poprawy. Kompetencje są niezbędne zarówno do funkcjonowania na nowoczesnym rynku pracy, ale także do osiągnięcia pełnego potencjału Europy w obszarze sieci i technologii informacyjno-komunikacyjnych. Takie podejście KE zaproponowała już w Europejskiej Agendzie Cyfrowej w 2010 roku, a także w kolejnym dokumencie strategicznym: *Strategii Jednolitego Rynku Cyfrowego dla Europy*[225] z 2015 roku.

Dalsze działania na rzecz rozwoju kompetencji cyfrowych w UE, będą podejmowane w ramach programu *Cyfrowa Europa 2021-2027,* który aktualnie znajduje się na etapie konsultacji. Tematyka kompetencji została uwzględniona w działaniach programowych jako jeden z pięciu szczegółowych celów wspierających transformację cyfrową w Europie.

Kompetencje cyfrowe w dokumentach strategicznych UE

Maj 2010

Europejska Agenda Cyfrowa

Maj 2015

Strategia Jednolitego Rynku Cyfrowego dla Europy

Czerwiec 2016

Nowy europejski program na rzecz umiejętności

Styczeń 2018

Plan działania w zakresie edukacji cyfrowej

Maj 2018

Zalecenie Rady UE w sprawie kompetencji kluczowych w procesie uczenia się przez całe życie

224 *Digital Skills & Jobs* (https://ec.europa.eu/digital-single-market/en/policies/digital-skills)

225 *Strategia Jednolitego Rynku Cyfrowego dla Europy* (A Digital Single Market Strategy for Europe) została opublikowana 6 maja 2015 roku. Dokument zakłada zniesienie ograniczeń regulacyjnych w kwestiach cyfrowych w taki sposób, aby możliwe było zbudowanie Wspólnego Europejskiego Rynku Cyfrowego. Ma to pomóc w szybszym rozwoju usług cyfrowych, a tym samym budować konkurencyjność europejskich firm. Źródło: *Raport Cyberbezpieczeństwo A.D 2018* s. 19 (https://cyberpolicy.nask.pl/wp-content/uploads/2019/04/Raport-Cyberbezpiecze%c5%84stwo-A.D.-2018.pdf)

Czerwiec 2019

Indeks Gospodarki Cyfrowej i Społeczeństwa Cyfrowego DESI 2019

Lipiec 2019

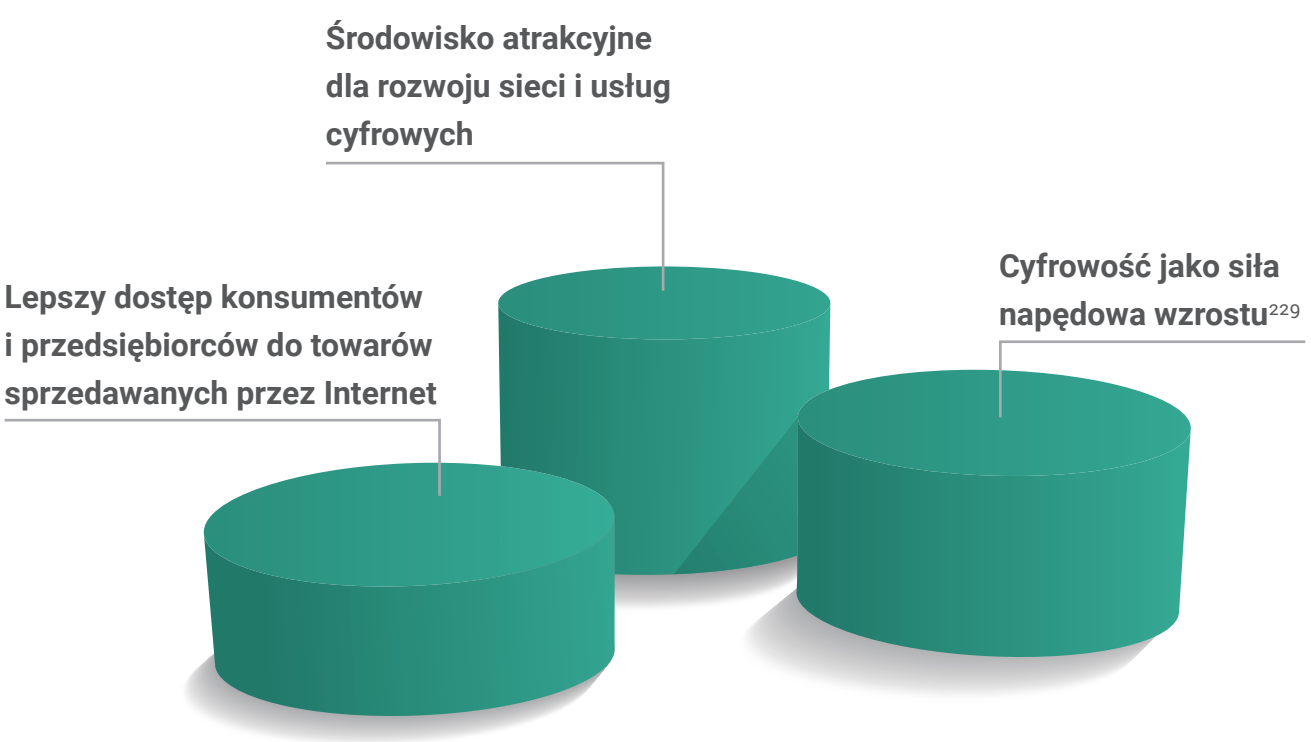
Otwarte konsultacje programu *Cyfrowa Europa 2021-2027*

Kompetencje cyfrowe w UE w okresie 2010-2018

Obecne podejście KE do kwestii kompetencji cyfrowych zostało zaprezentowane w 2010 roku w ***Europejskiej Agendzie Cyfrowej,*** która określała cele UE do końca 2020 roku w zakresie wykorzystania potencjału sieci i technologii informacyjno-komunikacyjnych. Agenda jest jednym z siedmiu kluczowych projektów programu Europa 2020[226]. Brak umiejętności wykorzystywania nowoczesnych technologii wskazano jako jedną z najważniejszych przeszkód dla realizacji programu[227].

6 maja 2015 roku Komisja Europejska opublikowała ***Strategię Jednolitego Rynku Cyfrowego dla Europy***[228] *(Digital Single Market).* Główne założenia strategii są oparte na 3 filarach:

Filary Strategii Jednolitego Rynku Cyfrowego dla Europy:



226 W dokumencie wskazano siedem priorytetowych obszarów działania: stworzenie jednolitego rynku cyfrowego; poprawa warunków ramowych dla interoperacyjności między produktami i usługami ICT; zwiększenie zaufania do Internetu i bezpieczeństwa prowadzonych w nim operacji; zapewnienie dostępu do znacznie szybszego Internetu; wzrost nakładów na badania i rozwój; rozwój umiejętności wykorzystywania technologii cyfrowych i włączenia społecznego; wykorzystanie technologii informacyjno-komunikacyjnych w celu sprostania wyzwaniom stojącym przed społeczeństwem, takim jak zmiana klimatu, wzrost kosztów leczenia i starzenie się społeczeństwa.

227 Tarkowski A., Majdecka E., Penza-Gabler Z., Sienkiewicz M., Stunża G.D., *Analiza strategii i działań mających na celu rozwój kompetencji cyfrowych w państwach Unii Europejskiej;* Fundacja Centrum Cyfrowe na zlecenie Centrum Projektów Polska Cyfrowa (2018), s. 28-29

228 *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Strategia Jednolitego Rynku Cyfrowego dla Europy* (2015) (https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52015DC0192&from=EN)

229 Wrzosek M., *Strategia Jednolitego Rynku Cyfrowego dla Europy – Strategia DSM*, Portal CyberPolicy (2015) (https://cyberpolicy.nask.pl/strategia-jednolitego-rynku-cyfrowego-dla-europy-strategia-dsm/)

W *strategii* umiejętności cyfrowe są traktowane jako kluczowy czynnik pozwalający na wzrost potencjału europejskiej gospodarki cyfrowej, przede wszystkim w kontekście rynku pracy i zatrudnienia. Ich brak wśród obywateli oznacza nie tylko brak kompetencji niezbędnych do wykonywania pracy i życia we współczesnym społeczeństwie, ale także niewykorzystywanie potencjału wzrostu europejskiej gospodarki cyfrowej. W dokumencie zapowiedziano ***Nowy europejski program na rzecz umiejętności***[230] *(New Skills Agenda for Europe)*, który przyjęto w czerwcu 2016 roku. Zawiera on 10 inicjatyw, których celem jest rozwijanie szerokiego zestawu umiejętności obywateli w celu maksymalnego wykorzystania kapitału ludzkiego w Europie. W proponowanych działaniach 2 odnoszą się bezpośrednio do kompetencji cyfrowych:

Zagwarantowanie wszystkim dorosłym obywatelom UE **minimalnego poziomu umiejętności czytania, pisania i umiejętności cyfrowych** (na poziomie wykształcenia średniego II stopnia)

Powołanie **Koalicji na Rzecz Umiejętności Cyfrowych i Zatrudnienia,** której zadaniem jest wspieranie współpracy stron odpowiedzialnych za edukację i zatrudnienie, na rzecz rozwoju kompetencji cyfrowych ludności aktywnej zawodowo[231]

Plan działania w zakresie edukacji cyfrowej

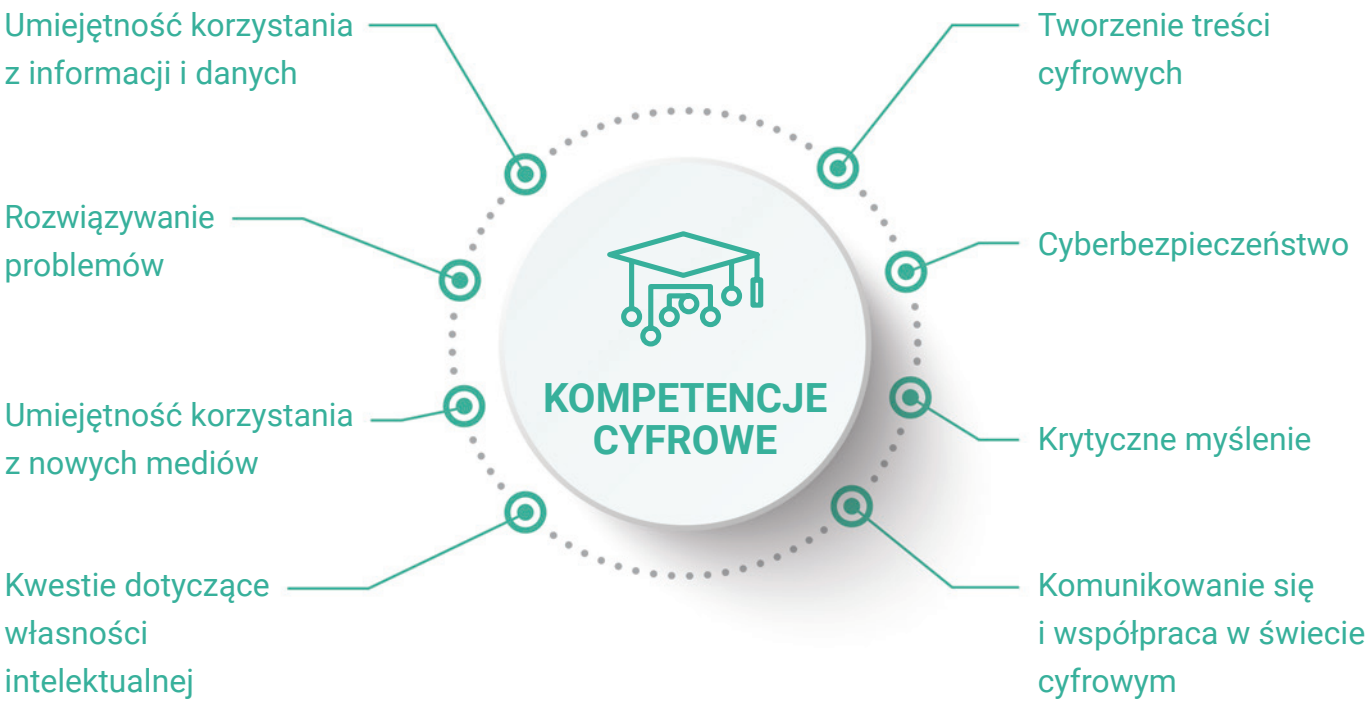
W styczniu 2018 roku opublikowano ***Plan działania w zakresie edukacji cyfrowej***[232] *(Digital Education Action Plan)*. Celem dokumentu jest budowa coraz bardziej mobilnego i cyfrowego społeczeństwa, poprzez rozwój połączonych umiejętności miękkich z solidnymi umiejętnościami cyfrowymi. Wśród trzech działań priorytetowych znalazły się:

1. Lepsze wykorzystywanie technologii w nauczaniu i uczeniu się.
2. Rozwijanie kompetencji i umiejętności cyfrowych potrzebnych w dobie transformacji cyfrowej.
3. Poprawa kształcenia dzięki lepszej analizie danych i prognozowaniu.

Zalecenie Rady w sprawie kompetencji kluczowych w procesie uczenia się przez całe życie

22 maja 2018 roku ukazało się ***Zalecenie Rady w sprawie kompetencji kluczowych w procesie uczenia się przez całe życie*** *(Council recommendation on key competences for lifelong learning)*. W załączniku do *Zalecenia* znajduje się wykaz **kompetencji kluczowych,** w którym znalazły się również kompetencje cyfrowe, definiowane jako **umiejętność krytycznego i odpowiedzialnego korzystania z technologii cyfrowych**[233]**.** Kompetencje cyfrowe zostały wskazane jako niezbędne do rozumienia sposobu wykorzystania technologii cyfrowych, budowania świadomości na temat możliwości, zagrożeń i korzyści, a także pojmowania ogólnych zasad i mechanizmów leżących u podstaw rozwoju nowoczesnych technologii.

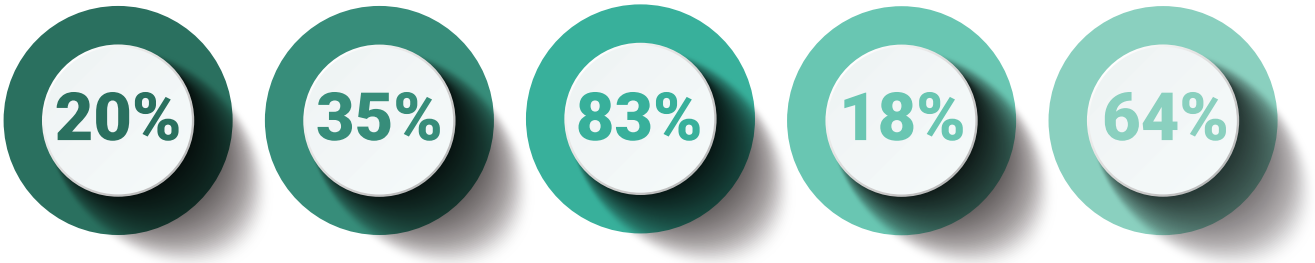
230 *New Skills Agenda for Europe (2016)* (https://ec.europa.eu/social/main.jsp?catId=1223&langId=en)
231 *New Skills Agenda for Europe (2016)* (https://ec.europa.eu/social/main.jsp?catId=1223&langId=en)
232 *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów ws. Planu działania w dziedzinie edukacji cyfrowej (2018)* (https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52018DC0022&from=EN)
233 *Zalecenie Rady z dnia 22 maja 2018 roku w sprawie kompetencji kluczowych w procesie uczenia się przez całe życie* (https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32018H0604(01)&from=EN)



Indeks Gospodarki Cyfrowej i Społeczeństwa Cyfrowego DESI 2019

11 czerwca 2019 roku Komisja Europejska opublikowała najnowsze wyniki indeksu *DESI*, który przedstawia aktualny stan gospodarki cyfrowej i społeczeństwa cyfrowego w krajach UE[234]. Indeks bierze pod uwagę pięć obszarów: łączność, kapitał ludzki, korzystanie z usług internetowych, wykorzystanie technologii cyfrowych i cyfrowe usługi publiczne.

Indeks gospodarki cyfrowej DESI 2019



Łączność

20% gospodarstw domowych w UE posiada dostęp do ultraszybkich sieci szerokopasmowych

Kapitał ludzki

35% aktywnych zawodowo obywateli nie posiada podstawowych kompetencji cyfrowych

Korzystanie z usług internetowych

83% obywateli UE korzysta z Internetu co najmniej raz w tygodniu

Wykorzystanie technologii cyfrowych

18% przedsiębiorstw korzysta z usług chmurowych

21% – z portali społecznościowych

12% – z analizy dużych zbiorów danych

Cyfrowe usługi publiczne

64% wynosi wskaźnik korzystania z cyfrowych usług publicznych w UE

Najlepsze wskaźniki zaawansowania gospodarki cyfrowej osiągnęła Finlandia, Szwecja, Holandia i Dania. Po drugiej stronie wykresu znalazła się Bułgaria, Rumunia, Grecja i Polska (czytaj dalej na stronie 136).

234 Pierwszy raport *DESI* ukazał się w 2014 roku. Od tego czasu analiza powtarzana jest co roku i dotyczy 34 wskaźników z 5 głównych kategorii: łączność, kapitał ludzki, korzystanie z usług internetowych, wykorzystanie technologii cyfrowych, cyfrowe usługi publiczne. Głównym celem raportu jest ocena postępów w realizacji celów gospodarki cyfrowej UE, monitorowanie stanu zaawansowania państw członkowskich, a także wskazanie obszarów, które wymagają poprawy. Źródło: Zegarow P.; *Indeks gospodarki cyfrowej i społeczeństwa cyfrowego (DESI 2019)* (https://cyberpolicy.nask.pl/indeks-gospodarki-cyfrowej-i-spoleczenstwa-cyfrowego-desi-2019/)

Kompetencje cyfrowe w UE w nowej perspektywie

Rozwój kompetencji został uwzględniony w wielu programach nowej perspektywy 2021-2027, w tym również w programie *Cyfrowa Europa 2021-2027* jako jeden z pięciu szczegółowych celów wspierających transformację cyfrową.

Program Cyfrowa Europa 2021-2027 *(Digital Europe Programme)*	Zwiększenie puli talentów w UE, w szczególności w obszarach: Big Data, cyberbezpieczeństwo, technologia Blockchain, robotyka i Sztuczna Inteligencja. Fundusze przeznaczone na: • **Długoterminowe szkolenia i kursy** dla studentów, prawników, informatyków (160 programów szkoleniowych na poziomie magisterium dla 80 tys. specjalistów w zakresie Sztucznej Inteligencji, cyberbezpieczeństwa i Big Data). • **Krótkoterminowe szkolenia** dla przedsiębiorców i pracowników (szkolenia z zaawansowanych technologii cyfrowych dla 150 tys. osób poszukujących pracy). • **Szkolenia w miejscu pracy i staże** dla studentów, młodych przedsiębiorców i absolwentów (w tym tworzenie miejsc pracy w firmach i ośrodkach badawczych, które umożliwią wyszkolenie wysokiej klasy specjalistów)[235]. Planowany budżet programu wynosi 700 milionów euro.
Nowy Europejski Fundusz Socjalny *(European Social Fund Plus, ESF+)*	Wsparcie państw członkowskich w poprawie jakości, skuteczności i przydatności krajowych systemów edukacji i szkoleń. Nabywanie kluczowych kompetencji, promowanie kształcenia przez całe życie, a także wsparcie możliwości przekwalifikowania się pracowników, ze szczególnym naciskiem na umiejętności cyfrowe. W ramach ESF+ zaplanowano **101 miliardów euro** na lata 2021-2027[236].
Europejski Fundusz Dostosowania do Globalizacji *(European Globalisation Adjustment Fund, EFG)*	Wsparcie dla szkoleń z obszaru kompetencji cyfrowych dla pracowników, którzy będą potrzebowali się przekwalifikować lub rozpocząć własną działalność.

235 *Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające program Cyfrowa Europa na lata 2021–2027* (https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=COM:2018:0434:FIN)
236 *EU budget: a new European Social Fund Plus* (https://ec.europa.eu/esf/main.jsp?catId=67&langId=en&newsId=9118)

Erasmus +	Wsparcie edukacji i zdobywania kompetencji (również cyfrowych) w ramach wymiany transgranicznej.
Horyzont Europa 2021-2027 *(Horizon Europe)*	Granty dla naukowców na studiach magisterskich, doktoranckich i podyplomowych we wszystkich dziedzinach, w tym również związanych z nowoczesnymi technologiami[237].

19 lutego 2020 roku KE opublikowała nową strategię cyfrową *UE Shaping Europe's digital future.* Jednym z kluczowych obszarów strategii są kompetencje obywateli w obszarze nowoczesnych technologii. KE planuje przygotować *Plan działania w sprawie edukacji cyfrowej,* a także wzmocnić *Europejską Agendę Cyfrową*. Oba dokumenty zostały zapowiedziane na drugi kwartał 2020 roku. Komisja zamierza także pochylić się nad kwestiami prawnymi nowych form zatrudnienia, np. pracy wykonywanej dla platform internetowych[238].

Polska

Poziom kompetencji cyfrowych w Polsce wymaga poprawy. W indeksie *DESI* 2019 Polska zajęła 25 miejsce na 28 państw europejskich i mimo wyższych wskaźników w stosunku do poprzedniego badania, nie poprawiła swojej pozycji w rankingu. Wyniki *DESI* pokazują, że działania, które są podejmowane w obszarze edukacji w Polsce są niewystarczające i zbyt rozproszone. Tymczasem bez zaawansowanych kompetencji cyfrowych polskich obywateli, ale też specjalistów z zakresu Sztucznej Inteligencji, nie ma mowy o budowaniu innowacyjności w państwie. Dlatego w styczniu 2019 roku polski rząd przyjął *Zintegrowaną Strategię Umiejętności 2030* (część ogólna), która jest kompleksowym dokumentem, wyznaczającym ramy umożliwiające wdrażanie spójnej polityki na rzecz rozwijania umiejętności i uczenia się przez całe życie. Ważnym elementem *Strategii* są umiejętności cyfrowe.

Przegląd ważnych wydarzeń dotyczących rozwoju kompetencji cyfrowych w Polsce w 2019 roku

Styczeń 2019

Uchwalenie *Zintegrowanej Strategii Umiejętności 2030 (część ogólna).*

Luty 2019

Powstaje Fundacja Platforma Przemysłu Przyszłości.

Luty 2019

Ministerstwo Obrony Narodowej tworzy program CYBER.MIL.PL.

238 *European Commission: Shaping Europe's Digital Future* (https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf)

Sierpień 2019

Konsultacje dokumentu *Polityka Rozwoju Sztucznej Inteligencji w Polsce na lata 2019 – 2027.*

Listopad 2019

Powołanie Akademii Innowacyjnych Zastosowań Technologii Cyfrowych.

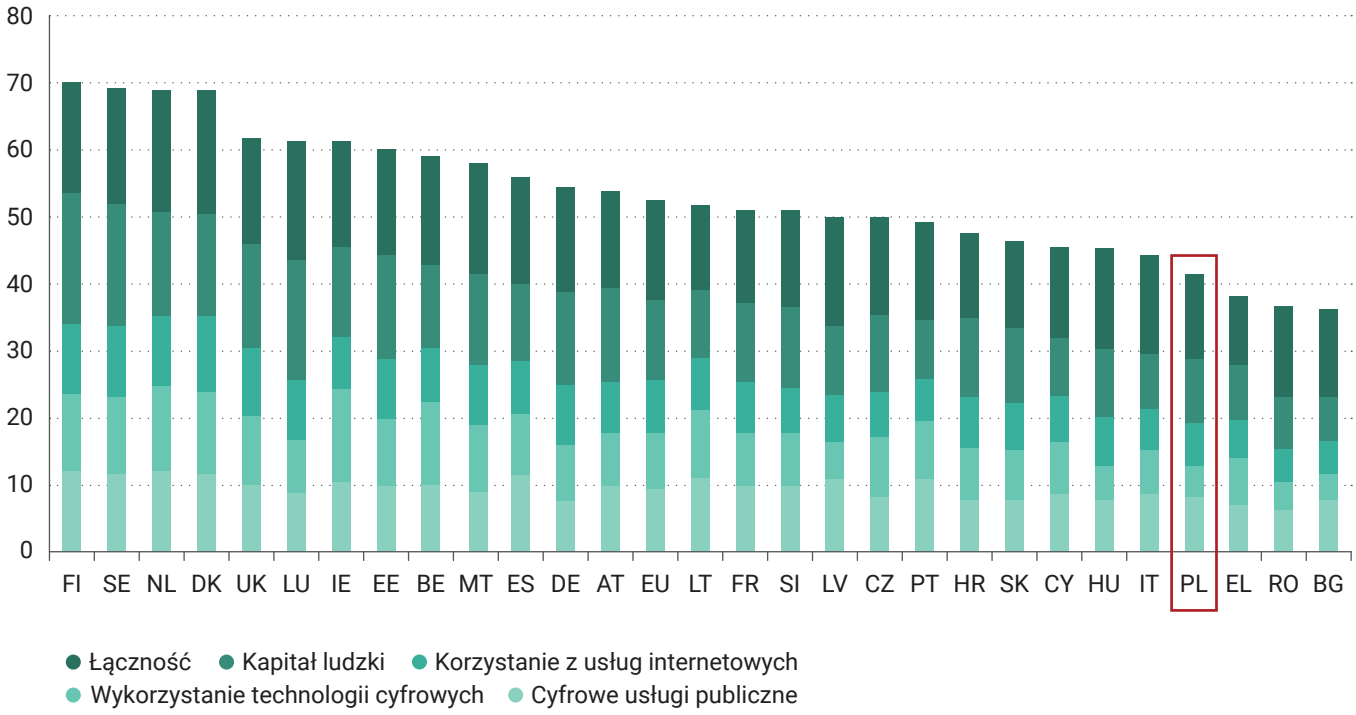
Grudzień 2019

Strategia umiejętności OECD: Polska.

Stan kompetencji cyfrowych w Polsce

Polska w najnowszym Indeksie *DESI* 2019 zajęła 25 miejsce na 28 państw europejskich. Polacy najgorzej wypadają w obszarze wykorzystania technologii cyfrowych i korzystania z usług internetowych. Wciąż 1/5 obywateli nie korzysta z sieci, a prawie połowie brakuje podstawowych kompetencji cyfrowych. Rośnie liczba specjalistów ICT, jednak pozostaje ona poniżej średniej europejskiej. Polskie firmy posiadają niski wskaźnik cyfryzacji. 56% znajduje się na niskim poziomie cyfryzacji (w UE jest to już tylko 46%), a zaledwie 12% na wysokim poziomie (w UE 18%).

Indeks gospodarki cyfrowej DESI 2019



Indeks DESI 2019
Wyniki Polski na tle Unii Europejskiej

Łączność	Kapitał ludzki	Korzystanie z usług internetowych	Wykorzystanie technologii cyfrowych	Cyfrowe usługi publiczne
Średnia Unii Europejskiej	Średnia Unii Europejskiej	Średnia Unii Europejskiej	Średnia Unii Europejskiej	Średnia Unii Europejskiej
59,3	**48**	**53,4**	**41,4**	**62,9**
Miejsce Polski wśród krajów	Miejsce Polski wśród krajów	Miejsce Polski wśród krajów	Miejsce Polski wśród krajów	Miejsce Polski wśród krajów
UE 24/28	**UE 22/28**	**UE 24/28**	**UE 26/28**	**UE 23/28**

Kompetencje cyfrowe w polskich dokumentach strategicznych

Konieczność podjęcia działań na rzecz rozwoju kompetencji cyfrowych w Polsce została uwzględniona w licznych dokumentach strategicznych, również w ***Strategii na Rzecz Odpowiedzialnego Rozwoju***[239], która określa priorytety działania Polski do 2020 roku, z perspektywą do roku 2030. Głównym celem strategii jest tworzenie warunków dla rozwoju cyfryzacji i dopasowanie kompetencji pracowników do wyzwań rynku pracy. Przekłada się to na utrzymanie poziomu zatrudnienia i wzrost dochodów mieszkańców Polski. Rozwój kompetencji cyfrowych powinien odbywać się na każdym etapie życia, również poprzez edukację pozaformalną[240].

Kompetencje cyfrowe są obszarem przekrojowym.

Konieczność ich rozwoju podkreślono w wielu strategiach sektorowych:

Dokument strategiczny	Proponowane działania na rzecz rozwoju kompetencji cyfrowych
Strategia Rozwoju Kapitału Ludzkiego	Opracowanie programu rozwoju kompetencji cyfrowych do 2030 roku.
Strategia Innowacyjności i Efektywności Gospodarki (Strategia Produktywności)	Dostosowanie kompetencji do wyzwań przyszłości. Rozwój kompetencji cyfrowych na wszystkich etapach kształcenia.
Strategia Rozwoju Kapitału Społecznego	Zwiększenie poziomu umiejętności korzystania z zasobów cyfrowych, a także edukacja medialna.
Strategia Sprawne i Nowoczesne Państwo 2020	Podnoszenie kompetencji cyfrowych społeczeństwa i administracji.
Strategia Zrównoważonego Rozwoju Wsi, Rolnictwa i Rybactwa 2030	Podnoszenie umiejętności mieszkańców terenów wiejskich w wykorzystywaniu technologii ICT.
Krajowa Strategia Rozwoju Regionalnego 2030	Rozwój kompetencji cyfrowych Polaków.

239 Uchwała nr 8 Rady Ministrów z dn. 14 lutego 2017 roku w sprawie przyjęcia *Strategii na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 roku).* (https://www.infor.pl/akt-prawny/MPO.2017.044.0000260,uchwala-nr-8-rady-ministrow-w-sprawie-przyjecia-strategii-na-rzecz-odpowiedzialnego-rozwoju-do-roku-2020-z-perspektywa-do-2030-r.html)

240 *Informacje o Strategii na rzecz Odpowiedzialnego Rozwoju* (https://www.gov.pl/web/fundusze-regiony/informacje-o-strategii-na-rzecz-odpowiedzialnego-rozwoju)

Założenia do strategii AI w Polsce

Kwestia konieczności dostosowania edukacji do realiów ery cyfrowej coraz częściej pojawia się w kontekście rozwoju nowoczesnych technologii, Sztucznej Inteligencji, Big Data, Internetu Rzeczy czy sieci 5G. Ponieważ warunkiem koniecznym do rozwoju technologii jest wykształcenie wysokiej klasy specjalistów i konsumentów danego rozwiązania, kwestia edukacji była jednym z kluczowych tematów przy tworzeniu ***Założeń do strategii Sztucznej Inteligencji w Polsce***[241]**.** Dokument ten został opublikowany przez Ministerstwo Cyfryzacji 9 listopada 2018 roku[242].

Eksperci przygotowujący wkład do *Założeń* w ramach grupy roboczej dotyczącej edukacji podkreślili potrzebę systemowego budowania kompetencji cyfrowych na każdym etapie kształcenia. Zauważyli, że niski poziom kompetencji cyfrowych dzieci i młodzieży przekłada się na niewystarczające umiejętności dorosłych. To z kolei skutkuje brakiem wykwalifikowanych pracowników i niechęcią do poznawania nowych rozwiązań technologicznych.

Poniższa tabela przedstawia główne kierunki rekomendowanych działań, podzielone według grup tematycznych: tworzenie, wdrożenie, użytkowanie i adaptacja.

241 *Założenia do strategii AI w Polsce* (https://www.gov.pl/documents/31305/436699/Za%C5%82o%C5%BCenia_do_strategii_AI_w_Polsce_-_raport.pdf)

242 W opracowaniu dokumentu brali udział przedstawiciele administracji publicznej, sektora prywatnego, organizacji pozarządowych, oświaty i szkolnictwa wyższego, nauki i związków zawodowych. Raport stanowi wkład do projektu założeń do *Polityki Rozwoju Sztucznej Inteligencji* (czytaj więcej na str. 156).

Kierunki Działań

1. TWORZENIE Kształcenie specjalistów tworzących AI	1.1. Zwiększenie potencjału AI w Polsce oraz przygotowanie programów zachęcających firmy do uruchamiania staży w zakresie AI dla uczniów i studentów 1.2. Budowanie zainteresowania edukacją w specjalizacjach AI
2. WDRAŻANIE Kształcenie specjalistów współtworzących i wykorzystujących rozwiązania AI	2.1. Podniesienie kompetencji specjalistów branżowych wdrażających AI oraz specjalistów i decydentów otoczenia AI (administracja publiczna) 2.2. Działania edukacyjne dla kadr zarządzających przedsiębiorstw dot. skali szans i zagrożeń związanych z transformacją cyfrową (AI)
3. UŻYTKOWANIE Kształcenie użytkowników AI	3.1. Rozwój powszechnych kompetencji cyfrowych tak, by wspierać wykorzystanie AI we wszystkich sferach życia – ze szczególnym uwzględnieniem liderów zmiany i osób zdolnych edukować innych 3.2. Wprowadzenie rozwoju kompetencji związanych z AI, pracą z danymi i programowaniem jako zagadnienia strategicznego dla systemu oświaty
4. ADAPTACJA Przekwalifikowanie w związku z zastępowaniem pracowników przez narzędzia oparte o AI	4.1. Dostosowywanie systemu edukacji i kształcenia ustawicznego do wyzwań postępu technologicznego 4.2. Budowa systemu prognozowania zapotrzebowania na przyszłe zawody i kwalifikacje, w związku z rozwojem AI

Źródło: *Założenia do strategii AI w Polsce. Plan działań Ministerstwa Cyfryzacji*. s. 84 (https://www.gov.pl/documents/31305/436699/Za%C5%82o%C5%BCenia_do_strategii_AI_w_Polsce_-_raport.pdf)

Każdy z wyznaczonych kierunków działań został uzupełniony listą konkretnych rekomendacji podzielonych na krótko i długookresowe. Zaprezentowano propozycję planu finansowania, a także działania strategiczne, które mogą podjąć poszczególne resorty.

Polityka Rozwoju Sztucznej Inteligencji w Polsce na lata 2019-2027

Rekomendacje z *Założeń* zostały uwzględnione i rozszerzone w dokumencie **Polityki Rozwoju Sztucznej Inteligencji w Polsce na lata 2019-2027**[243], wypracowanym przez międzyresortowy zespół analityczno-redakcyjny Ministerstwa Cyfryzacji oraz Ministerstwa Przedsiębiorczości i Technologii, ustanowiony

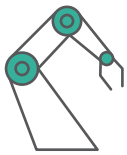
243 Konsultacje społeczne projektu *Polityki Rozwoju Sztucznej Inteligencji w Polsce na lata 2019 – 2027* (https://www.gov.pl/web/cyfryzacja/konsultacje-spoleczne-projektu-polityki-rozwoju-sztucznej-inteligencji-w-polsce-na-lata-2019–2027)

na podstawie memorandum zawartego w dniu 26 lutego 2019 roku przez Ministra Cyfryzacji, Ministra Przedsiębiorczości i Technologii, Ministra Nauki i Szkolnictwa Wyższego oraz Ministra Inwestycji i Rozwoju (czytaj więcej na str. 156). W dokumencie zauważono wyzwania, z jakimi boryka się Polska w kontekście rozwoju Sztucznej Inteligencji. Należą do nich:

Wyzwania Polski na drodze rozwoju Sztucznej Inteligencji

Personalizacja edukacji uniwersalnej – adaptacja systemu edukacyjnego do zmieniających się wymagań rynku pracy i zmian społecznych

Analfabetyzm cyfrowy – brak umiejętności korzystania z urządzeń i brak podstawowej wiedzy dotyczącej poruszania się w cyfrowym świecie



Bezrobocie technologiczne – zagrożenie automatyzacją najniżej wykwalifikowanych pracowników, wykonujących powtarzalne i rutynowe zadania

Polityka rekomenduje szereg działań, które mają podnieść świadomość w zakresie Sztucznej Inteligencji, wykształcić kulturę uczenia się przez całe życie, a także zwiększyć liczbę wysoko wykwalifikowanych specjalistów zajmujących się SI. Działania te są kierowane do uczniów i studentów, społeczeństwa, przedsiębiorców oraz administracji publicznej.

Wśród proponowanych rozwiązań znalazły się:

1. **Akademia Innowacyjnych Zastosowań Cyfrowych –** projekt skierowany do uczelni wyższych. Jego celem jest wykształcenie najwyższej klasy specjalistów w zakresie Sztucznej Inteligencji, uczenia maszynowego oraz cyberbezpieczeństwa (czytaj więcej na str 147).
2. **Wieloletni Program Rozwoju Talentów Informatycznych: *Mistrzostwa Algorytmiki i Programowania* –** program skierowany do młodych ludzi o ponadprzeciętnych zdolnościach matematycznych i algorytmicznych. Działanie będzie polegało na systemowym wsparciu w ramach edukacji pozaformalnej – wyjazdach edukacyjnych, zawodach drużynowych itp.
3. **Szkoła Doktorska Technologii Informacyjnych I Biomedycznych (TIB PAN) –** misją szkoły doktorskiej jest interdyscyplinarne kształcenie osób przygotowujących się do samodzielnego prowadzenia badań naukowych we wspólnym obszarze nauk technicznych, w tym informatyki, inżynierii biomedycznej, Sztucznej Inteligencji, cyberbezpieczeństwa oraz nauk medycznych. Projekt skierowany jest do młodych naukowców i badaczy.
4. **Doktoraty Wdrożeniowe AI –** program Doktoratów Wdrożeniowych nakierowanych na wyzwania AI, zarówno techniczne, jak i interdyscyplinarne. Program jest sposobem na połączenie wyzwań biznesu z zasobami nauki, a także metodą na zapewnienie wdrożeń wyników badań i wzmocnienia kadry naukowej w macierzystych ośrodkach akademickich lub instytutach badawczych.

Konsultacje Polityki Rozwoju Sztucznej Inteligencji w Polsce na lata 2019-2027 odbyły się drugim kwartale 2019 roku. Dokument spotkał się z krytycznym odbiorem przedsiębiorców, którzy widzą w nim raczej ocenę sytuacji gospodarczej Polski, a nie plan działania wspierający rozwój innowacyjności[244].

Zintegrowana Strategia Umiejętności 2030

Dokumentem strategicznym, który odnosi się bezpośrednio do umiejętności, jest ***Zintegrowana Strategia Umiejętności 2030***[245]**.** Część ogólna *Strategii* została przyjęta przez Radę Ministrów w styczniu 2019 roku[246]. Obecnie trwają prace nad częścią szczegółową.

Strategia koncentruje się na rozwoju umiejętności przekrojowych, które będą potrzebne na rynku pracy przyszłości i nie zagraża im proces automatyzacji. Należą do nich: umiejętności cyfrowe, umiejętność uczenia się przez całe życie, myślenie krytyczne, rozwiązywanie problemów, praca zespołowa i adaptacja do nowych warunków.

Umiejętności przekrojowe, które warunkują powodzenie w życiu społecznym i na rynku pracy przyszłości.

Źródło: Zintegrowana Strategia Umiejętności (część ogólna), s. 16

244 Puls Biznesu: *Narodowa strategia AI pod ostrzałem rynku* (https://www.pb.pl/narodowa-strategia-ai-pod-ostrzalem-rynku-970605)
245 *Zintegrowana Strategia Umiejętności 2030 (część ogólna)* (https://efs.men.gov.pl/wp-content/uploads/2019/08/Zintegrowana-Strategia-Umiej%C4%99tno%C5%9Bci-2030-cz%C4%99%C5%9B%C4%87-og%C3%B3lna.pdf)
246 Zobowiązanie do przyjęcia *Zintegrowanej Strategii Umiejętności* zostało zapisane w Umowie Partnerstwa, wpisuje się w działania Unii Europejskiej, OECD, ONZ, a także wymogi związane z zapisami krajowej *Strategii na rzecz Odpowiedzialnego Rozwoju i Systemu Zarządzania Rozwojem Polski.*

Nadrzędnym celem strategii jest **tworzenie możliwości i warunków do rozwoju umiejętności niezbędnych do wzmocnienia kapitału społecznego, włączenia społecznego, wzrostu gospodarczego i osiągnięcia wysokiej jakości życia.**

6 obszarów priorytetowych Zintegrowanej Strategii Umiejętności:

1. Podnoszenie poziomu umiejętności kluczowych u dzieci, młodzieży i osób dorosłych
2. Rozwijanie i upowszechnianie kultury uczenia się nastawionej na aktywny i ciągły rozwój umiejętności
3. Zwiększenie udziału pracodawców w rozwoju i lepszym wykorzystaniu umiejętności
4. Budowanie efektywnego systemu diagnozowania i informowania o obecnym stanie i zapotrzebowaniu na umiejętności
5. Wypracowanie skutecznych i trwałych mechanizmów współpracy i koordynacji międzyresortowej oraz międzysektorowej w zakresie rozwoju umiejętności
6. Wyrównywanie szans w dostępie do rozwoju i możliwości wykorzystania umiejętności

W *Zintegrowanej Strategii Umiejętności* dokonano diagnozy stanu edukacji w Polsce od wczesnej opieki i edukacji przedszkolnej, poprzez edukację szkolną, szkolnictwo wyższe, edukację pozaformalną i umiejętności osób dorosłych. Autorzy zwrócili uwagę na ograniczony zakres wykorzystywania nowoczesnych technologii w szkołach[247], czego powodem są niewystarczające kompetencje nauczycieli i brak oferty szkoleniowej dla nich. W szkolnictwie wyższym duże zmiany wprowadziła *Strategia na rzecz doskonałości naukowej, nowoczesnego szkolnictwa wyższego, partnerstwa z biznesem i społecznej odpowiedzialności nauki*[248]. Jednak największym wyzwaniem jest praca nad rozwojem umiejętności osób dorosłych. Niedobór specjalistów, w tym fachowców usług cyfrowych, stanowi jedną z barier wzrostu gospodarczego, a deficyty kadrowe są główną przeszkodą w prowadzeniu biznesu dla przedsiębiorców.

W ramach działań na rzecz edukacji pozaformalnej i kształcenia osób dorosłych, w 2016 roku Polska wdrożyła ***Zintegrowany System Kwalifikacji,*** który umożliwia walidację efektów uczenia się uzyskanych poza systemami oświaty i szkolnictwa wyższego[249].

247 Choć 90% nauczycieli deklaruje stosowanie technologii, najczęściej odbywa się to w celu komunikacji z rodzicami (elektroniczne dzienniki), albo w sposób frontalny (nauczyciel użytkuje sprzęt, a uczniowie biernie go obserwują).

248 W 2016 roku Ministerstwo Nauki i Szkolnictwa Wyższego ogłosiło *Strategię na rzecz doskonałości naukowej, nowoczesnego szkolnictwa wyższego, partnerstwa z biznesem i społecznej odpowiedzialności nauki*, która obejmuje 3 filary: Konstytucja dla Nauki, Innowacje dla gospodarki, Nauka dla Ciebie. Strategia ma przyczynić się do przezwyciężenia fragmentacji szkolnictwa wyższego, poszerzenia oferty dydaktycznej, większej mobilności naukowców, rosnącego zaangażowania społecznego uczelni, oraz wzmocnienia zarządzania i autonomii tych instytucji. Źródło: *Ogłoszenie Strategii Jarosława Gowina* (https://konstytucjadlanauki.gov.pl/prace-nad-reforma/ogloszenie-strategii-jaroslawa-gowina)

249 *Zintegrowany System Kwalifikacji* (http://kwalifikacje.edu.pl/)

Część ogólna Zintegrowanej Strategii Umiejętności kończy się wyznaczeniem celów strategicznych oraz wskazaniem kluczowych kierunków działań. Kolejnym etapem będzie opracowanie programów strategicznych wraz ze wskazaniem podmiotów odpowiedzialnych i źródeł finansowania, przy współpracy kluczowych interesariuszy.

Strategia umiejętności OECD: Polska

Strategia umiejętności OECD: Polska[250] została ogłoszona 11 grudnia 2019 roku. Raport powstał w ramach wsparcia OECD przy tworzeniu polskiego dokumentu strategicznego **– *Zintegrowanej Strategii Umiejętności.*** W diagnozie stanu umiejętności w Polsce OECD zastosowała ramy *Strategii Umiejętności OECD* (czytaj na stronie 122)[251]. W swoim raporcie OECD podkreśla, że Polska, podobnie jak pozostałe kraje, będzie musiała zmierzyć się z wpływem tzw. megatrendów czyli globalizacji, cyfryzacji i zmian demograficznych. Oznacza to, że obywatele będą potrzebowali solidnego i wszechstronnego zestawu umiejętności i lepszego ich dopasowania do zmieniającego się rynku pracy. Ze względu na zmniejszający się odsetek osób w wieku produkcyjnym, obniża się udział pracy jako czynnika wzrostu gospodarczego. Coraz większego znaczenia nabiera produktywność i metody jej zwiększania. Zmienia się również charakter zawodów, spowodowany głównie przez rozwój automatyzacji. OECD ocenia, że w Polsce ok. 31% pracowników jest zagrożonych utratą pracy z powodu automatyzacji, a 20% czekają istotne zmiany zawodowe spowodowane automatyzacją – to więcej niż średnia OECD[252]. Eksperci podkreślają, że aktualna sytuacja wzrostu gospodarczego Polski, niska stopa bezrobocia i wzrost zamożności dają naszemu krajowi wyjątkową szansę na wzmocnienie systemu umiejętności. W przyszłości Polska, w celu utrzymania konkurencyjności na rynku, będzie potrzebowała zwiększyć potencjał innowacji, który obecnie według wszystkich mierników pozostaje w tyle w stosunku do innych krajów. Konieczna jest zatem praca nad systemem, który w perspektywie długofalowej zapewni Polsce mocne podstawy dobrobytu gospodarczego i spójności społecznej.

Diagnoza polskiego systemu umiejętności wg. OECD

- Polska ma jeden z **najwyższych odsetków osób z co najmniej średnim wykształceniem** w przedziale wiekowym 25-34 lat.
- Wraz ze wzrostem liczby osób uzyskujących wyższe wykształcenie (44% osób w wieku 25-34) spadła jakość kształcenia. **Umiejętności absolwentów szkół wyższych plasują się poniżej lub na poziomie średniej OECD.**
- Przeciętne **umiejętności polskich dorosłych są poniżej poziomu krajów OECD,** szczególnie w obszarze umiejętności rozwiązywania problemów.
- Ok. 50% polskich dorosłych **nie ma żadnego doświadczenia lub ma jedynie ograniczone doświadczenie** w posługiwaniu się komputerem.
- Polska **ma bardzo niski wskaźnik kształcenia dorosłych.** Ok. 60% dorosłych nie uczestniczy i nie chce uczestniczyć w kształceniu albo szkoleniu.
- W 2017 roku 63% polskich pracodawców zgłaszało, że **problemy ze znalezieniem pracowników** o odpowiednich umiejęt-

250 *Strategia umiejętności OECD Polska. Wnioski i rekomendacje. Streszczenie Raportu* (http://ibe.edu.pl/download/MEN/Skills-strategy-poland-report-summary-PL.PDF)
251 Wyniki raportu zostały skonsultowane i przedyskutowane w ścisłej współpracy z polskimi interesariuszami, którzy uczestniczyli w warsztatach organizowanych przez Organizację wspólnie z Ministerstwem Edukacji Narodowej i Instytutem Badań Edukacyjnych w październiku 2018, lutym i maju 2019 roku. Źródło: *Zintegrowana Strategia Umiejętności* (https://www.ibe.edu.pl/pl/projekty-krajowe/zintegrowana-strategia-umiejetnosci)
252 *Strategia umiejętności OECD Polska. Wnioski i rekomendacje. Streszczenie Raportu* s. 7-8 (http://ibe.edu.pl/download/MEN/Skills-strategy-poland-report-summary-PL.PDF)

nościach stanowiły główną przeszkodę w inwestycjach.

- Polska ma jeden z **najniższych wskaźników wydatków na badania i rozwój** wśród krajów OECD.

Diagnoza stanu umiejętności w Polsce umożliwiła wskazanie 4 priorytetowych obszarów działania, które dotyczą dostosowania systemu edukacji do zapotrzebowania rynku pracy; kształcenia dorosłych; zwiększenia efektywności pracowników poprzez wykorzystanie umiejętności w czasie pracy; wzmocnienie zarządzania systemem umiejętności. OECD przedstawiło szczegółowe rekomendacje dla każdego z obszarów priorytetowych:

Priorytet 1: Zwiększenie sprawności reagowania systemu edukacji na potrzeby rynku pracy

- Rozszerzenie zakresu usług doradztwa zawodowego w instytucjach edukacyjnych.
- Wzmocnienie zachęt dla instytucji edukacyjnych w celu dostosowania ich oferty do potrzeb rynku pracy.
- Większe zachęty i wsparcie dla skutecznego nauczania.
- Wzmacnianie współpracy pomiędzy instytucjami edukacyjnymi a pracodawcami.

Priorytet 2: Wspieranie większego uczestnictwa we wszystkich formach uczenia się dorosłych

- Podnoszenie świadomości z korzyści i szans edukacji dorosłych.
- Zwiększenie elastyczności i dostępności kształcenia dorosłych.
- Szersze współfinansowanie i lepsze ukierunkowanie źródeł finansowania na uczenie się dorosłych.

Priorytet 3: Wzmocnienie wykorzystania umiejętności w polskich przedsiębiorstwach

- Podnoszenie świadomości na temat znaczenia skutecznego wykorzystania umiejętności i powiązanych praktyk HPWP[253].
- Wspieranie przedsiębiorstw i organizacji we wdrażaniu praktyk HPWP.
- Wyposażenie kadry kierowniczej we właściwe umiejętności potrzebne do wdrażania praktyk HPWP.
- Skuteczne angażowanie pracowników we wdrażanie praktyk HPWP.

Priorytet 4: Wzmocnienie zarządzania systemem umiejętności w Polsce

- Wzmocnienie współpracy w zakresie rozwiązań dotyczących umiejętności na poziomie krajowym.
- Wzmocnienie współpracy między różnymi poziomami administracji i współpracy regionalnej, w zakresie rozwiązań dotyczących umiejętności.
- Integracja i efektywne wykorzystanie informacji o umiejętnościach.

253 HPWP *(High-Performance Workplace Practices)* – zgodnie z definicją OECD na praktyki sprzyjające efektywności w miejscu pracy składają się: elastyczność i autonomia, praca zespołowa i wymiana informacji, szkolenia i rozwój, korzyści z pracy, rozwój kariery i zarządzanie wynikami (w tym perspektywy rozwoju zgodne z profilami kompetencji). Źródło: *OECD Skills Strategy Poland Assessment and Recommendations* s. 123

Finansowanie rozwoju kompetencji cyfrowych z programów europejskich

Fundusz	Finansowane działania
Program Operacyjny Polska Cyfrowa (POPC) 2014-2020 – III oś priorytetowa Cyfrowe kompetencje społeczeństwa	• Szkolenia dla osób dorosłych (ze szczególnym uwzględnieniem osób wykluczonych cyfrowo). • Naukę programowania dla dzieci. • Podnoszenie kompetencji cyfrowych i dydaktycznych nauczycieli. • Podnoszenie kompetencji pracowników instytucji kultury. • Budowanie zaawansowanych umiejętności specjalistów ICT. • Rozwój uzdolnień informatycznych wśród młodzieży.
Europejski Fundusz Społeczny (EFS) – w ramach *Regionalnych Programów Operacyjnych (RPO)*, a także *Programu Operacyjnego Wiedza Edukacja Rozwój (POWER)*	• Wyposażenie szkół w sprzęt komputerowy. • Budowę szkolnych sieci komputerowych. • Podnoszenie kompetencji cyfrowych nauczycieli i trenerów.

Wybrane inicjatywy w obszarze kompetencji cyfrowych w Polsce

W Polsce działa wiele inicjatyw w obszarze kompetencji cyfrowych, powołanych w ramach administracji rządowej, nauki, czy organizacji obywatelskich. Poniżej przedstawiono przykładowe.

Fundacja Platforma Przemysłu Przyszłości

6 lutego 2019 roku powołano Fundację Platforma Przemysłu Przyszłości[254] (czytaj więcej na stronie 154). Jednym z zadań Fundacji jest wzmacnianie kompetencji kadr dla przemysłu przyszłości poprzez szkolenia, a w szczególności:

- Prowadzenie działań na rzecz podnoszenia kapitału ludzkiego i społecznego;
- Informowanie i szkolenie przedsiębiorców i pracowników w zakresie cyfryzacji przemysłu;
- Wzmacnianie kompetencji pracowników dla przemysłu przyszłości poprzez współpracę z organizacjami prowadzącymi kształcenie techniczne.[255]

254 *Ustawa z dnia 17 stycznia 2019 roku o Fundacji Platforma Przemysłu Przyszłości* (http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20190000229/O/D20190229.pdf)
255 *Kierunek Przemysł 4.0* (https://przemyslprzyszlosci.gov.pl/co-robimy/)

Akademia Innowacyjnych Zastosowań Technologii Cyfrowych

20 listopada 2019 roku Ministerstwo Cyfryzacji podpisało list intencyjny z dziesięcioma uczelniami[256] wchodzącymi w skład konsorcjum projektu Akademii Innowacji Zastosowań Technologii Cyfrowych. Celem projektu jest wypracowanie modelu systemowego kształcenia najlepszej klasy specjalistów ICT na poziomie studiów wyższych. Realizacja projektu odbędzie się w latach 2020-2023 i przewidziano na nią 81 mln zł[257].

Szerokie Porozumienie na Rzecz Umiejętności Cyfrowych w Polsce

Od 2013 roku działa w Polsce Szerokie Porozumienie na Rzecz Umiejętności Cyfrowych[258]. Porozumienie jest nieformalną organizacją zrzeszającą instytucje oraz firmy, które zamierzają rozwijać kompetencje cyfrowe Polaków. Aktualnie do Porozumienia należy 80 organizacji. Co roku odbywa się konferencja z podsumowaniem działalności. Ostatnia miała miejsce 5 grudnia 2019 roku w NASK.

Program Ministerstwa Obrony Narodowej – CYBER.MIL.PL

W lutym 2019 roku Ministerstwo Obrony Narodowej uruchomiło program CYBER.MIL.PL. Głównym zadaniem programu jest zwiększenie bezpieczeństwa państwa i obywateli w cyberprzestrzeni, ale również edukacja i szkolenia. Do zrealizowanych dotychczas działań należą:

- Zwiększenie limitu przyjęć na uczelniach wojskowych na kierunkach związanych z bezpieczeństwem informacyjnym (celem jest wyszkolenie 2 tys. oficerów cyberbezpieczeństwa w ciągu 5 lat).
- Uruchomienie studiów inżynierskich na kierunku informatyka w Akademii Wojsk Lądowych (rok akademicki 2020/2021).
- Utworzenie Wojskowego Ogólnokształcącego Liceum Informatycznego przy Wojskowej Akademii Technicznej.
- Uruchomienie pierwszych w Polsce studiów MBA z zarządzania cyberbezpieczeństwem na Wojskowej Akademii Technicznej.
- Start programu „CYBER.MIL z klasą", skierowanego do szkół średnich. Wybrane placówki otrzymają od Ministerstwa Obrony Narodowej dofinansowanie na wyposażenie sali informatycznej (maks. 200 tys. złotych) i wynagrodzenia dla nauczycieli przedmiotów specjalistycznych (maks. 60 tys. zł rocznie)[259].

256 Do konsorcjum należą: Uniwersytet Warszawski (Wydział Matematyki, Informatyki i Mechaniki), Uniwersytet Jagielloński w Krakowie (Wydział Fizyki, Astronomii i Informatyki Stosowanej, Wydział Matematyki i Informatyki), Uniwersytet Wrocławski (Wydział Matematyki i Informatyki), Uniwersytet im. Adama Mickiewicza w Poznaniu (Wydział Matematyki i Informatyki), Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie (Wydział Informatyki, Elektroniki i Telekomunikacji, Wydział Elektrotechniki, Automatyki, Informatyki i Inżynierii Biomedycznej, Wydział Fizyki i Informatyki Stosowanej), Politechnika Warszawska (Wydział Elektroniki i Technik Informacyjnych, Wydział Matematyki i Nauk Informacyjnych), Politechnika Wrocławska (Wydział Informatyki i Zarządzania, Wydział Elektroniki), Politechnika Gdańska (Wydział Elektroniki, Telekomunikacji i Informatyki, Politechnika Poznańska (Wydział Informatyki), Wojskowa Akademia Techniczna (Wydział Cybernetyki). Źródło: *Będziemy kształcić najlepszych specjalistów cyfrowej gospodarki* (https://www.gov.pl/web/cyfryzacja/bedziemy-ksztalcic-najlepszych-specjalistow-cyfrowej-gospodarki)

257 W ramach funduszy ponad 500 studentów otrzyma możliwość uzyskania stypendiów zagranicznych, nawiązanie współpracy międzynarodowej z wiodącymi uczelniami i przedsiębiorstwami, a także dofinansowanie do przedsięwzięć naukowo-wdrożeniowych realizowanych przez uczelnie we współpracy z biznesem i administracją.

258 *Szerokie Porozumienie na rzecz Umiejętności Cyfrowych w Polsce* (http://umiejetnoscicyfrowe.pl/)

259 *Cyber.Mil.Pl 2019* (*https://www.gov.pl/attachment/53f813c7-5f3f-4d20-874e-58937d7fcaeb*)

Podsumowanie

Szybki rozwój nowoczesnych technologii wymaga dostosowania się pracowników, pracodawców, ale i obywateli do nowej rzeczywistości. Dotychczasowa wiedza, zdobywana w tradycyjnych systemach edukacyjnych, przestała spełniać współczesne oczekiwania, a brak wiedzy z obszaru nowoczesnych technologii i cyfryzacji stanowi przeszkodę na drodze do rozwoju. Z biegiem czasu zaczynamy rozumieć, że w technologicznym wyścigu zbrojeń kompetencje odgrywają równie ważną rolę jak sama technologia. Ważne bowiem, aby na etapie wdrożenia danej technologii znaleźli się ludzie, którzy będą potrafili z nią pracować, rozwijać ją, ale również wykorzystywać w codziennym życiu. Kwestię tę rozumieją organizacje międzynarodowe, które nawołują do podjęcia działań na rzecz dostosowania edukacji do ery cyfrowej. Rekomendacje podpierają wynikami badań diagnozujących poziom kompetencji w poszczególnych krajach. Prowadzą również obserwacje trendów światowych i na ich podstawie przewidują możliwe zmiany w obszarze przemian rynku pracy, nowych zawodów, nowych form zatrudnienia i cyfrowym stylu życia. W publikowanych wytycznych zachęcają państwa do proaktywnych postaw w celu przygotowania się na te zmiany.

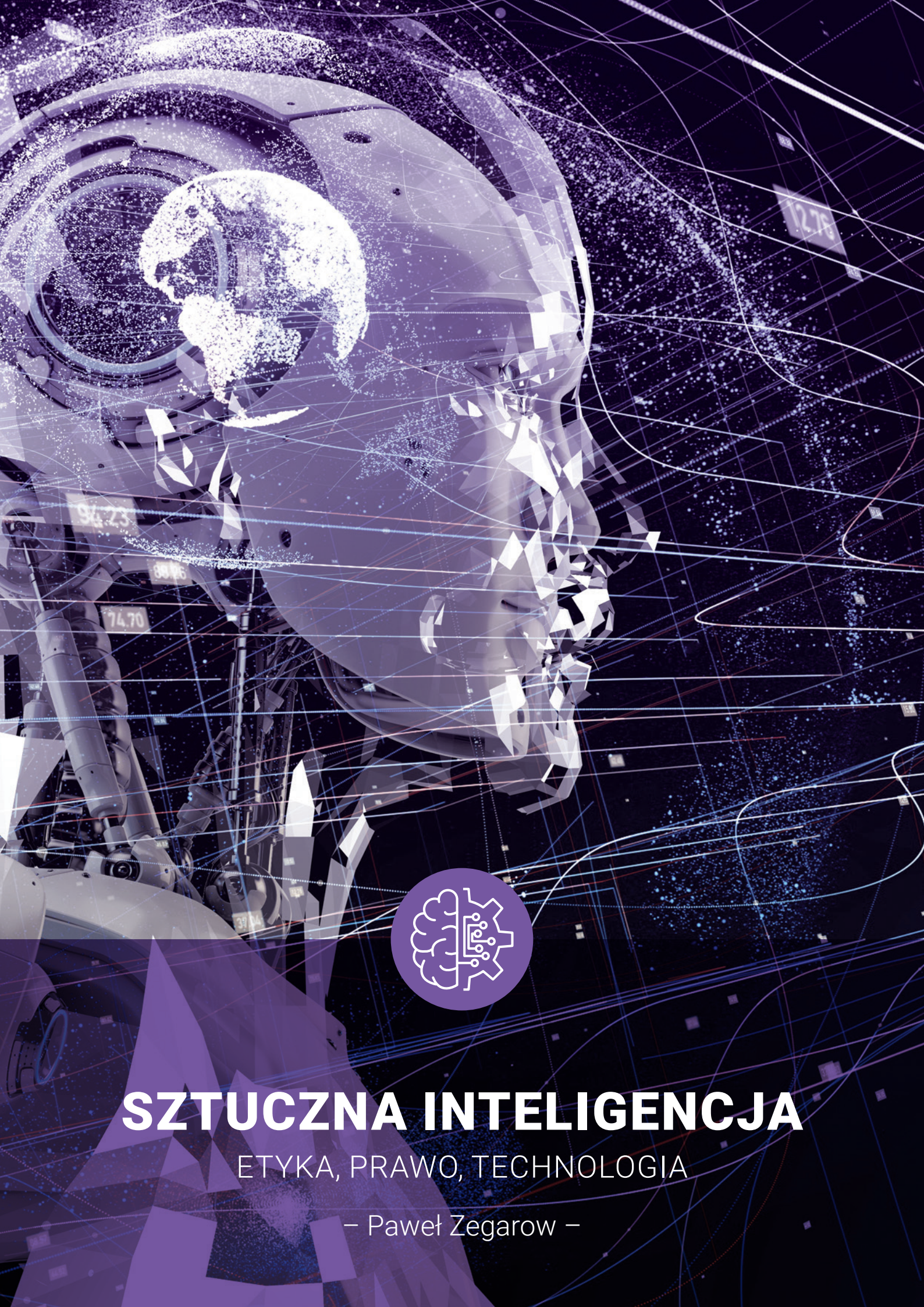
Konkretne działania podejmuje również Unia Europejska, która już w 2010 roku zdefiniowała obszar kompetencji jako kluczowy na drodze do budowania silnej i innowacyjnej gospodarki cyfrowej. Uchwalona wówczas *Europejska Agenda Cyfrowa* zaproponowała priorytetowe obszary działalności, wśród których znalazła się zapowiedź stworzenia jednolitego rynku cyfrowego, zwiększenia zaufania i dostępu do Internetu, a także rozwoju umiejętności wykorzystywania technologii cyfrowych wśród wszystkich obywateli Europy. Wdrożenie tych postulatów zakończy się w 2020 roku, natomiast rok 2021 otworzy nową perspektywę, w której kompetencje cyfrowe nadal będą zajmowały priorytetowe miejsce. Na ich wzmacnianie zaplanowano fundusze w programie *Cyfrowa Europa 2021-2027, Nowym Europejskim Funduszu Socjalnym, Europejskim Funduszu Dostosowania do Globalizacji i nowym Horyzoncie 2021-2027*. W opublikowanej w lutym 2020 roku strategii cyfrowej UE, KE zapowiedziała opracowanie planu działania w sprawie edukacji cyfrowej i wzmocnienie *Europejskiej Agendy Cyfrowej*. Dokumenty te mają pojawić się w drugim kwartale 2020 roku i wyznaczą perspektywę UE w obszarze edukacji w nowoczesnych technologiach na kolejne lata.

Potrzeba rozwoju kompetencji cyfrowych jest widoczna również w Polsce. Wyniki z ostatniego indeksu *DESI* pokazują, że podejmowane dotychczas działania są niewystarczające. Eksperci OECD, w diagnozie przygotowanej dla Polski w związku z pracami nad *Zintegrowaną Strategią Umiejętności,* wskazują 4 priorytetowe obszary do poprawy:

- Priorytet 1: Zwiększenie sprawności reagowania systemu edukacji na potrzeby rynku pracy.
- Priorytet 2: Wspieranie większego uczestnictwa we wszystkich formach uczenia się dorosłych.
- Priorytet 3: Wzmocnienie wykorzystania umiejętności w polskich przedsiębiorstwach.

- Priorytet 4: Wzmocnienie zarządzania systemem umiejętności w Polsce.

OECD zwraca uwagę na niski potencjał innowacji Polski, który według wszystkich mierników pozostaje w tyle w stosunku do innych krajów. W połączeniu z niskim poziomem umiejętności cyfrowych Polaków istnieje ryzyko spadku konkurencyjności Polski na rynku międzynarodowym w przyszłości. Eksperci wskazują, że należałoby wykorzystać obecną dobrą sytuację gospodarczą (wzrost gospodarczy, niska stopa bezrobocia, wzrost zamożności obywateli) jako szansę na wzmocnienie poziomu umiejętności, który jest niezbędny dla dalszego rozwoju kraju. Odpowiedzią na to zapotrzebowanie są prace nad częścią szczegółową *Zintegrowanej Strategii Umiejętności,* a także *Program Rozwoju Kompetencji Cyfrowych do roku 2030,* który jest przygotowywany przez Ministerstwo Cyfryzacji.



SZTUCZNA INTELIGENCJA

ETYKA, PRAWO, TECHNOLOGIA

– Paweł Zegarow –

Sztuczna Inteligencja staje się obszarem o priorytetowym znaczeniu dla państw świadomych potencjału nowych technologii. Inwestycje w rozwój SI umożliwią nie tylko poprawę jakości życia obywateli, ale będą także warunkiem utrzymania suwerenności państwa. Technologie wykorzystujące SI już za kilka lat mogą rozwiązać wiele społecznych problemów: od szybkiego diagnozowania chorób przewlekłych i poprawienia bezpieczeństwa transportu, aż po walkę ze zmianami klimatycznymi, zapobieganie incydentom w cyberprzestrzeni czy też wykrywanie nadużyć finansowych.

Dynamiczny rozwój nowych technologii budzi jednak pewien społeczny niepokój. Wszystko za sprawą trudnego do przewidzenia ryzyka związanego z ich powszechnym wykorzystaniem i wpływem na otaczającą nas rzeczywistość. Dla globalnych liderów w dziedzinie SI, jakimi są Stany Zjednoczone Ameryki Północnej i Chiny, Sztuczna Inteligencja jest obszarem o strategicznym znaczeniu społecznym i gospodarczym. Mimo że strategie rozwoju SI obu państw podkreślają kwestie etyczne, to nie wykluczone, że w przyszłości Sztuczna Inteligencja będzie wykorzystana do budowy przewagi militarnej. Istnieją uzasadnione obawy, że deklaracje chińskiego rządu w sprawie etyki SI mogą znacznie różnić się od realnych działań podejmowanych w tym obszarze. Z tego powodu rywalizacja między wymienionymi wcześniej liderami przenosi się z ośrodków akademickich na arenę międzynarodową. Jednym z przykładów takich działań są intensywne prace administracji USA nad wprowadzeniem coraz bardziej restrykcyjnych regulacji ograniczających eksport rozwiązań opartych na Sztucznej Inteligencji do Chin i innych państw konkurujących[260]. W ten sposób rząd USA chce ograniczyć ryzyko udoskonalania własnej technologii poza granicami kraju[261].

Warto podkreślić, że Unia Europejska w ciągu ostatnich dwóch lat poczyniła istotne postępy w kwestii regulacji, strategii rozwoju i etyki Sztucznej Inteligencji. Analizując dokumenty źródłowe i sytuację geopolityczną wydaje się, że ochrona przewagi konkurencyjnej i obawa przed przejęciem przełomowych rozwiązań w dziedzinie Sztucznej Inteligencji przez autokratyczne reżimy jest motorem napędowym regulacji w UE i USA.

Mimo że w literaturze naukowej istnieje wiele definicji Sztucznej Inteligencji, to obecnie nie obowiązuje jedna oficjalna definicja tego pojęcia. Wśród najczęściej spotykanych wyjaśnień, SI odnosi się do specjalistycznej dziedziny wiedzy, która rozwija się na gruncie robotyki, logiki, sieci neuronowych, a także nauk społecznych, jak ekonomia, psychologia i filozofia. SI jest również kojarzona z odrębną dziedziną badań naukowych lub z działem informatyki zajmującym się tworzeniem programów, naśladujących działanie ludzkiego umysłu. Potocznie termin Sztuczna Inteligencja bywa rozumiany jako rodzaj nowej technologii.

Twórcą terminu Sztuczna Inteligencja *(Artificial Intelligence, AI)* jest amerykański informatyk John McCarthy. Naukowiec ten w 1956 roku zorganizował w Dartmouth pierwszą konferencję naukową poświęconą Sztucznej Inteligencji. Rozwój tej dziedziny rozpoczął się jednak znacznie wcześniej. Pierwsze prace teoretyczne na temat tworzenia inteligentnych maszyn zostały zapoczątkowane w połowie XX wieku przez brytyjskiego matematyka Alana Methisona Turinga. Turing już w 1935 roku opisał abstrakcyjną maszynę zdolną

260 *Addition of Software Specially Designed To Automate the Analysis of Geospatial Imagery to the Export Control Classification Number 0Y521 Series* (https://www.federalregister.gov/documents/2020/01/06/2019-27649/addition-of-software-specially-designed-to-automate-the-analysis-of-geospatial-imagery-to-the-export)

261 *U.S. government limits exports of artificial intelligence software* (https://www.reuters.com/article/us-usa-artificial-intelligence/u-s-government-limits-exports-of-artificial-intelligence-software-idUSKBN1Z21PT)

do wykonywania wcześniej zaprogramowanych operacji matematycznych – prototyp dzisiejszego komputera. Piętnaście lat później Turing opublikował kolejną pracę zatytułowaną *Computing Machinery and Intelligence*[262], w której opisał nie tylko proces tworzenia inteligentnej maszyny, ale także sposób testowania jej inteligencji. Innowacyjne koncepcje Turinga były impulsem dla środowiska akademickiego do rozpoczęcia badań nad Sztuczną Inteligencją.

W ciągu ostatnich 70 lat naukowcy poczynili istotne postępy w zakresie doskonalenia algorytmów odpowiedzialnych za integrację analiz statystycznych i uczenie maszynowe. Przejawy działania Sztucznej Inteligencji możemy zaobserwować w codziennym życiu np. korzystając z filtru antyspamowego, który bez naszej wiedzy wyszukuje w treści wiadomości charakterystycznego dla spamu ciągu znaków, słów lub całych zdań. Kolejnym przykładem jest asystent głosowy w smartfonie, który odpowiada na proste pytania, informuje o pogodzie, kierunku jazdy lub terminie nadchodzącego spotkania.

Sztuczna Inteligencja posiada ogromny potencjał, który z jednej strony może zmienić świat na lepszy, a z drugiej strony może zwiększyć ryzyko wystąpienia nieznanych wcześniej zagrożeń. Największe kontrowersje dotyczą uczciwości i odpowiedzialności SI. Dlatego też Unia Europejska i inne organizacje międzynarodowe dążą do ustanowienia racjonalnej strategii rozwoju Sztucznej Inteligencji oraz określenia ram prawnych gwarantujących etyczny i bezpieczny rozwój. Niniejszy rozdział opisuje działania w tym zakresie podejmowane w Polsce, Unii Europejskiej i na świecie.

Polska

Polski rząd od blisko trzech lat stara się wypracować strategię rozwoju Sztucznej Inteligencji. Wydarzeniem, które wyznaczyło kierunek prac w tym obszarze, było podpisanie 10 kwietnia 2018 roku przez Polskę oraz państwa z Grupy Wyszehradzkiej (V4) wspólnego stanowiska w sprawie rozwoju Sztucznej Inteligencji. W listopadzie 2018 roku Ministerstwo Cyfryzacji opublikowało *Założenia do strategii AI w Polsce*. Dokument zawierał opis najważniejszych zagadnień i rekomendacji międzyresortowych służących rozwojowi Sztucznej Inteligencji. Należy podkreślić, że mimo wysiłków podejmowanych przez międzyresortowe zespoły, obecnie w naszym kraju nie obowiązują regulacje dotyczące Sztucznej Inteligencji. Ogłoszony 21 sierpnia 2019 roku projekt *Polityki Rozwoju Sztucznej Inteligencji w Polsce na lata 2019-2027*[263] spotkał się z krytyką ze strony lokalnych instytucji i ekspertów zaangażowanych w rozwój Sztucznej Inteligencji.

262 Turing, A. M. (2009). *Computing machinery and intelligence. In Parsing the Turing Test* (pp. 23-65). Springer, Dordrecht.
263 Projekt został opracowany przez międzyresortowy zespół analityczno-redakcyjny, ustanowiony na podstawie memorandum Ministra Cyfryzacji, Ministra Przedsiębiorczości i Technologii, Ministra Nauki i Szkolnictwa Wyższego oraz Ministra Inwestycji i Rozwoju.

Najważniejsze wydarzenia z obszaru Sztucznej Inteligencji w Polsce w 2019 roku:

22-23 stycznia

Konferencja *Mapa Drogowa Sztucznej Inteligencji w Polsce* w MPiT.

17 marca

Przyjęcie ustawy powołującej Fundację Platforma Przemysłu Przyszłości (FPPP).

26 maja

Podpisanie memorandum na rzecz rozwoju Sztucznej Inteligencji przez Ministra Cyfryzacji, Ministra Inwestycji i Rozwoju, Ministra Nauki i Szkolnictwa Wyższego oraz Ministra Przedsiębiorczości i Technologii.

2 lipca

Zaprezentowanie raportu *IoT w polskiej gospodarce*, przygotowanego przez grupę roboczą do spraw Internetu Rzeczy działającą przy Ministerstwie Cyfryzacji.

21 sierpnia

Ogłoszenie konsultacji społecznych projektu *Polityki Rozwoju Sztucznej Inteligencji w Polsce na lata 2019-2027.*

31 sierpnia

Inauguracja Wirtualnej Katedry Etyki i Prawa.

4-5 września

Forum Cyberbezpieczeństwa zorganizowane przez Ministerstwo Cyfryzacji i NASK podczas XXIX Forum Ekonomicznego w Krynicy-Zdroju.

Konferencja Mapa Drogowa Sztucznej Inteligencji w Polsce

W dniach 22-23 stycznia 2019 roku w Ministerstwie Przedsiębiorczości i Technologii odbyła się konferencja *Mapa Drogowa Sztucznej Inteligencji w Polsce.* Wydarzenie było okazją do integracji środowiska zajmującego się SI oraz dyskusji na temat szans, wyzwań i zagrożeń związanych z rozwojem tej dziedziny w Polsce. Podczas konferencji miały również miejsce debaty i warsztaty z udziałem polskich i zagranicznych ekspertów reprezentujących środowiska akademickie, administrację publiczną, biznes, a także przedstawicieli społeczeństwa obywatelskiego.

Fundacja Platforma Przemysłu Przyszłości

17 marca 2019 roku przyjęto ustawę powołującą Fundację Platforma Przemysłu Przyszłości (FPPP) z siedzibą w Radomiu[264]. Utworzenie FPPP wynikało z realizacji postulatów zawartych w *Strategii na rzecz Odpowiedzialnego Rozwoju*[265] przyjętej przez Radę Ministrów 14 lutego 2017 roku. Powołanie FPPP, której celem jest wspieranie polskich przedsiębiorstw w dostosowaniu się do wymagań ery Przemysłu 4.0, ma ułatwić modernizację poprzez zastępowanie dużego zapotrzebowania na surowce, energię i siłę roboczą, odkryciami naukowymi i wysoko wykwalifikowanymi pracownikami. Fundatorem FPPP jest Skarb Państwa, reprezentowany przez ministra właściwego do spraw gospodarki. Działania są finansowane z dotacji celowych i podmiotowych. W przyszłości fundacja ma integrować i wspierać działania na rzecz transformacji cyfrowej Polski[266].

Memorandum na rzecz rozwoju Sztucznej Inteligencji w Polsce

26 maja 2019 roku Minister Cyfryzacji, Minister Inwestycji i Rozwoju, Minister Nauki i Szkolnictwa Wyższego oraz Minister Przedsiębiorczości i Technologii podpisali memorandum na rzecz rozwoju Sztucznej Inteligencji w Polsce. Celem wielostronnej umowy było wspólne zaangażowanie w prace nad utworzeniem strategicznych ram dla dynamicznego rozwoju technologii i szerokich zastosowań SI w Polsce.

W deklaracji szefowie resortów zobowiązali się do:

- Zaangażowania w działania dotyczące rozwoju Sztucznej Inteligencji w Polsce.
- Podjęcia skoordynowanych działań na rzecz szerokiego wyposażenia obywateli w kompetencje z zakresu *data science*.
- Wypracowania Mapy drogowej Rozwoju Sztucznej Inteligencji w Polsce, w oparciu o międzyresortowy zespół roboczy.
- Zaprezentowania 21 maja 2019 roku ram Mapy drogowej Sztucznej Inteligencji.
- Uwzględnienia w Strategii Produktywności długofalowej perspektywy rozwoju Sztucznej Inteligencji, w tym koncepcji Szkoły Głównej Kompetencji Cyfrowych.
- Zaprezentowania w czerwcu 2019 roku na forum Unii Europejskiej spójnej polityki krajowej wspierającej Zintegrowany Plan na Rzecz Rozwoju Sztucznej Inteligencji w UE.
- Zaprojektowania krajowych instrumentów wsparcia w ramach nowej perspektywy finansowej UE, która zapewni realizację celów określonych w Strategii Produktywności oraz Mapie drogowej Rozwoju Sztucznej Inteligencji.

264 http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20190000229/T/D20190229L.pdf
265 Dokument opisujący średnio- i długofalową politykę gospodarczą zakładał, że reindustrializacja przemysłu jest ważnym filarem nowego modelu rozwoju polskiej gospodarki. (https://archiwum.miir.gov.pl/strony/strategia-na-rzecz-odpowiedzialnego-rozwoju/informacje-o-strategii/)
266 https://www.gov.pl/attachment/1f6e4ba8-20ea-4743-80ed-29a9e372f48c

Konferencja Internet Rzeczy – Polska Przyszłości

2 lipca 2019 roku podczas konferencji *Internet Rzeczy – Polska Przyszłości*, grupa robocza do spraw Internetu Rzeczy działająca przy Ministerstwie Cyfryzacji zaprezentowała raport *IoT w polskiej gospodarce*. Raport opisał aktualny stan instytucjonalno-prawny oraz otoczenie biznesowe branży IoT w Polsce. Autorzy wskazali szereg problemów i barier wspólnych dla wszystkich branż, które spowalniają rozwój Internetu Rzeczy w Polsce. Dokument opisał również zestaw rekomendacji, których wdrożenie zdaniem ekspertów przyniesie polskiej gospodarce i społeczeństwu istotne korzyści.

W raporcie znalazły się także definicje Internetu Rzeczy (IoT), opisujące zagadnienie z trzech różnych perspektyw. Zdaniem ekspertów termin Internet Rzeczy odnosi się do:

- Ekosystemu biznesowego, który umożliwia świadczenie usług przetwarzania danych i ich interoperacyjnego wykorzystania w środowisku biznesowym.
- Internetu wszystkiego, czyli wszystkich urządzeń i produktów konsumenckich podłączonych do Internetu, które w przyszłości będą współpracowały ze sobą poprzez aplikacje zwiększające ich funkcjonalność.
- Internetu Rzeczy rozumianego, jako sieć fizycznych obiektów, które komunikują się ze sobą, obserwują zjawiska, wpływają na stan wewnętrzny obiektów i wpływają na ich otoczenie.

Grupa robocza do spraw Internetu Rzeczy rozpoczęła pracę 24 sierpnia 2018 roku. W skład grupy wchodzą eksperci reprezentujący środowiska akademickie, biznesowe oraz instytucje państwowe. Celem grupy jest wypracowanie rekomendacji działań, jakie rząd RP powinien podjąć dla zapewnienia warunków rozwoju i upowszechnienia wykorzystania technologii IoT, a także zagwarantowania przewagi konkurencyjnej polskiej gospodarki na rynkach międzynarodowych.

Rekomendacje Grupy roboczej do spraw Internetu Rzeczy:

- Poprawa koordynacji działań agencji rządowych w kontekście IoT i innych nowoczesnych technologii.
- Stworzenie i uruchomienie programu finansowania wdrożeń pilotażowych i referencyjnych dla innowacyjnych rozwiązań IoT o dużym potencjale umiędzynarodowienia (tworzonych zarówno przez startupy IoT, jak i firmy dojrzałe).
- Uregulowanie możliwości wymiany lub komercjalizacji informacji uzyskanych na bazie IoT, w zakresie, który nie narusza podstawowych zasad ochrony danych osobowych, tajemnic sektorowych lub zawodowych.
- Promocja dobrych praktyk i prekursorskich rozwiązań, np. w formie organizowanych przez rząd konkursów wyróżniających wzorcowe firmy IoT.

- Stworzenie programów wspierających jednostki publiczne na poziomie centralnym (finansowanie, wsparcie przy wyborze technologii i wdrażaniu).
- Zwiększenie transparentności działań organów nadzorczych, w tym – w przypadkach, gdy dana kwestia leży w zakresie właściwości kilku z nich – wydawanie wspólnych jednoznacznych objaśnień, będących efektem konsultacji społecznych i uzgodnień między organami.
- Wprowadzenie ulg podatkowych za stosowanie rozwiązań IoT.

Inauguracja Wirtualnej Katedry Etyki i Prawa

31 sierpnia 2019 roku Minister Cyfryzacji zainaugurował działalność Wirtualnej Katedry Etyki i Prawa. To pierwsza tego typu jednostka w Polsce i w Europie zrzeszająca przedstawicieli nauk ścisłych i prawnych. Głównymi zadaniami Wirtualnej Katedry Etyki i Prawa są monitorowanie i prowadzenie badań na temat prawnych i etycznych aspektów Sztucznej Inteligencji w powiązaniu z nowymi technologiami. Jednostka została powołana na podstawie wielostronnego porozumienia, które podpisali: Minister Cyfryzacji, reprezentanci NASK, Polskiej Akademii Nauk oraz uczelni wyższych[267]. Jednak do dnia publikacji niniejszego raportu jednostka nie poinformowała publicznie o zakresie i efektach prowadzonych prac.

Konsultacje projektu Polityki Rozwoju Sztucznej Inteligencji w Polsce na lata 2019-2027

Polski rząd od blisko trzech lat stara się stworzyć strategię rozwoju Sztucznej Inteligencji. 21 sierpnia 2019 roku Ministerstwo Cyfryzacji ogłosiło konsultacje społeczne projektu *Polityki Rozwoju Sztucznej Inteligencji w Polsce na lata 2019-2027*. Liczący 117 stron projekt został opracowany przez międzyresortowy zespół analityczno-redakcyjny, ustanowiony na podstawie memorandum Ministra Cyfryzacji, Ministra Przedsiębiorczości i Technologii, Ministra Nauki i Szkolnictwa Wyższego oraz Ministra Inwestycji i Rozwoju.

Projekt *Polityki Rozwoju Sztucznej Inteligencji w Polsce na lata 2019-2027* został przygotowany w taki sposób, aby zachować spójność z działaniami podejmowanymi przez Unię Europejską i OECD w obszarze SI, a także aby uwzględniać dokumenty strategiczne tych organizacji.

Opisana w dokumencie wizja rozwoju Sztucznej Inteligencji w Polsce zakłada wzmocnienie świadomości człowieka i jego autonomii w relacjach z systemami wykorzystującymi SI, ochronę uczciwej konkurencji oraz zapewnienie suwerenności państwa.

Na szczególną uwagę zasługuje precyzyjnie zdefiniowany i ambitny cel dla Polski, która do roku 2025 ma dołączyć do grona 20-25% państw wiodących w rozwoju Sztucznej Inteligencji na świecie. Oznacza to, że w ciągu najbliższych 5 lat przedsiębiorstwa rozwijające SI muszą zwiększyć swoją wielkość blisko 25 razy. Biorąc pod uwagę aktualne tempo zmian i rozwoju Sztucznej Inteligencji w Polsce, cel ten wydaje się niezwykle trudny do zrealizowania.

267 Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego, Uniwersytetu w Białymstoku, Uniwersytetu Kardynała Stefana Wyszyńskiego, Uniwersytetu Łódzkiego, Uniwersytetu Opolskiego, Uniwersytetu Śląskiego w Katowicach, Uniwersytetu Warszawskiego i Politechniki Warszawskiej.

Celami *Polityki Rozwoju Sztucznej Inteligencji w Polsce na lata 2019-2027* są:

Wzrost inwestycji w cyfryzację przemysłu i usług wykorzystujących Sztuczną Inteligencję

Efektywne finansowanie badań naukowych

Zmniejszenie odpływu specjalistów za granicę

Moderowanie wpływu SI na rynek pracy

Zniwelowanie ryzyk zakłócenia autonomii człowieka i podejmowania świadomych decyzji w korzystaniu z SI

Autorzy projektu podkreślają, że rozwój Sztucznej Inteligencji musi być połączony ze wzmacnianiem autonomii człowieka i jego nadrzędnej roli w stosunku do technologii. Ich zdaniem, tempo i kierunek rozwoju SI w Polsce będą miały istotny wpływ na gospodarczą suwerenność naszego państwa. Budowanie dobrobytu obywateli i odpowiedzialny rozwój Polski wiąże się z inwestycjami w rozwój Sztucznej Inteligencji. W przeciwnym wypadku Polska uzależni się od zagranicznych technologii.

Projekt spotkał się z krytyką ze strony ekspertów zaangażowanych w rozwój Sztucznej Inteligencji w Polsce, którzy uznali, że ma więcej wspólnego z opisem bieżącej sytuacji gospodarczej niż z konkretnym planem działania[268]. Eksperci poddali również w wątpliwość słuszność założeń leżących u podstaw projektu, a także realną możliwość osiągniecia założonych celów. Zwrócono także uwagę na to, że polskie regulacje i inicjatywy są znacznie mniej zaawansowane niż działania Niemiec czy Francji w obszarze SI.

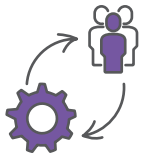
Unia Europejska

Sztuczna Inteligencja stosunkowo niedawno stała się obszarem o strategicznym znaczeniu dla rozwoju społeczeństwa i gospodarki Unii Europejskiej. W porównaniu do światowych liderów w dziedzinie rozwoju SI, jakimi są USA i Chiny, europejskie państwa są na początkowym etapie rozwoju tej dziedziny. Prace nad tzw. europejską Sztuczną Inteligencją rozpoczęły się w 2018 roku. Wydarzeniem, które wyznaczyło wspólny kierunek rozwoju SI w Europie, było podpisanie 10 kwietnia 2018 roku przez 25 państw członkowskich wspólnej deklaracji *Współpraca w zakresie Sztucznej Inteligencji.* Kilka dni później Komisja Europejska w komunikacie *Sztuczna Inteligencja dla Europy* przedstawiła wizję rozwoju opartą na trzech filarach:

Trzy filary europejskiej Sztucznej Inteligencji zawarte w komunikacie KE *Sztuczna Inteligencja dla Europy*

Zwiększenie inwestycji publicznych i prywatnych w SI w celu jej szerszego rozpowszechnienia

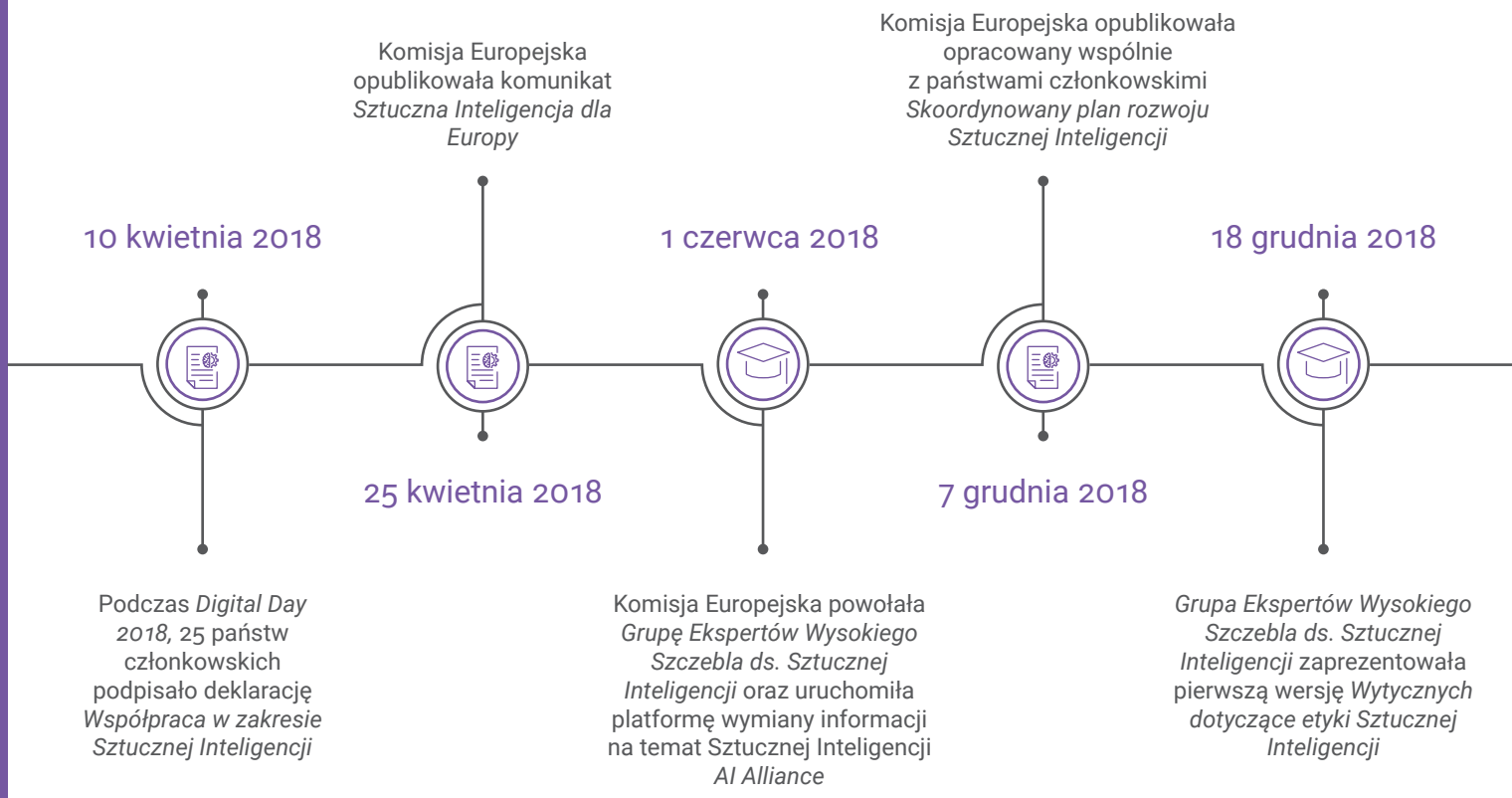
268 https://www.pb.pl/narodowa-strategia-ai-pod-ostrzalem-rynku-970605



Przygotowanie się na zmiany społeczno-gospodarcze

Zapewnienie odpowiednich ram etycznych i prawnych, wzmacniających europejskie wartości

Kolejnymi działaniami KE było powołanie Grupy Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji *(High-Level Expert Group on Artificial Intelligence, AI HLEG),* której zadaniem było wsparcie prac KE wiedzą ekspercką[269], oraz opublikowanie *Skoordynowanego planu rozwoju Sztucznej Inteligencji.* Obecne działania KE koncentrują się na tworzeniu sprzyjającego ekosystemu i wytycznych, które będą promować europejskie wartości w SI.



Działania Grupy Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji

1. Wytyczne dotyczące etyki godnej zaufania Sztucznej Inteligencji

8 kwietnia 2019 roku Grupa Ekspertów *AI HLEG* opublikowała ostateczną wersję *Wytycznych dotyczących etyki godnej zaufania sztucznej inteligencji (The Ethics Guidelines for Trustworthy Artificial Intelligence).* Pierwszy projekt dokumentu był przedmiotem konsultacji publicznych, które trwały od grudnia 2018 roku. Opublikowane wytyczne utworzyły horyzontalne ramy na potrzeby promowania i wdrażania godnej zaufania Sztucznej Inteligencji w Unii Europejskiej, a także wspierania

269 Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (High-Level Expert Group on Artificial Intelligence, AI HLEG) – w skład grupy wchodzi 52 niezależnych ekspertów, reprezentantów różnych krajów, przedstawicieli środowiska akademickiego, społeczeństwa obywatelskiego i biznesu. Grupa ekspertów wspiera Komisję Europejska w procesie wdrażania strategii dla Sztucznej Inteligencji w Unii Europejskiej.

badań naukowych w tym obszarze. Według ekspertów dokument ten należy regularnie aktualizować, aby zapewnić adekwatność wytycznych w świetle zachodzących zmian społeczno-gospodarczych i zwiększającego się poziomu wiedzy.

W pierwszej części dokument koncentruje się na **czterech kluczowych zasadach etycznych,** które powinna spełniać technologia korzystająca ze Sztucznej Inteligencji:

Poszanowanie autonomii człowieka

Zapobieganie szkodom

Sprawiedliwość

Możliwość wyjaśnienia

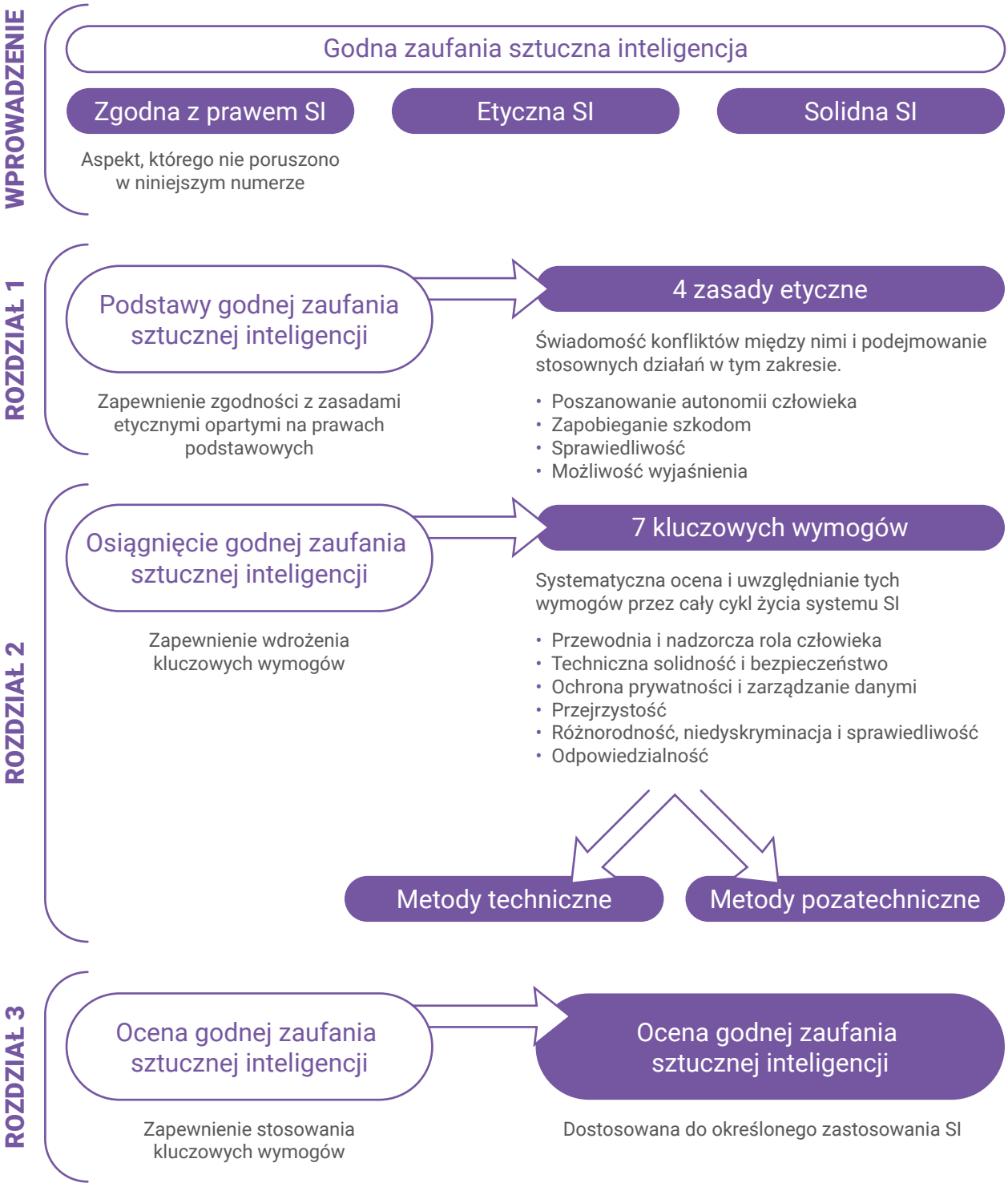
Druga część dokumentu zawiera siedem kluczowych wymogów, które powinna spełniać technologia korzystająca ze Sztucznej Inteligencji:

7 wymogów dla technologii wykorzystującej Sztuczną Inteligencję

- **Przewodnia i nadzorcza rola człowieka –** systemy wykorzystujące SI nie powinny ograniczać ludzkiej autonomii, ale wspierać jej rozwój poprzez wzmacnianie przewodniej i nadzorczej roli człowieka.
- **Solidność techniczna i bezpieczeństwo –** systemy wykorzystujące SI powinny dbać o bezpieczeństwo użytkowników i swoją niezawodność, a także radzić sobie z błędami, które mogą występować na każdym etapie cyklu życia systemu SI.
- **Ochrona prywatności i zarządzanie danymi –** systemy wykorzystujące SI powinny zapewniać ochronę prywatności i kontrolę nad danymi użytkowników. Ponadto przetwarzane w systemie SI dane nie mogą być wykorzystywane do szkodzenia ani dyskryminowania użytkowników.
- **Przejrzystość –** systemy wykorzystujące SI powinny być transparentne i identyfikowalne, zarówno w zakresie wiedzy o wkomponowanych algorytmach i procesie podejmowania decyzji. Wiedza ta powinna być również dostępna dla każdego użytkownika danego systemu SI.
- **Różnorodność, niedyskryminacja i sprawiedliwość –** systemy wykorzystujące SI powinny brać pod uwagę cały zakres ludzkich zdolności i umiejętności.
- **Dobrostan społeczny i środowiskowy –** systemy wykorzystujące SI powinny działać na rzecz pozytywnych zmian społecznych i odpowiedzialności ekologicznej.
- **Odpowiedzialność –** należy wprowadzić mechanizmy zapewniające odpowiedzialność za systemy SI oraz konsekwencje ich działania.

Dokument zawiera także przykładową listę kontrolną służącą do oceny godnej zaufania Sztucznej Inteligencji. Zdaniem ekspertów, lista kontrolna musi być dostosowana do konkretnej technologii wykorzystującej SI, ponieważ technologie te istotnie różnią się od siebie.

Ramy dotyczące godnej zaufania sztucznej inteligencji



Opracowano na podstawie: *„Wytyczne dotyczące etyki godnej zaufania sztucznej inteligencji"*

2. Definicja SI: główne funkcje i dyscypliny

8 kwietnia 2019 roku Grupa Ekspertów *AI HLEG* opublikowała dokument *Definicja SI: główne funkcje i dyscypliny (A Definition of AI: Main Capabilities and Disciplines)*. Celem dokumentu było zaktualizowanie i rozszerzenie definicji Sztucznej Inteligencji, zaproponowanej przez KE w 2018 roku oraz wyjaśnienie niektórych aspektów SI jako dyscypliny naukowej i technologii. Zdaniem ekspertów, pozwoli to osiągnąć wspólny poziom wiedzy i uniknąć nieporozumień w dyskusjach ze specjalistami niezajmującymi się Sztuczną Inteligencją. W dokumencie termin „system SI" odnosi się do dowolnego podzespołu, oprogramowania komputerowego lub sprzętu opartego na Sztucznej Inteligencji. Eksperci podkreślają, że systemy SI są zwykle częścią bardziej złożonych systemów.

Zaktualizowana definicja Sztucznej Inteligencji zaproponowana przez Grupę Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji

Systemy Sztucznej Inteligencji (SI) to oprogramowania komputerowe (i ewentualnie również sprzęt komputerowy) stworzone przez człowieka, które, biorąc pod uwagę złożony cel, działają w wymiarze fizycznym lub cyfrowym poprzez postrzeganie ich otoczenia dzięki gromadzeniu danych, interpretacji zebranych, ustrukturyzowanych lub nieustrukturyzowanych danych, rozumowaniu na podstawie wiedzy lub przetwarzaniu informacji pochodzących z tych danych oraz podejmowaniu decyzji w sprawie najlepszych działań, które należy podjąć w celu osiągnięcia określonego celu.

Systemy SI mogą wykorzystywać symboliczne reguły albo uczyć się modelu numerycznego, a także dostosowywać swoje zachowanie, analizując wpływ ich poprzednich działań na otoczenie.

Definicja Sztucznej Inteligencji zaproponowana w komunikacie Komisji Europejskiej z 24 kwietnia 2018 roku

Termin Sztuczna Inteligencja odnosi się do systemów, które wykazują inteligentne zachowanie dzięki analizie otoczenia i podejmowaniu działań – do pewnego stopnia autonomicznie – w celu osiągnięcia konkretnych celów.

W literaturze naukowej istnieje wiele definicji terminu Sztuczna Inteligencja. Autorzy niniejszego opracowania przyjęli, że koncepcja systemów wykorzystujących SI opiera się na pojęciu „racjonalności", a nie „inteligencji". W rozumieniu naukowców „inteligencja" jest przedmiotem badań psychologów, biologów i neurofizjologów. Natomiast „racjonalność" jest przedmiotem badań nauk technicznych i określa możliwość wyboru najlepszego działania z uwzględnieniem wcześniej ustanowionych kryteriów i dostępnych zasobów, żeby osiągnąć konkretny cel. Zgodnie ze stanem najnowszej wiedzy[270], tak rozumiana „racjonalność" stanowi istotną część koncepcji Sztucznej Inteligencji.

270 *"Artificial Intelligence: A Modern Approach"*, S. Russell and P. Norvig, Prentice Hall, 3rd edition, 2009.

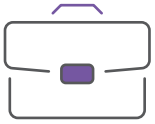
Jako dyscyplina naukowa SI obejmuje różne podejścia i techniki, takie jak uczenie się maszyn (czego konkretnymi przykładami są uczenie głębokie i uczenie przez wzmacnianie), rozumowanie maszyn (obejmujące planowanie, programowanie działań, reprezentowanie wiedzy i rozumowanie, wyszukiwanie i optymalizację) oraz robotyka (obejmująca sterowanie, postrzeganie, czujniki i urządzenia wykonawcze, a także integrację wszystkich innych technik w systemach cyberfizycznych)[271].

3. Wytyczne w zakresie polityki i inwestycji w godną zaufania sztuczną inteligencję

26 czerwca 2019 roku Grupa Ekspertów *AI HLEG* przedstawiła *Wytyczne w zakresie polityki i inwestycji w godną zaufania Sztuczną Inteligencję (Policy and Investment Recommendations for Trustworthy Artificial Intelligence).* Dokument zawiera 33 zalecenia skierowane do instytucji unijnych i państw członkowskich. Zdaniem ekspertów wdrożenie tych rekomendacji przyczyni się do zrównoważonego rozwoju, wzrostu konkurencyjności i integracji przy jednoczesnym wzmocnieniu ochrony i dobrostanu obywateli Unii Europejskiej. Rekomendacje koncentrują się na czterech kluczowych obszarach.

4 obszary rekomendacji

Obywatele i ogół społeczeństwa



Sektor prywatny

Sektor publiczny

Badania i środowisko akademickie

33 rekomendacje dotyczące regulacji i inwestycji dla godnej zaufania Sztucznej Inteligencji:

OBYWATELE I OGÓŁ SPOŁECZEŃSTWA

- Wzrost świadomości społecznej w obszarze Sztucznej Inteligencji.
- Ochrona integralności ludzi, społeczeństwa i środowiska.
- Promowanie podejścia skupionego na człowieku w kontekście rozwoju Sztucznej Inteligencji w pracy.
- Działanie przeciw wykluczeniu.
- Monitorowanie wpływu Sztucznej Inteligencji na społeczeństwo.

271 *A Definition of AI: Main Capabilities and Disciplines, (* https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines)

SEKTOR PRYWATNY

- Wzrost wdrażania technologii i systemów Sztucznej Inteligencji w Europie.
- Rozwój i zwiększenie skali rozwiązań SI, które promują innowację i transfer technologii
- Utworzenie partnerstw publiczno-prywatnych w celu wzmocnienia europejskiego ekosystemu SI.

SEKTOR PUBLICZNY

- Wdrażanie podejścia skupionego na człowieku w kontekście rozwoju Sztucznej Inteligencji w usługach publicznych.
- Wykorzystanie administracji państwowej jako katalizatora rozwoju Sztucznej Inteligencji w Europie.
- Strategiczne wykorzystanie zamówień publicznych dla wspierania innowacji i rozwoju godnej zaufania SI.
- Ochrona praw podstawowych w usługach publicznych opartych na SI.

BADANIA I ŚRODOWISKO AKADEMICKIE

- Opracowanie i wprowadzenie europejskiej strategii – mapy drogowej – dla badań z zakresu SI.
- Zwiększenie finansowania badań podstawowych i celowych.
- Rozwijanie kompetencji badawczych naukowców zajmujących się Sztuczną Inteligencją.
- Budowa europejskiego kapitału naukowego.
- Wsparcie budowy infrastruktury dla Sztucznej Inteligencji w państwach członkowskich.
- Rozwój inicjatyw wspierających wymianę danych w Europie.
- Wspieranie UE na drodze do światowego przywództwa w rozwoju Sztucznej Inteligencji.
- Opracowanie i wspieranie infrastruktury cyberbezpieczeństwa.
- Reforma systemów edukacji od szkoły podstawowej do szkolnictwa wyższego.
- Rozwijanie i zatrzymywanie talentów na uczelniach wyższych.
- Zwiększenie proporcji kobiet w nauce i technologii.
- Zwiększenie kwalifikacji aktualnej siły roboczej.
- Zbudowanie wsparcia dla nowych polityk edukacyjnych i świadomości wśród wszystkich interesariuszy.
- Uwzględnienie szacowania ryzyka i różnorodnych potrzeb interesariuszy w nowych regulacjach.
- Wykonanie przeglądu prawa unijnego, ze szczególnym uwzględnieniem najważniejszych dziedzin z punktu widzenia rozwoju Sztucznej Inteligencji.
- Rozważenie potrzeby nowych regulacji w celu zapewnienia odpowiedniej ochrony przed zagrożeniami wynikającymi z rozwoju Sztucznej Inteligencji.

- Sprawdzenie, czy istniejące struktury i możliwości z zakresu egzekwowania prawa są wystarczające, aby zapewnić obywatelom dostateczną ochronę przed zagrożeniami wynikającymi z rozwoju Sztucznej Inteligencji.
- Ustanowienie mechanizmów zarządzania godną zaufania Sztuczną Inteligencją dla jednolitego rynku cyfrowego.
- Zapewnienie odpowiedniego finansowania działań rekomendowanych w tym dokumencie.
- Odpowiednie zaadresowanie wyzwań inwestycyjnych na rynku.
- Stworzenie warunków dla lukratywnych inwestycji w godną zaufania Sztuczną Inteligencję.

Grupa Ekspertów ds. Odpowiedzialności i Nowych Technologii

21 października 2019 roku Grupa Ekspertów ds. Odpowiedzialności i Nowych Technologii *(Expert Group on Liability and New Technologies, NTF)*[272] opublikowała raport *Odpowiedzialność za Sztuczną Inteligencję i inne nowe technologie (Liability for Artificial Intelligence and other emerging digital technologies)*. Dokument zawiera szereg zaleceń i zmian, które należy wprowadzić do systemów odpowiedzialności na poziomie Unii Europejskiej, aby mogły one sprostać wyzwaniom związanym z rozwojem nowoczesnych technologii. Zdaniem ekspertów, obecnie obowiązujące przepisy w państwach członkowskich oraz w całej Unii Europejskiej w sposób niewystarczający, nieefektywny, a w niektórych przypadkach niesprawiedliwy, regulują kwestię prawnej odpowiedzialności za Sztuczną Inteligencję i nowe technologie cyfrowe, takie jak Internet Rzeczy czy Technologię Zdecentralizowanych Ksiąg Rachunkowych *(distributed ledger technology, DLT)*[273].

NTF sformułowała listę podstawowych zasad, które należy wdrożyć do porządku prawnego na poziomie Unii Europejskiej i państw członkowskich. Zdaniem autorów raportu należy uwzględnić specyfikę Sztucznej Inteligencji i nowych technologii – ich złożoność, możliwość zmiany istoty działania po modyfikacji, ograniczoną przewidywalność oraz podatność na zagrożenia cyberbezpieczeństwa. Dlatego konieczne jest wprowadzenie stosownych zmian w prawie Unii Europejskiej, które m.in. ułatwią uzyskanie odszkodowania w przypadku szkód powstałych w wyniku działania nowych technologii. Należy jednak podkreślić, że poniższe zasady ograniczają się wyłącznie do kwestii pozaumownej odpowiedzialności, pomijając normy techniczne.

Kluczowe wnioski Grupy Ekspertów ds. Odpowiedzialności i Nowych Technologii

- Osoba obsługująca dopuszczoną technologię, której działanie niesie ze sobą zwiększone ryzyko wyrządzenia szkody innym osobom (np. roboty wykorzystujące Sztuczną Inteligencję poruszające się w przestrzeni publicznej), powinna podlegać ścisłej odpowiedzialności za szkody powstałe w wyniku działania tej technologii.
- Należy zwrócić szczególną uwagę na ustalenie faktycznej odpowiedzialności za działanie technologii w sytuacji, w której to dostawca usług lub produktów wyposażonych w Sztuczną Inteligencję, a nie użytkownik danej usługi lub produktu, posiada wyższy stopień kontroli nad tymi usługami lub produktami.
- Osoba korzystająca z technologii, której działanie nie niesie ze sobą zwiększonego ryzyka wyrządzenia szkody innym osobom, powinna być zobowiązana do przestrzegania należytej staranności w kwestii wyboru technologii, sposobu jej działania i monitorowania. W przeciwnym wypadku taka osoba powinna ponieść odpowiedzialność za niedopełnienie tych obowiązków.
- Producenci wykorzystujący nowe technologie powinni ponosić odpowiedzialność za szkody wyrządzone przez wadliwe produkty bądź treści cyfrowe, które wprowadzają na rynek. W przypadku współpracy wielu firm, każda z nich powinna solidarnie przyjąć odpowiedzialność za ewentualne szkody spowodowane przez dany produkt lub treść cyfrową.

272 *Grupa Ekspertów ds. Odpowiedzialności i Nowych Technologii (NTF) została powołana przez Komisję Europejską w marcu 2018 roku. Decyzja o powołaniu grupy została podyktowana koniecznością zmian obecnych ram prawnych na poziomie UE w odniesieniu do regulacji na temat odpowiedzialności cywilnej i ubezpieczeń pojazdów autonomicznych. Grupa ekspertów NTF pełni rolę doradczą w stosunku do KE, opracowuje również nowe zasady i wytyczne dla obecnie obowiązujących unijnych przepisów dotyczących nowych technologii. Prace grupy koncentrują się na dwóch obszarach: odpowiedzialności za produkty oraz nowych technologii*

273 *Technologia Zdecentralizowanych Ksiąg Rachunkowych (ang. distributed ledger technology, DLT) – technologia wykorzystywana do replikowania, współdzielenia, wymiany i synchronizowania informacji elektronicznych pochodzących z różnych, rozproszonych geograficznie instytucji, przedsiębiorstw i osób. Technologia DLT stanowi obecnie technologiczną podstawę ponad 600 wirtualnych walut.*

- Zasadne wydaje się wprowadzenie obowiązkowych ubezpieczeń, które w przypadku wyrządzenia szkody osobom trzecim, na skutek niewłaściwego działania technologii, umożliwiłyby ofiarom lepszy dostęp do odszkodowania.
- W przypadku, w którym wyraźne przypisanie odpowiedzialności za szkody wyrządzone przez technologię jest niemożliwe, osoba poszkodowana powinna móc skorzystać z ułatwień dowodowych.
- Nowe technologie cyfrowe powinny być wyposażone w funkcje rejestrowania i przechowywania oraz wglądu do danych dotyczących ich funkcjonowania. W przypadku wystąpienia szkody, brak takich rozwiązań powinien skutkować odwróceniem ciężaru dowodu na korzyść poszkodowanego.
- Zniszczenie danych osoby poszkodowanej powinno być traktowane jako szkoda, która podlega odszkodowaniu.
- Nadanie autonomicznym produktom, systemom lub usługom osobowości prawnej nie jest konieczne, ponieważ szkody powstałe w wyniku funkcjonowania nowych technologii mogą i powinny być przypisane odpowiedzialnym za nie osobom lub instytucjom.
- Osoba korzystająca z technologii, która posiada pewien stopień autonomii, nie powinna ponosić mniejszej odpowiedzialności za wynikłe szkody, niż gdyby szkoda ta została spowodowana działaniem wyłącznie ludzkim.

Komisja Europejska (European Commision, EC)

8 kwietnia 2019 roku Komisja Europejska opublikowała komunikat w sprawie *Budowania zaufania do sztucznej inteligencji ukierunkowanej na człowieka (Building Trust in Human Centric Artificial Intelligence)*, w którym stwierdziła, że Sztuczna Inteligencja nie może być celem samym w sobie, ale godnym zaufania narzędziem, szanującym demokrację, ludzką godność i ostatecznie służącym wzmacnianiu dobrobytu człowieka. Komisja podkreśliła również, że zagadnienia etyczne nie mogą być traktowane jako dodatek do Sztucznej Inteligencji, ale jako jej integralna część. KE z zadowoleniem przyjęła działania Grupy Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji i zapowiedziała rozpoczęcie ukierunkowanej fazy pilotażowej, która sprawdzi, czy zaproponowane przez ekspertów wytyczne, dotyczące godnej zaufania Sztucznej Inteligencji, mogą zostać wdrożone w praktyce. Zakończenie etapu pilotażowego jest planowane na pierwszy kwartał 2020 roku. Na podstawie zebranych danych grupa ekspertów dokona przeglądu list kontrolnych dotyczących kluczowych wymogów. Ostatecznej oceny dokona Komisja Europejska, która określi kolejne działania w tym zakresie.

Dążąc do budowy globalnego konsensusu w sprawie SI ukierunkowanej na człowieka, KE planuje zacieśnić współpracę z partnerami wyznającymi podobne wartości w kwestii rozwoju Sztucznej Inteligencji.

Organizacja Współpracy Gospodarczej i Rozwoju

Organizacja Współpracy Gospodarczej *(Organisation for Economic Co-operation and Development, OECD)* od kilku lat wspiera rządy państw na całym świecie w monitorowaniu skutków gospodarczych i społecznych spowodowanych wdrażaniem rozwiązań opartych o Sztuczną Inteligencję. OECD tworzy również rekomendacje i standardy w obszarze polityki publicznej i nowych technologii, a także podejmuje dialog ze wszystkimi stronami zaangażowanymi w rozwój godnej zaufania Sztucznej Inteligencji.

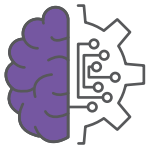
Standardy rozwoju Sztucznej Inteligencji OECD

22 maja 2019 roku OECD opublikowało pierwsze międzyrządowe standardy rozwoju Sztucznej Inteligencji *(The OECD Principles on Artificial Intelligence)*. Rekomendacje promują godną zaufania Sztuczną Inteligencję opartą na innowacyjności, szanującą prawa człowieka oraz demokratyczne wartości. Aktywność OECD w obszarze SI jest zbieżna z promowanymi wartościami i działaniami Komisji Europejskiej. Rekomendacje zostały przygotowane przez Grupę Ekspertów ds. Sztucznej Inteligencji powołaną przez OECD we wrześniu 2018 roku. Licząca ponad 50 członków grupa składa się z przedstawicieli 20 rządów oraz ekspertów reprezentujących środowisko biznesowe, akademickie i społeczeństwo obywatelskie.

Zalecenia dotyczące rozwoju Sztucznej Inteligencji zostały podzielone na dwie kategorie. Pierwsza opisuje 5 powiązanych ze sobą wartości opartych na zasadach odpowiedzialnego zarządzania wiarygodną SI, a druga 5 zaleceń skierowanych do decydentów odpowiedzialnych za tworzenie polityk krajowych.

Sekcja 1:

Zasady odpowiedzialnego zarządzania wiarygodną Sztuczną Inteligencją



Rozwój SI dla dobrobytu i zrównoważonego rozwoju

Sztuczna Inteligencja powinna zapewniać dobrobyt ludzkości i przynosić korzyści planecie. Zwiększać możliwości ludzkie, rozwijać kreatywność, umożliwiać integrację grup wykluczonych, minimalizować nierówności gospodarcze, społeczne, płciowe i inne. Ważne, aby rozwój technologii odbywał się z poszanowaniem środowiska naturalnego i w myśl idei zrównoważonego rozwoju.

Odpowiedzialność

Twórcy Sztucznej Inteligencji są odpowiedzialni za prawidłowe funkcjonowanie systemów SI i przestrzeganie zasad etyki.

Transparentność

Systemy Sztucznej Inteligencji powinny być projektowane w sposób transparentny i umożliwiający uzyskanie przez użytkownika informacji o sposobach działania systemu, logice podejmowania decyzji przez algorytm i czynnikach wpływających na tę decyzję. Ważne, aby użytkownikowi przysługiwało prawo zakwestionowania decyzji podjętej przez maszynę.

Koncentracja na wartościach i człowieku

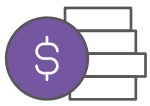
Twórcy Sztucznej Inteligencji powinni respektować praworządność, prawa człowieka i wartości demokratyczne. Rozwój technologii musi odbywać się z poszanowaniem wolności, prywatności, godności człowieka, z uwzględnieniem ochrony danych, sprawiedliwości i równości społecznej. Eksperci zalecają, aby systemy miały zabezpieczenia umożliwiające ludziom przejęcie kontroli nad maszyną, gdy zajdzie taka potrzeba.

Bezpieczeństwo

Sztuczna Inteligencja powinna być projektowana w taki sposób, aby zapewnić bezpieczeństwo użytkownikowi, a także przeciwdziałać wykorzystywaniu jej do nieodpowiednich celów. Dlatego konieczna jest możliwość systematycznej analizy ryzyka na każdym etapie cyklu życia maszyny lub systemu wykorzystującego Sztuczną Inteligencję. Użytkownicy powinni również mieć możliwość wglądu w historię podejmowanych przez algorytmy decyzji.

Sekcja 2:

Zasady dla decydentów na poziomie policy



Inwestowanie w badania i rozwój

Państwa powinny rozważyć długofalowe inwestycje w badania i rozwój Sztucznej Inteligencji, a także zachęcać sektor prywatny do podejmowania inwestycji w technologię, która będzie godna zaufania, etyczna i odpowiedzialna społecznie.

Wspieranie ekosystemu dla rozwoju SI

Państwa powinny promować działania budujące zaufanie do otwartych zbiorów danych i Sztucznej Inteligencji, a także dbać o to, aby rozwój technologii odbywał się w sposób legalny, uczciwy i etyczny. Konieczne jest również budowanie platform dzielenia się wiedzą.

Kształtowanie środowiska politycznego

Stworzenie i kształtowanie środowiska politycznego, które umożliwia rozwój i eksploatację Sztucznej Inteligencji w sposób etyczny. Zapewnienie kontroli i odpowiednie skalowanie nowych rozwiązań.

Budowa kompetencji i przygotowanie rynku pracy

Państwa powinny blisko współpracować ze wszystkimi interesariuszami na rzecz wdrażania transformacji cyfrowej. Ważne, aby motywować obywateli do wykorzystywania nowoczesnych technologii i zwiększać ich kompetencje w tym zakresie.

Współpraca międzynarodowa

Konieczne jest kontynuowanie współpracy międzynarodowej w ramach OECD i innych organizacji, na rzecz budowania etycznej i godnej zaufania Sztucznej Inteligencji. Państwa powinny zachęcać do udziału w międzynarodowych, międzysektorowych inicjatywach, które służą wymianie wiedzy i dobrych praktyk, a także promować rozwój standardów technicznych dla godnych zaufania systemów. OECD proponuje opracowanie porównywalnych na poziomie międzynarodowym wskaźników, które mogą służyć do badań, pomiarów rozwoju i wdrażania SI. Zalecenia OECD nie mają mocy prawnej, ale są brane pod uwagę przy ustalaniu międzynarodowych standardów i projektowaniu prawa krajowego. Stanowią też wytyczne do przeprowadzania dalszych analiz i wypracowania narzędzi wspierających państwa we wdrażaniu etycznej i godnej zaufania Sztucznej Inteligencji. Wdrażanie zaleceń będzie monitorowane przez Komitet ds. Polityki

Gospodarki Cyfrowej. Komitet ma również kontynuować prace nad Sztuczną Inteligencją we współpracy z UNESCO, Radą Europy i innymi organizacjami międzynarodowymi[274].

USA

Realizacja amerykańskiej wizji rozwoju Sztucznej Inteligencji została zapoczątkowana 10 maja 2018 roku podczas szczytu w Białym Domu *Artificial Intelligence for American Industry*. Wydarzenie, które zgromadziło ponad 100 ekspertów wysokiego szczebla, służyło opracowaniu długoterminowej strategii zapewniającej USA światowe przywództwo w dziedzinie Sztucznej Inteligencji. Zdaniem prezydenta Donalda Trumpa utrzymanie przez USA pozycji lidera w dziedzinie SI będzie miało istotne znaczenie dla bezpieczeństwa gospodarczego i obronności USA. Podczas majowego szczytu w Białym Domu Narodowa Rada Nauki i Technologii (NSTC) ustanowiła Komitet ds. Sztucznej Inteligencji. Pełni on rolę doradczą na rzecz Biura Wykonawczego Prezydenta USA w zakresie prowadzenia krajowej i zagranicznej polityki w dziedzinie badań i rozwoju Sztucznej Inteligencji.

Krajowa strategia Stanów Zjednoczonych w sprawie Sztucznej Inteligencji

11 lutego 2019 roku prezydent Donald Trump podpisał *Dekret 13589* ogłaszający *Amerykańską Inicjatywę Sztucznej Inteligencji (Executive Order 13859 announcing the American AI Initiative — the United States' national strategy on Artificial Intelligence)*. Inicjatywa zakłada wzajemną współpracę na rzecz rozwoju Sztucznej Inteligencji pomiędzy agencjami federalnymi, sektorem publicznym, prywatnym,

274 https://cyberpolicy.nask.pl/etyczna-sztuczna-inteligencja-rekomendacje-oecd/

akademickim, obywatelskim i partnerami międzynarodowymi. Silna koncentracja zasobów Rządu USA na rozwoju SI ma zapewnić Stanom Zjednoczonym pozycję niezależnego światowego lidera w tej dziedzinie. Zgodnie z inicjatywą wprowadzanie Sztucznej Inteligencji ma wspierać budowanie społecznego zaufania do przełomowych technologii.

5 filarów Strategii rozwoju Sztucznej Inteligencji w USA:

- **Inwestowanie w badania i rozwój SI**

  Przyczynianie się do przełomów technologicznych w rozwoju Sztucznej Inteligencji na poziomie administracyjnym, w przemyśle i środowisku akademicki. Realizacja tego celu wymaga zwiększenia nakładów finansowych na wynagrodzenia, badania podstawowe i rozwój SI.

- **Wyznaczanie standardów rozwoju SI**

  Stymulowanie rozwoju odpowiednich wytycznych i standardów technicznych, które zmniejszą bariery w bezpiecznym testowaniu i wdrażaniu technologii Sztucznej Inteligencji.

- **Wzmacnianie zasobów ludzkich**

  Edukowanie obecnych i przyszłych pokoleń amerykańskich pracowników w zakresie umiejętności rozwoju i wdrażania Sztucznej Inteligencji. Realizacja tego celu wymaga wprowadzenia systemu stypendiów i programów szkoleniowych.

- **Uwolnienie potencjału i innowacji SI**

  Promowanie zaufania do technologii wykorzystującej Sztuczną Inteligencję wśród amerykańskich obywateli przy jednoczesnej ochronie ich swobód, prywatności i wyznawanych wartości. Inicjatywa nakazuje agencjom federalnym udostępnianie ekspertom i naukowcom danych i modeli obliczeniowych, które mogą być wykorzystane do długoterminowych badań naukowych nad SI.

- **Międzynarodowe zaangażowanie i ochrona przewagi**

  Otwieranie nowych rynków dla amerykańskich branż SI, a także promowanie międzynarodowego środowiska wspierającego amerykańskie badania i innowacje w zakresie Sztucznej Inteligencji. Jednocześnie Stany Zjednoczone zamierzają zdecydowanie chronić swoją przewagę w tej dziedzinie przed państwami wrogo nastawionymi do USA.

Za koordynację amerykańskiej strategii rozwoju Sztucznej Inteligencji będzie odpowiedzialna Specjalna komisja ds. Sztucznej Inteligencji działającą w ramach prezydenckiej Narodowej Rady Nauki i Technologii *(National Science and Technology Council (NSTC) Select Committee on Artificial Intelligence)*.

Podsumowanie

Sztuczna Inteligencja jest obszarem o olbrzymim potencjale i priorytetowym znaczeniu dla niemal wszystkich aspektów funkcjonowania państwa i jakości życia obywateli. Obecnie światowymi liderami w dziedzinie SI są USA i Chiny, które rywalizują ze sobą o to, które państwo jako pierwsze dokona przełomu technologicznego i jeszcze bardziej wzmocni swoją przewagę na arenie międzynarodowej. Do rywalizacji przyłącza się także Unia Europejska, która w ostatnich latach intensywnie pracuje nad stworzeniem ekosystemu sprzyjającego rozwojowi godnej zaufania Sztucznej Inteligencji. W 2019 roku unijne regulacje skupiały się głównie na etycznych aspektach Sztucznej Inteligencji. Mimo ustanawiania nowych ram prawnych i zwiększenia funduszy na badania, szanse UE na zajęcie pozycji światowego lidera w najbliższych latach są niewielkie. Jak wynika z danych Światowej Organizacji Własności Intelektualnej, blisko 85% wszystkich patentów w dziedzinie Sztucznej Inteligencji należy do USA, Chin i Japonii. Analizując obecną sytuację geopolityczną wydaje się, że Unia Europejska i USA przyjęły podobną strategię polegającą na systematycznym budowaniu i ochronie przewagi konkurencyjnej przed autokratycznymi reżimami. Główne obawy dotyczące rozwoju Sztucznej Inteligencji koncentrują się na jej nieetycznym wykorzystywaniu np. do budowy przewagi militarnej lub działaniu na szkodę obywateli.

DEZINFORMACJA

W DOBIE CYFROWEJ REWOLUCJI

– Rafał Babraj –

Głównym wyzwaniem w kontekście dezinformacji w 2019 roku były wybory do Parlamentu Europejskiego. Wytężone prace prowadzone w 2018 roku na poziomie Unii Europejskiej, miały wzmocnić odporność społeczeństwa i uchronić demokratyczne procesy przed ingerencją z zewnątrz. Komisja podsumowała efekty *Planu Działania Przeciwko Dezinformacji,* a platformy internetowe zaprezentowały swoją aktywność w ramach *Kodeksu postępowania w zakresie zwalczania dezinformacji.*

W Polsce, oprócz majowych wyborów europejskich, w październiku odbyły się też wybory do Sejmu i Senatu. W przeciwdziałanie zjawisku dezinformacji zaangażowały się nie tylko administracja rządowa oraz krajowe instytucje, ale także organizacje trzeciego sektora. Polska była również gospodarzem *NATO Information and Communication Conference,* która stanowi przykład na to, że komunikacja strategiczna oraz zagrożenia hybrydowe wciąż są istotnymi zagadnieniami dla Sojuszu Północnoatlantyckiego.

Dezinformacja w dobie rewolucji cyfrowej

Zjawisko dezinformacji to obecnie jedno z większych wyzwań w przestrzeni cyfrowej, adresowanych nie tylko na poziomie pojedynczych państw, ale także organizacji i instytucji międzynarodowych. Dezinformacja może destabilizować sytuację w państwie, wywierać destrukcyjny wpływ na jego struktury administracyjne i decyzyjne, a także podważać podstawy społeczne, ekonomiczne oraz kulturowe.

Rewolucja cyfrowa zapoczątkowała wiele przemian. Jedną z nich było wykształcenie nowej formacji społecznej: społeczeństwa informacyjnego, dla którego strategicznym zasobem, zamiast kapitału i pracy, stały się informacje. W przestrzeni cyfrowej są one dostarczane nieustannie i w czasie rzeczywistym. Jeszcze nigdy dostęp do wiedzy i informacji nie był tak łatwy. Równocześnie jednak, Internet stał się głównym obszarem działań dezinformacyjnych.

Błyskawiczna ekspansja mediów społecznościowych zmieniła układ sił w sferze informacyjnej. Media tradycyjne straciły na znaczeniu. Obecnie informacje publikować może każdy – dziennikarz obywatelski, bloger czy influencer korzystający z *social media.* A zatem użytkownicy Internetu nie są jedynie odbiorcami komunikatów, ale mają bezpośredni wpływ na ich kreację i rozprzestrzenianie się. Udostępniając lub komentując wybrane treści, zwiększają ich zasięgi. A to, w wymierny sposób, przekłada się na zarobki generowane przez reklamy. W efekcie priorytetem często staje się dostarczanie treści „klikalnych", a więc takich, które pozwolą osiągnąć największy profit. Ważniejszy bywa czas reakcji niż rzetelność.

To wszystko sprawiło, że dotychczasowa rola mediów musiała ulec zmianie. Nowym, niezwykle ważnym zadaniem dziennikarzy stało się sprawdzanie publikowanych w Internecie informacji, czyli *fact-checking.*

Wpływ dezinformacji na państwo, społeczeństwo, politykę i biznes został szczegółowo omówiony w raporcie *Zjawisko dezinformacji w dobie rewolucji cyfrowej,* dostępnym na stronie: www.cyberpolicy.nask.pl/raport-zjawisko-dezinformacji-w-dobie-rewolucji-cyfrowej-panstwo-spoleczenstwo-polityka-biznes.

Unia Europejska

Wybory do Parlamentu Europejskiego były centralnym wydarzeniem, dookoła którego ogniskowały się wszelkie działania dotyczące zwalczania dezinformacji na poziomie Unii Europejskiej. W 2018 roku ukazały się cztery ważne dokumenty, które poruszały problem fałszywych narracji:

- *Komunikat KE: Zwalczanie dezinformacji w Internecie: podejście europejskie* (kwiecień 2018).
- *Kodeks postępowania w zakresie zwalczania dezinformacji* (wrzesień 2018).
- *Komunikat KE w sprawie wolnych i uczciwych wyborów europejskich* (wrzesień 2018).
- *Plan Działania Przeciwko Dezinformacji* (grudzień 2018).

Większość działań podejmowanych w 2019 roku wynikała z założeń oraz planów przyjętych w roku 2018. Według Komórki UE ds. Syntezy Informacji o Zagrożeniach Hybrydowych *(EU Hybrid Fusion Cell)*, to właśnie dezinformacja ze strony Federacji Rosyjskiej miała być największym zagrożeniem dla wyborów do Parlamentu Europejskiego. Czy te obawy się sprawdziły?

Prowadzony przez grupę zadaniową ds. komunikacji strategicznej dotyczącej Wschodu *(East Strat Com Task Force)* portal *EU vs. Disinfo* wskazał, że nie zaobserwowano zmasowanej kampanii, połączonej ze spektakularnymi włamaniami, wyciekami danych oraz cyberatakami[275]. Choć nie znaczy to, że wybory były wolne od dezinformacji. Wręcz przeciwnie, poziom zmanipulowanej aktywności w sieci wzrósł przed wyborami ponad dwukrotnie w porównaniu do analogicznego okresu w 2018 roku[276].

275 *EU elections update: reaping what was sown* (https://euvsdisinfo.eu/eu-elections-update-reaping-what-was-sown/)

276 Według *East StratCom Task Force* od stycznia do czerwca 2019 roku odnotowano 998 przypadków dezinformacji przypisywanej rosyjskim źródłom, w porównaniu do 434 przypadków w roku 2018 (Źródło: Rezolucja Parlamentu Europejskiego z dnia 10 października 2019 r. w sprawie ingerencji zewnętrznej w wybory i dezinformacji w krajowych i unijnych procesach demokratycznych, https://www.europarl.europa.eu/doceo/document/TA-9-2019-0031_PL.html)

Brak ewidentnie dostrzegalnego wpływu na przebieg wyborów do Parlamentu Europejskiego może oznaczać, że działania podjęte przez Komisję, państwa członkowskie, środowiska dziennikarzy, organizacje *fact-checkingowe* czy duże platformy internetowe, przyniosły pewne rezultaty i utrudniły efektywne prowadzenie kampanii dezinformacyjnych. Jednak cały czas jest jeszcze wiele pracy do wykonania, np. w zakresie współpracy z platformami internetowymi, które mają do odegrania istotną rolę w przeciwdziałaniu dezinformacji. Konieczne wydaje się również wzmocnienie zdolności komunikacji strategicznej zarówno na poziomie UE, jak i poszczególnych państw członkowskich.

Efekty Planu Działania Przeciwko Dezinformacji

14 czerwca 2019 roku Komisja Europejska opublikowała **sprawozdanie z realizacji *Planu Działania Przeciwko Dezinformacji***[277]**.** Dokument podsumował postępy w walce z dezinformacją oraz przedstawił główne wnioski z wyborów do Parlamentu Europejskiego. KE podkreśliła, że choć majowe wybory nie były wolne od dezinformacji, to podjęte działania przyczyniły się do zawężenia przestrzeni dla zagranicznych ingerencji.

W ocenie KE współpraca z dziennikarzami, fact-checkerami, platformami internetowymi, władzami krajowymi, badaczami oraz społeczeństwem obywatelskim, pomogła ujawnić próby wpływania na procesy demokratyczne oraz manipulowania debatą publiczną. Zaobserwowano stałą aktywność źródeł powiązanych z Federacją Rosyjską, które miały zmniejszyć frekwencję i wpłynąć na preferencje wyborców. Co ważne, taktyka autorów kampanii dezinformacyjnych wciąż się zmienia. Fałszywe narracje w coraz większym stopniu ukierunkowane są lokalnie. Zamiast dużych kampanii w mediach społecznościowych, częściej stosowane są mniejsze operacje, które trudniej zdemaskować[278].

Aktywności w ramach *Planu Działania Przeciwko Dezinformacji* koncentrowały się na czterech obszarach.

Obszar	Działania
Wzmocnienie zdolności do identyfikowania i przeciwdziałania dezinformacji oraz poprawa skoordynowanej odpowiedzi na fałszywe narracje	• Zwiększenie finansowania oraz zatrudnienia w **grupach zadaniowych ds. komunikacji strategicznej** w Europejskiej Służbie Działań Zewnętrznych. Budżet na strategiczną komunikację w 2019 roku zwiększył się ponad dwukrotnie, do 5 mln euro, a w ciągu najbliższych dwóch lat zatrudnionych zostanie około 50 pracowników[279]. • Uruchomienie w marcu ***Rapid Alert System.*** System szybkiego ostrzegania ułatwił wymianę informacji między organami UE i państwami członkowskimi.

277 Komunikat Komisji Europejskiej: Sprawozdanie z realizacji Planu Działania przeciwko dezinformacji (https://eeas.europa.eu/sites/eeas/files/joint_report_on_disinformation.pdf)
278 Sprawozdanie z realizacji *Planu Działania Przeciwko Dezinformacji*, s. 9, (https://eeas.europa.eu/sites/eeas/files/joint_report_on_disinformation.pdf)
279 *Action Plan Against Disinformation: Report on progress* (https://ec.europa.eu/commission/sites/beta-political/files/factsheet_disinfo_elex_140619_final.pdf)

Współpraca z platformami internetowymi i sektorem prywatnym w ramach *Kodeksu postępowania w zakresie zwalczania dezinformacji*	• Usprawnienie kontroli zamieszczania reklam, aby ograniczyć *clickbaity* oraz zmniejszyć przychody z reklam dla osób publikujących dezinformację. • Poprawa przejrzystości reklam politycznych. Oznaczanie oraz udostępnianie w bibliotece reklam. • Zaangażowanie w zwalczanie fałszywych informacji, promowanych przy użyciu m.in. botów i nieprawdziwych kont.
Zwiększenie świadomości i odporności na dezinformację w społeczeństwie	• Działania takie jak: kampania społeczna *This Time I'm Voting,* organizacja 320 wydarzeń w ramach *Media Literacy Week,* uruchomienie projektu *SOMA – Social Observatory for Disinformation and Social Media Analysis* finansowanego w ramach programu Horyzont 2020. • Przeznaczenie 2,5 mln euro w ramach *Connecting Europe Facility* na nowe usługi cyfrowe, mające połączyć dziennikarzy, badaczy oraz fact-checkerów[280].
Wsparcie państw członkowskich w zapewnieniu wiarygodności wyborów i wzmocnieniu odporności systemów demokratycznych	• Sieci wyborcze składające się z organów, mających związek z procesem wyborczym, ustanowione we współpracy z państwami członkowskimi. • Ćwiczenia dotyczące reagowania na incydenty w cyberprzestrzeni, zorganizowane przy wsparciu ENISA. • Wydanie przez KE wytycznych dotyczących stosowania ogólnego rozporządzenia o ochronie danych w kontekście wyborczym.

Realizacja Kodeksu postępowania w zakresie zwalczania dezinformacji przed wyborami do Parlamentu Europejskiego

Od stycznia do maja 2019 roku Komisja Europejska otrzymywała comiesięczne sprawozdania od Google, Facebooka i Twittera[281] dotyczące działań podjętych w celu zwalczania dezinformacji przed wyborami do Parlamentu Europejskiego. 14 czerwca 2019 roku Komisja opublikowała wyniki pośrednie przesłane przez platformy[282].

280 *Commission launches call to create the European Digital Media Observatory* (https://ec.europa.eu/digital-single-market/en/news/commission-launches-call-create-european-digital-media-observatory)
281 W maju 2019 roku również Microsoft podpisał *Kodeks postępowania w zakresie zwalczania dezinformacji.*
282 *Last intermediate results of the EU Code of Practice against disinformation* (https://ec.europa.eu/digital-single-market/en/news/last-intermediate-results-eu-code-practice-against-disinformation)

Działania podjęte przez platformy internetowe przed wyborami do Europarlamentu[283]

Kontrola rynku reklamy:

- Google: działania przeciwko **157 tys.** kont (130 tys. mogło wprowadzać w błąd, a 27 tys. naruszało zasady oryginalności treści).
- Facebook: ponad **1,2 mln** działań związanych z naruszeniem zasad publikowania reklam i treści.
- Twitter: odrzucił **16 tys.** reklam (6 tys. naruszało zasady praktyk biznesowych, a 10 tys. zasady wysokiej jakości).

Integralność usług:

- Facebook: usunął **2,2 miliarda** fałszywych kont. Podjął działania przeciwko 1742 stronom, grupom i kontom (tylko 168 było z UE), zaangażowanym w nieautentyczne zachowania skierowane wobec państw członkowskich UE.
- Twitter: zakwestionował **77 mln** kont fałszywych lub używanych do spamu.
- YouTube: usunął **3,39 mln** kanałów z powodu spamu, wprowadzania w błąd i oszustw, a także **8,6 tys.** kanałów podszywających się pod inne osoby.

Przejrzystość reklam politycznych:

Wszystkie platformy podjęły działania przed wyborami do Parlamentu Europejskiego, oznaczając reklamy polityczne i udostępniając je publicznie.

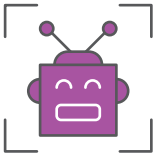
Komisja doceniła postępy w zakresie poprawy przejrzystości reklam politycznych oraz ich upubliczniania. Dostrzegła również wysiłki platform, takie jak działania przeciwko nieetycznemu wykorzystaniu botów i fałszywych kont. Podkreśliła jednak, że platformy muszą zrobić jeszcze więcej. Powinny m.in. nawiązać głębszą współpracę z organizacjami fact-checkingowymi we wszystkich państwach członkowskich, a także w większym stopniu udostępniać dane społeczności badawczej. Umożliwi to lepsze wykrywanie i analizę kampanii dezinformacyjnych oraz rzetelne monitorowanie wdrażania Kodeksu.

Realizacja Kodeksu postępowania w zakresie zwalczania dezinformacji po roku od podpisania

29 października 2019 roku Komisja Europejska opublikowała **pierwsze roczne sprawozdania z realizacji zobowiązań Kodeksu,** przesłane przez Facebooka, Google'a, Microsoft, Mozillę, Twittera i 7 europejskich stowarzyszeń handlowych[284]. Komisja dostrzegła poczynione postępy, zwracając uwagę, że po roku od podpisania Kodeksu sytuacja uległa poprawie. Wciąż konieczne są jednak dalsze działania oraz niesłabnące zaangażowanie platform.

Kodeks skupiał się na działaniach ograniczających wpływ dezinformacji w pięciu obszarach:

Transparentność sponsorowanych treści



Identyfikacja fałszywych kont i botów

283 *Action Plan Against Disinformation Report on progress* (https://ec.europa.eu/commission/sites/beta-political/files/factsheet_disinfo_elex_140619_final.pdf)
284 Kodeks postępowania w zakresie dezinformacji rok później: platformy internetowe przesyłają raporty z samooceny (https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019)

Przejrzystość i możliwość weryfikacji algorytmów

Dostęp do różnorodnych źródeł informacji

Monitoring prowadzony przez instytucje badawcze i władze publiczne

Komisja zwróciła uwagę, że zwłaszcza w obszarach 1, 2 oraz 3, które były monitorowane przed wyborami do Parlamentu Europejskiego, można zauważyć poprawę. Jednak aktywność w obszarach 4 i 5, mających wzmocnić pozycję użytkowników oraz społeczności badawczej, nie jest zadowalająca. Podkreślono także różny stopień zaawansowania działań poszczególnych platform oraz rozbieżności w zakresie wdrażania działań w państwach członkowskich.

Kolejnym etapem będzie **całościowa ocena skuteczności *Kodeksu postępowania w zakresie zwalczania dezinformacji*.** Komisja Europejska weźmie pod uwagę samoocenę sygnatariuszy, jak również m.in. wkład Europejskiej Grupy Regulatorów ds. audiowizualnych usług medialnych (ERGA), ocenę organizacji zewnętrznej wybranej przez sygnatariuszy oraz ocenę niezależnego konsultanta zaangażowanego przez Komisję. Na tej podstawie w 2020 roku powstanie kompleksowa ocena realizacji Kodeksu. Jeżeli jej wynik okaże się niezadowalający, Komisja może zaproponować dalsze środki, w tym o charakterze regulacyjnym.

Ingerencja w wybory i dezinformacja w procesach demokratycznych państw oraz UE

10 października 2019 roku Parlament Europejski opublikował rezolucję w sprawie ingerencji zewnętrznej w wybory i dezinformacji w krajowych i unijnych procesach demokratycznych[285]. Podkreślono w niej, że kampanie dezinformacyjne oraz zagraniczne ingerencje w wybory są częścią szerszej strategii wojny hybrydowej. Reagowanie na te zagrożenia powinno więc stać się głównym zagadnieniem bezpieczeństwa i polityki zagranicznej Unii Europejskiej. Tego typu ingerencje ze strony innych państw należy zaś traktować jako naruszenie prawa międzynarodowego.

Parlament wyraził zaniepokojenie nowymi dowodami na zewnętrzne ingerencje w okresie poprzedzającym wszystkie najważniejsze wybory krajowe i europejskie. Dlatego wezwał Komisję Europejską do wprowadzenia skutecznej strategii przeciwdziałania rosyjskim kampaniom dezinformacyjnym.

Rezolucja wskazuje, że ingerencja wyborcza w jednym państwie członkowskim wpływa na całą UE, dlatego zagrożeniom hybrydowym nie mogą przeciwdziałać wyłącznie władze krajowe, ani platformy internetowe w ramach samoregulacji. Konieczne jest opracowanie ram prawnych dla zwalczania tego typu zagrożeń, w tym cyberataków i dezinformacji, które umożliwią zdecydowaną reakcję oraz adekwatną odpowiedź.

Parlament zaapelował o finansowanie krajowe i europejskie na aktywne prowadzenie własnej komunikacji strategicznej[286]. Środki mogłyby pochodzić m.in. z programów *Horyzont Europa* i *Cyfrowa Europa*. Wskazał też, że warto pod-

285 Rezolucja Parlamentu Europejskiego z dnia 10 października 2019 r. w sprawie ingerencji zewnętrznej w wybory i dezinformacji w krajowych i unijnych procesach demokratycznych (https://www.europarl.europa.eu/doceo/document/TA-9-2019-0031_PL.html)

286 Komunikacja strategiczna to skoordynowane działania komunikacyjne danego państwa, organizacji lub podmiotu, które mają umożliwiać lub wspierać prowadzone działania, operacje oraz szerzej – politykę. Mogą się na nią składać np. działania dyplomatyczne, prasowo-informacyjne (także wojskowe), operacje informacyjne czy psychologiczne, mające kształtować opinie i zachowania.

nieść status grupy zadaniowej *East StratCom* do stałej struktury w ramach Europejskiej Służby Działań Zewnętrznych, a także zwiększyć jego budżet oraz personel[287].

Kolejnym aspektem poruszonym przez Parlament Europejski było uzależnienie od zagranicznych technologii i sprzętu. Unia Europejska powinna dążyć do większej niezależności w tym zakresie, aby zmniejszyć ryzyko zewnętrznej ingerencji w wybory. Co więcej, **Parlament wezwał Komisję do uznania sprzętu wyborczego za infrastrukturę krytyczną.**

Polska

W Polsce w 2019 roku odbyły się nie tylko wybory do Parlamentu Europejskiego, ale także wybory do Sejmu i Senatu Rzeczypospolitej Polskiej. Oba te wydarzenia wiązały się ze szczególną aktywnością w zakresie przeciwdziałania dezinformacji. Przy czym wiele z działań podejmowanych przez krajowe instytucje wynikało z dokumentów przyjętych na poziomie Unii Europejskiej.

Działania instytucji państwowych

Minister Jacek Czaputowicz, przedstawiając w Sejmie zadania polskiej polityki zagranicznej w 2019 roku, podkreślił że sytuacja na Wschodzie oraz wytężona wojna informacyjno-propagandowa stanowi duże wyzwanie dla Polski[288]. Jako odpowiedź na to wyzwanie w 2019 roku w **Ministerstwie Spraw Zagranicznych** utworzono komórkę odpowiedzialną za identyfikację, przeciwdziałanie i reagowanie na kampanie dezinformacyjne.

W marcu 2019 roku w Ministerstwie Spraw Zagranicznych uruchomiony został *Rapid Alert System*[289]. Jego celem jest regularna wymiana informacji na temat działań dezinformacyjnych, między państwami członkowskimi oraz kluczowymi partnerami takimi jak NATO. Był to element realizacji *Planu Działania Przeciwko Dezinformacji* przyjętego w 2018 roku przez Komisję Europejską. Również w marcu MSZ przeprowadził szkolenie dla kadry kierowniczej polskich ministerstw.

W maju 2019 roku, jeszcze przed europejskimi wyborami, **Krajowa Rada Radiofonii i Telewizji** prowadziła monitoring reklam politycznych umieszczanych na Google, Twitterze i Facebooku. Działanie to odbywało się w ramach grupy zadaniowej funkcjonującej w ERGA *(European Regulators Group for Audiovisual Media Services)*, której zadaniem była obserwacja realizacji zobowiązań sygnatariuszy *Kodeksu postępowania w zakresie przeciwdziałania dezinformacji*[290]. Był to pierwszy etap monitoringu. Drugi będzie stanowić kompleksową analizę realizacji wszystkich pięciu obszarów Kodeksu i posłuży Komisji Europejskiej do przygotowania całościowej oceny skuteczności samoregulacji sektora prywatnego.

Wiele działań przed majowymi wyborami do Parlamentu Europejskiego podjął również **NASK PIB.** Ich głównym celem było podniesienie poziomu świadomości na temat zagrożeń związanych z dezinformacją w sieci. Informacje o tym, jak rozpoznawać *fake newsy* i zadbać o swoje cyberbezpieczeństwo skierowano do kilku grup odbiorców: użytkowników, komitetów wyborczych, mediów i organizacji pozarządowych. Warto w tym kontekście wymienić m.in.:

- Rozbudowę strony www.BezpieczneWybory.pl, którą uruchomiono przed wyborami samorządowymi w październiku 2018 roku.

287 Unijny zespół *East StratCom Task Force,* zajmujący się m.in. walką z rosyjską dezinformacją, ma w swoich strukturach polską przedstawicielkę, dr Martynę Bildziukiewicz.
288 Działania Ministerstwa Spraw Zagranicznych RP w obszarze przeciwdziałania obcej dezinformacji, Raport *Zjawisko dezinformacji w dobie rewolucji cyfrowej* (https://cyberpolicy.nask.pl/raport-zjawisko-dezinformacji-w-dobie-rewolucji-cyfrowej-panstwo-spoleczenstwo-polityka-biznes/)
289 *Rapid Alert System* (RAS) – system szybkiego ostrzegania, ustanowiony ramach *Planu Działania Przeciwko Dezinformacji*, aby ułatwić wymianę informacji między organami UE i państwami członkowskimi.
290 Działania monitorujące Krajowej Rady Radiofonii i Telewizji – Kodeks postępowania w zakresie przeciwdziałania dezinformacji, Raport *Zjawisko dezinformacji w dobie rewolucji cyfrowej* (https://cyberpolicy.nask.pl/raport-zjawisko-dezinformacji-w-dobie-rewolucji-cyfrowej-panstwo-spoleczenstwo-polityka-biznes/)

- Warsztaty dla komitetów wyborczych oraz przedstawicieli mediów przeprowadzone przez ekspertów CSIRT NASK.
- Badanie opinii o (dez)informacji w sieci przeprowadzone przez Pracownię Badań Społecznych NASK[291].

Natomiast przed październikowymi wyborami parlamentarnymi w Polsce, NASK PIB opublikował raport ***Dezinformacja w dobie rewolucji cyfrowej***[292]**.** Do współpracy zaproszono instytucje i organy państwowe, które odgrywają wiodącą rolę z przeciwdziałaniu dezinformacji w Polsce, a więc: Ministerstwo Spraw Zagranicznych, Ministerstwo Obrony Narodowej, Biuro Bezpieczeństwa Narodowego, Rządowe Centrum Bezpieczeństwa, Urząd Ochrony Danych Osobowych oraz Krajową Radę Radiofonii i Telewizji. Swoje artykuły przygotowali przedstawiciele sektora prywatnego i ośrodków analitycznych oraz akademickich (Ośrodek Studiów Wschodnich, Akademia Sztuki Wojennej), a także eksperci NASK PIB z zespołów CyberPolicy, CERT Polska, Dyżurnet czy z Działu Edukacji Cyfrowej.

Dzięki tak szerokiej współpracy możliwe było kompleksowe podejście do zjawiska dezinformacji w odniesieniu do czterech obszarów: państwo, polityka, społeczeństwo i biznes. Premierze raportu towarzyszyło zamknięte spotkanie dla przedstawicieli administracji państwowej, które było okazją do zacieśnienia współpracy i podzielenia się dobrymi praktykami.

Działania trzeciego sektora

Przed wyborami do Parlamentu Europejskiego, Stowarzyszenie Demagog poinformowało o dołączeniu do Międzynarodowej Sieci Fact-Checkingowej (IFCN)[293]. Tym samym stało się pierwszą w Polsce organizacją należącą do International *Fact-Cheking Network*[294]. Dzięki temu we wrześniu, przed wyborami parlamentarnymi w Polsce, Demagog mógł dołączyć do programu niezależnej weryfikacji informacji Facebooka[295]. Wcześniej platforma, przy sprawdzaniu fałszywych wiadomości w Polsce, korzystała z usług warszawskiego biura Francuskiej Agencji Prasowej (AFP).

We wrześniu 2019 roku Fundacja Panoptykon we współpracy z Fundacją Reporterów przygotowała publikację ***Stop dezinformacji. Przewodnik dla dziennikarzy i redakcji***[296]. Dokument stanowi pewnego rodzaju instrukcję na temat tego, jak weryfikować źródła informacji, jak relacjonować wybory, czy też jak budować pozycję swojej redakcji jako rzetelnej i godnej zaufania.

Dezinformacja a cyberbezpieczeństwo – obserwacje CSIRT NASK

Dane wykradzione w wyniku ataków teleinformatycznych często są potem wykorzystywane do kreowania fałszywych narracji. Dlatego techniczne aspekty realizacji kampanii dezinformacyjnych znajdują się w obszarze zainteresowań zespołu CERT Polska, który jest częścią CSIRT NASK, jednego z trzech krajowych zespołów ds. reagowania na incydenty w cyberprzestrzeni[297].

Kampanie dezinformacyjne mają pogłębiać istniejące podziały oraz podburzać opinię publiczną. Dlatego ich częstym celem są stosunki z sąsiadującymi krajami (Ukraina, Niemcy) lub sojusznikami (USA).

I tak w kwietniu 2019 roku w Internecie pojawiła się informacja o poszukiwaniach amery-

291 Bezpieczne wybory – raport na temat dezinformacji w sieci (https://bezpiecznewybory.pl/raporty/bezpieczne-wybory-raport-na-temat-dezinformacji-w-sieci)
292 Raport *Dezinformacja w dobie rewolucji cyfrowej* (https://cyberpolicy.nask.pl/raport-zjawisko-dezinformacji-w-dobie-rewolucji-cyfrowej-panstwo-spoleczenstwo-polityka-biznes/)
293 Dołączyliśmy do Międzynarodowej Sieci Fact-Checkingowej (IFCN)! (https://demagog.org.pl/analizy_i_raporty/demagog-dolaczyl-do-miedzynarodowej-sieci-fact-checkingowej-ifcn/)
294 Międzynarodowa Sieć Organizacji Fact-Checkingowych *(International Fact-Checking Network, IFCN)* powstała we wrześniu 2015 roku z inicjatywy *Poynter Institute*. W 2016 roku opracowała specjalny kodeks zasad, który do tej pory (stan na 20.02.2020 r.) podpisały 72 organizacje z całego świata.
295 Demagog dołącza do Programu niezależnej weryfikacji informacji Facebook (https://demagog.org.pl/analizy_i_raporty/demagog-dolacza-do-programu-niezaleznej-weryfikacji-informacji-facebooka/)
296 Stop dezinformacji. Przewodnik dla dziennikarzy i redakcji (https://panoptykon.org/wiadomosc/stop-dezinformacji-przewodnik-dla-dziennikarzy-i-redakcji)
297 Ustawa o Krajowym Systemie Cyberbezpieczeństwa wyznaczyła trzy zespoły CSIRT poziomu krajowego: CSIRT NASK, CSIRT GOV oraz CSIRT MON.

kańskiego żołnierza oskarżonego o zabójstwo polskiego wojskowego. Wiadomość zawierała cechy charakterystyczne dla *fake newsa*, takie jak krzykliwy tytuł (*clikbait*), budzące negatywne emocje zdjęcia, brak autora czy błędy stylistyczne. Wpis pojawił się na portalach należących do samorządów oraz lokalnych mediów, choć wiele z nich dość szybko usunęło fałszywą wiadomość.

Kolejny przykład dezinformacji wymierzonej w obecność żołnierzy USA w Polsce miał miejsce w czerwcu 2019 roku. Tym razem informacja dotyczyła konieczności ewakuacji obywateli w związku z ćwiczeniami Dragon 19. Pojawiła się ona na kilku portalach prowadzonych przez samorządy i lokalne media.

W październiku 2019 roku do sieci trafiła informacja, że polski rząd podpisał umowę z rządem niemieckim, na mocy której niemieccy obywatele będą mogli przejmować nieruchomości, w których mieszkali przed II wojną światową. Również w tym przypadku administratorzy stron urzędów oraz lokalnych mediów przyznali, że padli ofiarą cyberataku.

Do przeprowadzenia kampanii wykorzystano podatności w nieaktualnych komponentach aplikacji internetowej. Jest to o tyle proste, że w sieci można znaleźć gotowe narzędzia do tego typu ataków. Dlatego zespół CERT Polska rekomenduje regularne aktualizacje systemów zarządzania treścią[298].

Wymienione wcześniej przykłady stanowią potwierdzenie obserwacji, że fałszywe narracje są w coraz większym stopniu ukierunkowane lokalnie[299].

NATO

Kampanie dezinformacyjne, które stanowią element zagrożeń hybrydowych, znalazły się również w obrębie zainteresowania Sojuszu Północnoatlantyckiego. W maju 2019 roku w kwaterze głównej NATO odbyło się pierwsze spotkanie doradców ds. bezpieczeństwa narodowego poświęcone zagrożeniom hybrydowym. Sekretarz generalny Jens Stoltenberg podkreślił, że NATO musi być przygotowane na zagrożenia konwencjonalne i hybrydowe: „od czołgów po tweety"[300].

Szczególnie aktywne w zakresie przeciwdziałania dezinformacji było ***NATO StratCom COE***[301]**.** Centrum doskonałości ds. komunikacji strategicznej w Rydze powstało w 2014 roku, a wśród jego założycieli znalazła się Polska. Warto również podkreślić, że szefem sztabu jest obecnie polski oficer. *NATO StratCom* przygotowało wiele raportów oraz dokumentów dotyczących kampanii dezinformacyjnych. Wśród nich wymienić warto m.in.:

- **Czarny rynek manipulacji mediami społecznościowymi**[302] **–** dokument opisuje dynamiczny rynek manipulacji w social mediach. Przeprowadzone badania pokazały, że wciąż można łatwo i tanio prowadzić dezinformację online – pomimo zobowiązań firm, które podpisały *Kodeks postępowania w zakresie zwalczania dezinformacji.* Rynek manipulacji dominują rosyjscy dostawcy tego typu usług.
- **Rola *deepfakes* w kampaniach o szkodliwym wpływie**[303] **–** autorzy raportu wskazują, że już niedługo tego typu algorytmy uczenia maszynowego, będą wykorzystywane na porządku dziennym. Skutkiem ubocznym będzie osłabienie zaufania w sferze online.

298 Techniczne aspekty realizacji kampanii dezinformacyjnych, Raport *Dezinformacja w dobie rewolucji cyfrowej* (https://cyberpolicy.nask.pl/raport-zjawisko-dezinformacji-w-dobie-rewolucji-cyfrowej-panstwo-spoleczenstwo-politykа-biznes/)
299 Komunikat Komisji Europejskiej: Sprawozdanie z realizacji planu działania przeciwko dezinformacji (https://eeas.europa.eu/sites/eeas/files/joint_report_on_disinformation.pdf)
300 *National Security Advisers meet at NATO Headquarters* (https://www.nato.int/cps/en/natohq/news_166394.htm)
301 Centrum zostało początkowo założone przez Łotwę, Estonię, Niemcy, Włochy, Litwę, Polskę i Zjednoczone Królestwo w 2014 r.
302 *The Black Market for Social Media Manipulation, 9 stycznia 2019*, NATO StratCom COE (https://www.stratcomcoe.org/black-market-social-media-manipulation)
303 *The Role of Deepfakes in Malign Influence Campaigns*, 8 listopada 2019, NATO StratCom COE (https://www.stratcomcoe.org/role-deepfakes-malign-influence-campaigns)

W kontekście komunikacji strategicznej i cyberzagrożeń, *deepfakes* z czasem staną się kluczowe dla kampanii dezinformacyjnych wykorzystywanych w konflikcie hybrydowym.

Komunikacja strategiczna była także tematem ***NATO Information and Communication Conference,*** która odbyła się 25 września w Warszawie pod hasłem "Komunikacja w NATO w 70. rocznicę powstania: Jedność przekazu i przekaz jedności". Lokalizacja nie była przypadkowa, ponieważ w 2019 roku Polska obchodziła 20. rocznicę przystąpienia do Sojuszu. Wydarzenie zgromadziło blisko 400 ekspertów reprezentujących dowództwo NATO, kraje członkowskie oraz partnerskie. Uczestnicy brali udział w warsztatach, pracach grup roboczych oraz sesjach plenarnych o komunikacji strategicznej.

Miejscem zacieśnionej współpracy między Unią Europejską oraz NATO jest również *The European Centre of Excellence for Countering Hybrid Threats* w Helsinkach. ***Hybrid COE***[304] powstało w 2017 roku dzięki współpracy UE-NATO, a obecnie liczy 27 członków. Tylko w 2019 roku do centrum dołączyło 6 krajów. W ramach prowadzonych działań zorganizowano szereg warsztatów oraz szkoleń, a także opublikowano wiele analiz strategicznych dotyczących m.in.:

- Wykorzystywania podmiotów niepaństwowych do prowadzenia działań dezinformacyjnych[305].
- Podatności we współczesnej infrastrukturze krytycznej[306].
- Zwalczania zjawiska manipulacji informacją na przykładach wybranych państw[307].

Podsumowanie

Najważniejszym wydarzeniem w kontekście dezinformacji, w 2019 roku, były wybory do Parlamentu Europejskiego. *Portal EU vs. Disinfo*, podkreślił, że nie zaobserwowano zmasowanej kampanii dezinformacyjnej, choć poziom zmanipulowanej aktywności w sieci wzrósł przed wyborami ponad dwukrotnie. Fałszywe narracje w coraz większym stopniu ukierunkowane są jednak lokalnie, przez co trudniej je zdemaskować.

14 czerwca 2019 roku Komisja Europejska przedstawiła **sprawozdanie z realizacji *Planu Działania Przeciwko Dezinformacji*.** KE stwierdziła, że choć majowe wybory nie były wolne od dezinformacji, to podjęte kroki w pewnym stopniu ograniczyły zagraniczne ingerencje.

29 października 2019 roku Komisja Europejska zaprezentowała pierwsze roczne sprawozdania z realizacji zobowiązań ***Kodeksu postępowania w zakresie zwalczania dezinformacji*.** KE dostrzegła poczynione przez sygnatariuszy postępy, zwracając jednocześnie uwagę, że platformy wciąż mają wiele do zrobienia.

10 października 2019 roku Parlament Europejski opublikował **rezolucję w sprawie ingerencji zewnętrznej w wybory i dezinformacji w krajowych i unijnych procesach demokratycznych.** Wskazano w niej, że ingerencja wyborcza w jednym państwie członkowskim wpływa na całą UE. Dlatego niezbędne jest przygotowanie strategii oraz ram prawnych dla zwalczania zagrożeń hybrydowych. Parlament zaapelował też o większe finansowanie krajowe i europejskie na komunikację strategiczną.

W Polsce w 2019 roku odbyły się nie tylko wybory do Parlamentu Europejskiego, ale

304 Hybrid COE *(European Centre of Excellence for Countering Hybrid Threats)* to Europejskie Centrum Doskonalenia ds. przeciwdziałania zagrożeniom hybrydowym. Zadaniem centrum jest umożliwienie systematycznej wymiany wiedzy i doświadczeń między zainteresowanymi państwami, a także UE oraz NATO (www.hybridcoe.fi/).
305 *Strategic Analysis: How states use non-state actors. A modus operandi for covert state subversion and malign networks* (https://www.hybridcoe.fi/publications/strategic-analysis-how-states-use-non-state-actors-a-modus-operandi-for-covert-state-subversion-and-malign-networks/)
306 *Hybrid Threats and Vulnerabilities of Modern Critical Infrastructure – Weapons of Mass Disturbance (WMDi)?* (https://www.hybridcoe.fi/publications/hybrid-threats-and-vulnerabilities-of-modern-critical-infrastructure-weapons-of-mass-disturbance-wmdi/)
307 *Strategic Analysis: Combating the manipulation of information – a French case* (https://www.hybridcoe.fi/publications/strategic-analysis-2-2019-combating-the-manipulation-of-information-a-french-case/)

także wybory parlamentarne (do Sejmu i Senatu RP). Warto w tym kontekście podkreślić, że w 2019 roku w **Ministerstwie Spraw Zagranicznych** utworzono komórkę odpowiedzialną za identyfikację, przeciwdziałanie i reagowanie na kampanie dezinformacyjne. W marcu w MSZ uruchomiony został również *Rapid Alert System*.

Z kolei w maju 2019 roku **Krajowa Rada Radiofonii i Telewizji** przeprowadziła monitoring reklam politycznych umieszczanych na Google, Twitterze i Facebooku przed wyborami do Parlamentu Europejskiego. Działanie to odbywało się w ramach grupy zadaniowej funkcjonującej w ERGA *(European Regulators Group for Audiovisual Media Services)*.

Aktywny na polu przeciwdziałania dezinformacji był również **NASK PIB.** W 2019 roku rozbudowano stronę www.BezpieczneWybory.pl, przeprowadzono warsztaty dla komitetów wyborczych oraz badanie opinii o (dez) informacji w sieci. Ważnym wkładem był także raport ***Dezinformacja w dobie rewolucji cyfrowej,*** opracowany przy współpracy z najważniejszymi ośrodkami przeciwdziałającymi dezinformacji w kraju.


World
Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium
Nam libero tempore, cum soluta nobis est eligendi optio cumque nihil impedit quo minus id quod maxime placeat facere possimus
Lifestyle
Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium
Nam libero tempore, cum soluta nobis est eligendi optio cumque nihil impedit quo minus id quod maxime placeat facere possimus
Business
Quis autem vel eum iure reprehenderit qui in ea voluptate velit esse quam nihil molestiae consequatur
ta
e nihil
axime
et aut
e eveniet ut
non
a sapiente
es alias
iores
natus error
dantium,
nventore
a sunt
enim quibusdam ipsam
luptatem quia voluptas sit
pernatur aut odit aut fugit
90.94
29.87
55.29
94.23
75.35
33.26

Czytaj więcej... – lista ciekawych raportów i publikacji

Cyberbezpieczeństwo

- Komunikat Komisji Europejskiej *Shaping Europe's digital future,* 19 lutego 2020 roku, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en
- S.D. Krasner, *Power, the State, and Sovereignty, Routledge*, London – New York, 2009, https://euagenda.eu/publications/digital-sovereignty-steps-towards-a-new-system-of-internet-governance
- F. Gueham, *Digital Sovereignty*, Foundation Pour L'Innovation Politique, Styczeń 2017
- *Tallinn Manual 2.0 on the International Law application to Cyber Operations;* Międzynarodowa Grupa Ekspertów, Cambridge University Press, Cambridge 2017.
- *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* Lipiec 2010, https://undocs.org/A/65/201
- *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* Czerwiec 2013, https://undocs.org/A/68/98
- *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* Lipiec 2015, https://undocs.org/A/70/174
- J. Chipman, E. Tikk-Ringres, *Evolution of the cyber domain: the implication for National and Global Security,* The International Institute for Strategic Studies, 20015.
- *Strategia bezpieczeństwa cybernetycznego UE: otwarta, bezpieczna i chroniona cyberprzestrzeń,* 7 lutego 2013.
- Komunikat KE, *Wzmacnianie europejskiego systemu odporności cybernetycznej oraz wspieranie konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego,* 5 lipca 2017. https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A52016DC0410
- Komunikat KE, *Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej*, 13 września 2017, https://eur-lex.europa.eu/legal-content/pl/TXT/?uri=CELEX%3A52017JC0450
- *Digital Sovereignty,* Technolpedia, https://www.techopedia.com/definition/33887/digital-sovereignty

Sieć 5G

- *Biała Księga – Pole elektromagnetyczne a człowiek. O fizyce, biologii, medycynie, normach i sieci 5G*, https://www.gov.pl/web/5g/biala-ksiega1
- *Krótka opowieść o społeczeństwie 5.0, czyli jak żyć i funkcjonować w dobie gospodarki 4.0 i sieci 5G*, https://www.digitalpoland.org/assets/publications/krotka-opowiesc-50/krotka-opowiesc-s50.pdf
- *Oddziaływanie elektromagnetycznych fal milimetrowych na zdrowie pracowników projektowanych sieci 5G i populacji generalnej*, http://www.imp.lodz.pl/upload/npz/raport_5g.pdf
- *Analiza wykonalności wdrożenia usług w technologii 5G przy obecnych oraz zwiększonych normach dopuszczalnych poziomów promieniowania elektromagnetycznego*
  - Zadanie A, https://www.il-pib.pl/images/stories/raporty/pdf/PIIT/Raport-IL.-Zadanie-A-Analiza-wykonalnosci-wdrozenia-uslug-w-technologii-5G.pdf
  - Zadanie B, https://www.il-pib.pl/images/stories/raporty/pdf/PIIT/Raport-IL.-Zadanie-B-Analiza-wykonalnosci-wdrozenia-uslug-w-technologii-5G.pdf
- *Strategia 5G dla Polski*, https://www.gov.pl/web/cyfryzacja/strategia-5g-dla-polski
- *Shaping Europe's digital future: 5G Research & Standards*, https://ec.europa.eu/digital-single-market/en/research-standards
- *Shaping Europe's digital future: Towards 5G*, https://ec.europa.eu/digital-single-market/en/towards-5g
- *5G for Europe Action Plan*, https://ec.europa.eu/digital-single-market/en/5g-europe-action-plan
- *European 5G Observatory*, https://ec.europa.eu/digital-single-market/en/european-5g-observatory
- *Commission Recommendation of 26 March 2019 on Cybersecurity of 5G Networks*, https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks
- *EU coordinated risk assessment of the cybersecurity of 5G networks*, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049
- *ENISA threat landscape for 5G Networks*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks
- *Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures*, https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

- *The road to 5G networks*, https://www.oecd-ilibrary.org/science-and-technology/the-road-to-5g-networks_2f880843-en
- *IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond*, https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf
- *Huawei, 5G, and China as a Security Threat*, https://ccdcoe.org/library/publications/huawei-5g-and-china-as-a-security-threat

Umiejętności cyfrowe:

- *The Future of Jobs Report 2018.* Centre for the New Economy and Society. Wrold Economic Forum , http://www3.weforum.org/docs/WEF_Future_of_Jobs_2018.pdf
- *OECD Trends Shaping Education 2019*, OECD Publishing, Paris, https://www.oecd-ilibrary.org/education/trends-shaping-education-2019_trends_edu-2019-en
- *OECD The Future of Work. OECD Employment Outlook 2019*, https://www.oecd-ilibrary.org/employment/oecd-employment-outlook-2019_9ee00155-en
- *ITU Digital Skills Toolkit (2018)*, https://www.itu.int/en/ITU-D/Digital-Inclusion/Documents/ITU%20Digital%20Skills%20Toolkit.pdf
- *OECD Employment Outlook 2019, The Future of Work*, https://www.oecd-ilibrary.org/employment/oecd-employment-outlook-2019_9ee00155-en
- *OECD Skills Strategy 2019*, https://www.oecd-ilibrary.org/education/oecd-skills-strategy-2019_9789264313835-en
- *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Strategia Jednolitego Rynku Cyfrowego dla Europy (2015)*, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52015DC0192&from=EN
- *New Skills Agenda for Europe (2016)*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0381
- *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów ws. Planu działania w dziedzinie edukacji cyfrowej (2018)*, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52018DC0022&from=EN
- *Zalecenie Rady z dnia 22 maja 2018 roku w sprawie kompetencji kluczowych w procesie uczenia się przez całe życie*, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32018H0604(01)&from=EN
- *European Commission: Shaping Europe's Digital Future*, https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf

- *Uchwała nr 8 Rady Ministrów z dn. 14 lutego 2017 roku w sprawie przyjęcia Strategii na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 roku).*, https://www.infor.pl/akt-prawny/MPO.2017.044.0000260,uchwala-nr-8-rady-ministrow-w-sprawie-przyjecia-strategii-na-rzecz-odpowiedzialnego-rozwoju-do-roku-2020-z-perspektywa-do-2030-r.html
- *Założenia do strategii AI w Polsce*, https://www.gov.pl/documents/31305/436699/Za%C5%82o%C5%BCenia_do_strategii_AI_w_Polsce_-_raport.pdf
- *Zintegrowana Strategia Umiejętności 2030 (część ogólna)*, https://efs.men.gov.pl/wp-content/uploads/2019/08/Zintegrowana-Strategia-Umiej%C4%99tno%C5%9Bci-2030-cz%C4%99%C5%9B%C4%87-og%C3%B3lna.pdf
- *Ustawa z dnia 20 lipca 2018 roku Prawo o szkolnictwie wyższym i nauce*, https://www.gov.pl/attachment/1d89db9f-12f3-4186-a72a-ff388f64e481
- *Strategia umiejętności OECD Polska. Wnioski i rekomendacje. Streszczenie Raportu*, http://ibe.edu.pl/download/MEN/Skills-strategy-poland-report-summary-PL.PDF

Sztuczna Inteligencja

- *Polska droga do Strategii AI*, https://www.gov.pl/web/cyfryzacja/ai, strona internetowa opisująca przebieg prac nad polską strategią Sztucznej Inteligencji.
- *Sztuczna Inteligencja w UE*, https://ec.europa.eu/digital-single-market/en/artificial-intelligence, baza wiedzy na temat unijnych działań, wydarzeń i inicjatyw w obszarze Sztucznej Inteligencji.
- *Sztuczna Inteligencja w USA*, https://www.whitehouse.gov/ai/, strona internetowa opisująca inicjatywy i działania regulacyjne w obszarze Sztucznej Inteligencji w USA.
- *OECD.AI Policy Observatory*, https://oecd.ai/dashboards, obserwatorium światowych inicjatyw i działań regulacyjnych w obszarze Sztucznej Inteligencji.
- *ITU AI Repository*, https://www.itu.int/en/ITU-T/AI/Pages/ai-repository.aspx, repozytorium projektów, badań naukowych, think-thanków oraz organizacji rozwijających Sztuczną Inteligencję.
- *Sztucznainteligencja.org.pl*, https://www.sztucznainteligencja.org.pl, polski serwis internetowy popularyzujący wiedzę na temat Sztucznej Inteligencji.
- *Google AI*, https://ai.google/education/, platforma informacyjno-edukacyjna z obszaru Sztucznej Inteligencji.
- *Elements of AI*, https://www.elementsofai.com/, certyfikowany kurs on-line o Sztucznej Inteligencji przygotowany przez Fiński Rząd i Komisję Europejską.
- *Raport Artificial Intelligence Index Report 2019*, https://hai.stanford.edu/sites/g/files/sbiybj10986/f/ai_index_2019_report.pdf, raport na temat Sztucznej Inteligencji przygotowany przez Stanford University's Human-Centered Artificial Intelligence Institute (HAI).

- *Raport EIT Artificial Intelligence activities report 2019*, https://eit.europa.eu/sites/default/files/eit_ai_report_04-online.pdf, raport na temat Sztucznej Inteligencji przygotowany przez European Institute of Innovation and Technology (EIT).
- *Artificial Intelligence An International Journal*, https://www.journals.elsevier.com/artificial-intelligence, międzynarodowe, recenzowane czasopismo naukowe publikujące analizy i wyniki badań z obszaru Sztucznej Inteligencji.

Dezinformacja

- Raport *Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes*, www.cyberpolicy.nask.pl/raport-zjawisko-dezinformacji-w-dobie-rewolucji-cyfrowej-panstwo-spoleczenstwo-polityka-biznes
- *Rezolucja Parlamentu Europejskiego z dnia 10 października 2019 r. w sprawie ingerencji zewnętrznej w wybory i dezinformacji w krajowych i unijnych procesach demokratycznych*, https://www.europarl.europa.eu/doceo/document/TA-9-2019-0031_PL.html
- *Wspólny komunikat do Parlamentu Europejskiego, Rada Europejska, Europejski Komitet Ekonomiczno-Społeczny i Komitet Regionów. Sprawozdanie z realizacji Planu Działania przeciwko dezinformacji*, https://eeas.europa.eu/sites/eeas/files/joint_report_on_disinformation.pdf
- *Kodeks postępowania w zakresie dezinformacji rok później: platformy internetowe przesyłają raporty z samooceny*, https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019
- *Bezpieczne wybory – raport na temat dezinformacji w sieci*, https://bezpiecznewybory.pl/raporty/bezpieczne-wybory-raport-na-temat-dezinformacji-w-sieci
- *Stop dezinformacji. Przewodnik dla dziennikarzy i redakcji*, https://panoptykon.org/wiadomosc/stop-dezinformacji-przewodnik-dla-dziennikarzy-i-redakcji
- *Shaping Europe's digital future: Tackling online disinformation*, https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation
- Portal *EU vs. Disinfo*, https://euvsdisinfo.eu
- *NATO Strategic Communications Centre of Excellence*, https://www.stratcomcoe.org
- *European Centre of Excellence for Countering Hybrid Threats*, https://www.hybridcoe.fi

O autorach

Magdalena Wrzosek – Doktor nauk społecznych. Kierownik Zespołu Analiz Strategicznych i Wpływu Nowoczesnych technologii w NASK PIB, gdzie odpowiada za kwestie strategiczne, regulacyjne i organizacyjne związane z cyberbezpieczeństwa oraz rozwojem nowoczesnych technologii. NLO Europejskiej Agencji ds. Cyberbezpieczeństwa (ENISA). Twórca projektu CyberPolicy (https://cyberpolicy.nask.pl).

W latach 2014-2016 pracowała w Ministerstwie Cyfryzacji, gdzie odpowiadała m.in. za negocjacje Dyrektywy NIS, planowanie i koordynację europejskich ćwiczeń Cyber Europe (edycja 2014 i 2016).

Politolog, kulturoznawca, absolwentka Uniwersytetu Warszawskiego i Uniwersytetu w Konstancji w Niemczech, oraz licznych studiów podyplomowych. Ukończyła także Europejskie Centrum Studiów nad Bezpieczeństwem im. Greaorge'a Marshall'a w Garmisch-Partenkirchen (PCSS oraz SRS). W 2016 roku brała udział w programie dotyczącym cyberbezpieczeństwa, organizowanym przez Departament Stanu USA International Visitor Leadership Program.

Rafał Babraj – Starszy specjalista w zespole Analiz Strategicznych i Wpływu Nowoczesnych Technologii w NASK PIB. Specjalizuje się w analizach dotyczących dezinformacji i strategicznej komunikacji, przede wszystkim w kontekście polityki UE i NATO. Twórca projektu BezpieczneWybory.pl oraz kampanii #OznaczDezinfo.

Doświadczenie zdobywał jako dziennikarz i redaktor, a także pracując w biurach prasowych Mazowieckiego Urzędu Wojewódzkiego oraz Ministerstwa Zdrowia.

Absolwent Instytutu Edukacji Medialnej i Dziennikarstwa na Uniwersytecie Kardynała Stefana Wyszyńskiego w Warszawie. Prywatnie pisarz oraz pasjonat literatury fantastycznej.

Justyna Balcewicz-Majewska – Analityk ds. „czynnika ludzkiego w cyberbezpieczeństwie" w zespole Analiz Strategicznych i Wpływu Nowoczesnych Technologii w PIB NASK. Ekspert w zakresie rozwoju kompetencji cyfrowych, a także przemian transformacji cyfrowej i jej wpływu na społeczeństwo i relacje międzyludzkie.

Doświadczenie zdobywała w firmach sektora energetycznego oraz w sektorze finansowym. Wcześniej pracowała jako koordynator projektów unijnych finansowanych ze Szwajcarsko-Polskiego Programu Współpracy i Norweskiego Mechanizmu Finansowego.

Absolwentka Socjologii Instytutu Stosowanych Nauk Społecznych Uniwersytetu Warszawskiego oraz studiów w Wyższej Szkole Finansów i Zarządzania. W wolnych chwilach pisarka powieści przygodowych dla dzieci i młodzieży.

Paweł Zegarow – Specjalista w zespole Analiz Strategicznych i Wpływu Nowoczesnych Technologii w NASK PIB. Specjalizuje się w analizach dotyczących sztucznej inteligencji i psychologicznych aspektów cyberbezpieczeństwa.

Doświadczenie zdobywał jako badacz i wykładowca na Warszawskim Uniwersytecie Medycznym i Wojskowym Uniwersytecie Medycznym.

Absolwent psychologii na Uniwersytecie Kardynała Stefana Wyszyńskiego w Warszawie, studiów podyplomowych z psychologii klinicznej na Akademii Pedagogiki Specjalnej oraz doktorant Warszawskiego Uniwersytetu Medycznego. Prywatnie fotograf i pasjonat podróży.

NASK

Cyber POLICY

NASK

Cyber POLICY

NASK – Państwowy Instytut Badawczy
ul. Kolska 12, 01-045 Warszawa

nask@nask.pl