

Sprawozdanie z działalności Rady do Spraw Cyfryzacji za rok 2025

Rada do Spraw Cyfryzacji V kadencji została powołana 19 czerwca 2023 r. przez Janusza Cieszyńskiego, Ministra Cyfryzacji, w składzie:

1. Józef Orzeł – Przewodniczący Rady do 17 stycznia 2024 r.,
2. Izabela Albrycht,
3. Katarzyna Chałubińska-Jentkiewicz,
4. Andrzej Dulka,
5. Agnieszka Gryszczyńska,
6. Agnieszka Jankowska – Przewodnicząca Rady od 18 stycznia 2024 r.
7. Jolanta Jaworska,
8. Michał Kanownik,
9. Agnieszka Kister (do 21 stycznia 2024 r.),
10. Janusz Kosiński,
11. Anna Beata Kwiatkowska,
12. Dariusz Milka (do 17 stycznia 2024 r.),
13. Jarosław Mojsiejuk,
14. Marta Poślad,
15. Tomasz Rychter (do 17 stycznia 2024 r.),
16. Krzysztof Silicki,
17. Patrycja Staniszevska,
18. Robert Trętowski,
19. Sławomir Wojciechowski,
20. Małgorzata Zakrzewska

W 2024 r. do składu Rady do Spraw Cyfryzacji V kadencji zostały powołane przez Krzysztofa Gawkowskiego, Wiceprezesa Rady Ministrów, Ministra Cyfryzacji następujące osoby:

- Katarzyna Kopczewska (od 18 stycznia 2024 r.),
- Bianka Siwińska (od 18 stycznia 2024 r.),
- Katarzyna Szymielewicz (od 18 stycznia 2024 r.),
- Jan Maciej Czajkowski (od 3 kwietnia 2024 r.)

W 2025 roku Rada V kadencji funkcjonowała do dnia 18 czerwca 2025 r., tj. do dnia, w którym upływała kadencja Rady. W ciągu sześciu miesięcy 2025 r., Rada zebrała się na dziesięciu posiedzeniach. Tematami prac Rady były następujące zagadnienia:

1. Projekt Strategii Cyberbezpieczeństwa RP 2025-2029
2. Informacja na temat prac nad wdrożeniem portfela tożsamości cyfrowej
3. Systemowe wsparcie w zakresie cyberbezpieczeństwa dla sektora naukowo-badawczego:
 - Skala problemu na podstawie dostępnych danych z raportów firm analitycznych, wniosków z rozmów przeprowadzonych z przedstawicielami pionów IT / cyber uczelni (2024/2025) i debaty na temat bezpieczeństwa badań w kontekście nowego Programu Ramowego FP10
 - Wnioski z badań potrzeb dot. budowania kompetencji w zakresie cyberbezpieczeństwa pionów IT uczelni (2023)
 - Nowe obowiązki uczelni wynikające z NIS2/KSC 2.0 i problem zapewnienia finansowania na realizację tych obowiązków, działania KRASP
 - Wsparcie działań na rzecz rozwoju rozwiązań dla bezpieczeństwa sieci i systemów ICT, w tym inwestycje w R&I dla cyberbezpieczeństwa i kształcenie zaawansowanych kadr oraz badań podstawowych w obszarze AI, cyberbezpieczeństwa i innych technologii ICT w kontekście dyskusji o FP10
 - Krajobraz cyberzagrożeń dla sektora naukowo-badawczego w Polsce
4. System e-CzasPL - w kontekście wyzwań synchronizacji czasu
5. Informacja na temat prac dotyczących Krajowego Planu na rzecz Energii i Klimatu
6. Bezpieczeństwo dzieci w cyfrowym świecie: jakie zjawiska i zagrożenia obserwujemy i jak możemy na nie reagować?
 - „Internet dzieci. Raport z monitoringu obecności dzieci i młodzieży w Internecie” – najważniejsze wyniki oraz kluczowe rekomendacje działań
 - Skala i przyczyny kryzysu zdrowia psychicznego wśród dzieci
7. Ochrona małoletnich przed wykorzystywaniem seksualnym w sieci:
 - Techniczna implementacja zadań Krajowego Planu Przeciwdziałania Przestępstwom Przeciwko Wolności Seksualnej i Obyczajności na Szkodę Małoletnich: Przygotowanie do wdrożenia i wdrożenie systemu wymiany informacji o wartościach hash (zadanie 2.1.12.) oraz przygotowanie do wdrożenia krajowej bazy materiałów przedstawiających wykorzystywanie seksualne dzieci (zadanie 2.4.2.)
 - Postępowania karne dotyczące seksualnego wykorzystywania małoletnich

- Krajowy Plan Przeciwdziałania Przepięstwowm Przeciwko Wolności Seksualnej i Obyczajności na Szkodę Małoletnich i inne działania podejmowane w celu ochrony małoletnich przed seksualnym wykorzystywaniem
8. Dezinformacja – kluczowe zagrożenia oraz sposoby przeciwdziałania
 - Informacja w sprawie działań podejmowanych przez MC
 - Działania podejmowane przez MSZ w zakresie przeciwdziałania dezinformacji, w tym dezinformacji międzynarodowej
 - Diagnoza stanu współpracy z platformami w zakresie zwalczania dezinformacji
 - Jak budować odporność na dezinformację
 9. Stan prac i uwagi organizacji społecznych do projektu ustawy o ochronie małoletnich przed dostępem do treści szkodliwych w Internecie
 10. Dostęp do Informacji Publicznej – wyzwania w kontekście cyberbezpieczeństwa
 11. Informacja w sprawie prac prowadzonych w Ministerstwie Finansów w kontekście cyberbezpieczeństwa
 12. Europejska przestrzeń danych w zdrowiu:
 - Europejska przestrzeń danych dotyczących zdrowia – nowe wyzwania i możliwości
 - Informacja na temat prac Ministerstwa Zdrowia w zakresie przygotowania Polski do wdrożenia założeń unijnych w obszarze europejskiej przestrzeni danych dotyczących zdrowia
 13. Podsumowanie prac Rady ds. Cyfryzacji V kadencji, dyskusja o ewentualnych przyszłych tematach Rady kolejnej kadencji

Na zaproszenie Przewodniczącej Rady w posiedzeniach V kadencji uczestniczyły również osoby spoza grona Rady, np. eksperci, pracownicy Ministerstwa Cyfryzacji. Ponadto, podczas posiedzeń Rady zaproszeni eksperci przedstawiali prezentacje. W roku 2025 na forum Rady V kadencji zostały przedstawione następujące tematy:

1. Projekt Strategii Cyberbezpieczeństwa RP 2025-2029 (XXV posiedzenie z 31 stycznia 2025 r., zaproszeni goście: Łukasz Wojewoda, Dyrektor Departamentu Cyberbezpieczeństwa w MC; Michał Strzelczyk, Naczelnik Wydziału Analiz Cyberbezpieczeństwa w Departamencie Cyberbezpieczeństwa w MC)
2. Systemowe wsparcie w zakresie cyberbezpieczeństwa dla sektora naukowo-badawczego (XXVI posiedzenie z 21 lutego 2025 r., zaproszeni goście: Dariusz Szostek, prof. UŚ, Przewodniczący Komitetu ds. Cyberbezpieczeństwa przy Konferencji Rektorów Akademickich Szkół Polskich (KRASP); Mirosław Kutylowski, Przewodniczący Sekcji Bezpieczeństwa Teleinformatycznego Komitetu Informatyki PAN; Paweł Dziuba, Dyrektor Departamentu Cyberbezpieczeństwa w Ministerstwie

Obrony Narodowej; Wiesław Paluszyński, Prezes Polskiego Towarzystwa Informatycznego; Monika Pieniek, Zastępca Dyrektora Departamentu Cyberbezpieczeństwa w MC; Marcin Wysocki, Zastępca Dyrektora Departamentu Cyberbezpieczeństwa w MC)

3. System e-CzasPL - w kontekście wyzwań synchronizacji czasu (XXVII posiedzenie z 7 marca 2025 r., zaproszeni goście: Maciej Gruszczyński, Kierownik Laboratorium Nowych Technologii Czasu i Długości w Głównym Urzędzie Miar; Tomasz Widomski, Członek Rady Nadzorczej Elproma oraz krajowy delegat MC KPRM do ITU)
4. Informacja na temat prac dotyczących Krajowego Planu na rzecz Energii i Klimatu (XXVII posiedzenie z 7 marca 2025 r., zaproszeni goście: Wojciech Racięcki, Dyrektor Departamentu Strategii i Analiz w Ministerstwie Klimatu i Środowiska)
5. Bezpieczeństwo dzieci w cyfrowym świecie: jakie zjawiska i zagrożenia obserwujemy i jak możemy na nie reagować? (XXVIII posiedzenie z 21 marca 2025 r., zaproszeni goście: Konrad Ciesiołkiewicz, Współautor raportu "Internet dzieci", Członek Państwowej Komisji ds. przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15; Anna Dzielska, Adiunkt, p.o. Kierownika, Zakład Zdrowia Dzieci i Młodzieży, Instytut Matki i Dziecka; Wojciech Kulesza, Psycholog społeczny, Kierownik Katedry Psychologii Społecznej - Uniwersytet SWPS; Aleksandra Lewandowska, Konsultantka Krajowa w dziedzinie psychiatrii dzieci i młodzieży; Martyna Różycka, Kierownik Działu Reagowania na Nielegalne Treści w Internecie Dyżurnet.pl w NASK)
6. Ochrona małoletnich przed wykorzystywaniem seksualnym w sieci (XXIX posiedzenie z 17 kwietnia 2025 r., zaproszeni goście: Adam Cieślak, Komendant Centralnego Biura Zwalczania Cyberprzestępczości; Małgorzata Kluz, Prokurator Prokuratury Regionalnej, Departament Postępowania Przygotowawczego w Prokuraturze Krajowej; Katarzyna Sienkiewicz, Specjalista w Departamencie Cyberbezpieczeństwa w MC; Martyna Różycka, Kierownik Działu Reagowania na Nielegalne Treści w Internecie Dyżurnet.pl w NASK; Natalia Bender, Zastępca Dyrektora Departamentu Analiz i Strategii w Ministerstwie Sprawiedliwości; Aneta Ceglińska, Naczelnik Wydziału do walki z Handlem Ludźmi Biura Kryminalnego Komendy Głównej Policji; Konrad Ciesiołkiewicz, Członek Państwowej Komisji ds. przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15; Piotr Kubiak, Ekspert Wydziału do walki z Handlem Ludźmi Biura Kryminalnego Komendy Głównej Policji; Agnieszka Matysek, Główny Specjalista – Sędzia, Wydział Praw Dziecka i Ochrony Pokrzywdzonych, Departament Spraw Rodziny i Nieletnich w Ministerstwie Sprawiedliwości)
7. Dezinformacja – kluczowe zagrożenia oraz sposoby przeciwdziałania (XXX posiedzenie z 25 kwietnia 2025 r., zaproszeni goście: Katarzyna Nosalska, Dyrektor Centrum Rozwoju Kompetencji Cyfrowych w MC; Katarzyna Szaran, Dyrektor

Departamentu Komunikacji Strategicznej i Przeciwdziałania Dezinformacji Międzynarodowej w Ministerstwie Spraw Zagranicznych; Agnieszka Lipińska, Kierownik Ośrodka Analizy Dezinformacji w NASK; Patryk Zakrzewski, Wiceprezes Stowarzyszenia Demagog; Karina Stasiuk-Krajewska, prof. Uniwersytetu SWPS, badaczka Central European Digital Media Observatory)

8. Stan prac i uwagi organizacji społecznych do projektu ustawy o ochronie małoletnich przed dostępem do treści szkodliwych w Internecie (XXXI posiedzenie z 9 maja 2025 r., zaproszeni goście: Dorota Głowacka, Specjalistka ds. rzecznictwa i litygacji w Fundacji Panoptikon; Marzena Sawicka, Dyrektor Departamentu Telekomunikacji w MC; Katarzyna Sienkiewicz, Specjalista w Departamencie Cyberbezpieczeństwa w MC)
9. Europejska przestrzeń danych w zdrowiu (XXXII posiedzenie z 23 maja 2025 r., zaproszeni goście: Andrzej Ryś; Wojciech Demediuk, Dyrektor Departamentu e-Zdrowia w Ministerstwie Zdrowia; Grzegorz Borowiec, Zastępca Dyrektora Departamentu e-Zdrowia w Ministerstwie Zdrowia; Emilia Krawczyk, Główny specjalista w Departamencie e-Zdrowia w Ministerstwie Zdrowia; Artur Pruszek, Ekspert Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji)

Informacja o zespołach roboczych działających w ramach Rady V kadencji:

W celu realizacji Planu pracy Rady ds. Cyfryzacji V kadencji, który został przyjęty w pierwszym kwartale 2024 r., poza pracami realizowanymi na posiedzeniach Rady, odbywały się liczne spotkania zespołów roboczych, których efektem prac były opracowania merytoryczne oraz rekomendacje stanowiące bazę do stanowisk Rady, a także jej aktywności na posiedzeniach.

Poniżej przedstawiono działania podjęte w ramach zespołów roboczych w roku 2025.

W roku 2025 kontynuowane były prace Rady w szczególności w obszarze cyberbezpieczeństwa, m.in. w tematach: strategii cyberbezpieczeństwa RP, zagrożeń związanych z atakami na systemy synchronizacji czasu, bezpieczeństwa sektora naukowo-badawczego, cyberbezpieczeństwa w sektorze medycznym czy dotyczących innych zagadnień związanych z szeroko pojętym bezpieczeństwem jak bezpieczeństwo dzieci i młodzieży w cyfrowym świecie, zagrożenia oraz sposoby przeciwdziałania dezinformacji, wdrażanie portfela tożsamości cyfrowej, europejska przestrzeń danych w sektorze zdrowia, cyberbezpieczeństwo w elektroenergetyce, wyzwania cyberbezpieczeństwa związane z dostępem do informacji publicznej czy cyberprzestępczość – w szczególności związana z tzw. oszustwami inwestycyjnymi.

- [Cyberbezpieczeństwo](#)

Zespół koncentrował się na zagadnieniach związanych z budową systemowej odporności państwa w obszarze cyberbezpieczeństwa, w szczególności w kontekście prac nad Strategią Cyberbezpieczeństwa RP na lata 2025–2029, implementacji regulacji europejskich (NIS2/KSC

2.0), a także identyfikacji potrzeb sektorowych, w tym sektora naukowo-badawczego oraz ochrony zdrowia. W ramach zespołu podjęto również prace na rzecz analizy kwestii związanych z dostępem do informacji publicznej w kontekście rosnących wymagań cyberbezpieczeństwa, ochrony danych i systemów teleinformatycznych, a w szczególności równoważenia transparentności i bezpieczeństwa.

Jedno z posiedzeń Rady było w całości poświęcone zagadnieniu konieczności systemowego wsparcia w zakresie cyberbezpieczeństwa dla sektora naukowo-badawczego. Spotkanie odbyło się z udziałem zaproszonych gości reprezentujących środowisko naukowe i akademickie. Przedstawiona została skala cyberzagrożeń, przykłady cyberataków w tym sektorze i konieczność strategicznej, systemowej współpracy pomiędzy sektorem rządowym, akademickim i przemysłem. Dyskutowano również zagadnienia budowania kompetencji pionierów IT uczelni oraz kadr uczelni, nowych obowiązków wynikających z NIS2/KSC 2.0, kwestii finansowania i konieczności inwestycji w tym obszarze. Na bazie przeprowadzonych dyskusji powstało w marcu 2025 r. Stanowisko Rady dotyczące konieczności systemowego wsparcia cyberbezpieczeństwa w sektorze naukowo-badawczym.

Kolejnym tematem była kwestia wyzwań związanych z synchronizacją czasu w funkcjonowaniu systemów teleinformatycznych w wielu kluczowych sektorach gospodarki. Poświęcono temu dedykowane posiedzenie z udziałem gości z Głównego Urzędu Miar, który opracował i wdrożył ogólnodostępny, innowacyjny system e-CzasPL pozwalający na synchronizację do wiarygodnego, urzędowego źródła czasu i częstotliwości w Polsce. Omawiano zagrożenia i incydenty związane z globalnymi atakami na synchronizację czasu i korzyści ze stosowania systemu e-CzasPL. Wskazywano równocześnie na zbyt małe rozpropagowanie informacji o tym systemie wśród podmiotów sektorów energetyki, transportu, czy rynków finansowych. W konsekwencji Rada przyjęła w maju 2025 r. Stanowisko dotyczące systemu dystrybucji czasu urzędowego w RP – e-CzasPL, w którym m.in. wskazano na konieczność upowszechnienia tego systemu w administracji publicznej i kluczowych sektorach gospodarki.

W sprawie cyberbezpieczeństwa sektora medycznego, z uwagi na wzrost cyberincydentów i zagrożeń, Rada przyjęła stanowisko zawierające szereg rekomendacji, w tym konieczność określenia minimalnych wymagań dla komercyjnych aplikacji gabinetowych czy podmiotów prowadzących rejestry medyczne, jak również szerokie wdrożenie mechanizmów dwuskładnikowego uwierzytelnienia.

Podsumowując, w I półroczu 2025 r. prace zespołu obejmowały wypracowanie rekomendacji dotyczących:

- modelu wsparcia cyberbezpieczeństwa dla uczelni i instytucji badawczych (w tym finansowania nowych obowiązków regulacyjnych),
- cyberbezpieczeństwa w sektorze ochrony zdrowia,
- rozwoju kompetencji kadrowych w obszarze cyberbezpieczeństwa, zarówno w sektorze naukowym, jak i ochrony zdrowia,

- wzmocnienia krajowego ekosystemu badań i innowacji (R&I) w obszarze AI i cyberbezpieczeństwa, także w kontekście przygotowań do Programu Ramowego UE.
- [Odporność cyfrowa państwa](#)

Zespół zajmował się zagadnieniami dotyczącymi infrastruktury krytycznej i systemów wspierających funkcjonowanie państwa, w tym analizą systemu e-CzasPL w kontekście zapewnienia precyzyjnej synchronizacji czasu, powiązaniem między cyfryzacją a polityką energetyczno-klimatyczną (Krajowy Plan na rzecz Energii i Klimatu) oraz odpornością infrastruktury na zakłócenia.

W pierwszej połowie 2025 r. szczególną uwagę poświęcono:

- znaczeniu synchronizacji czasu dla bezpieczeństwa systemów finansowych i telekomunikacyjnych,
- integracji polityk cyfrowych i energetycznych,
- zapewnieniu ciągłości działania kluczowych systemów państwowych.
- [Ochrona dzieci i młodzieży w cyberprzestrzeni](#)

Istotnym obszarem prac Rady ds. Cyfryzacji V kadencji było bezpieczeństwo dzieci i młodzieży w środowisku cyfrowym, ze szczególnym uwzględnieniem problemu wykorzystywania seksualnego małoletnich w sieci. Tematyce tej poświęcono kilka posiedzeń Rady, z udziałem przedstawicieli administracji publicznej, organów ścigania, środowiska naukowego oraz organizacji społecznych.

Prace zespołu koncentrowały się na identyfikacji działań niezbędnych do zwiększenia poziomu ochrony małoletnich, w tym przeciwdziałaniu rozpowszechnianiu materiałów CSAM oraz usprawnieniu postępowań karnych w tym zakresie. Analizowano zarówno stan krajowych rozwiązań, jak i inicjatywy na poziomie UE, w tym projekt rozporządzenia dotyczącego zapobiegania i zwalczania wykorzystywania seksualnego dzieci, a także wdrażanie Krajowego Planu Przeciwdziałania Przystępstwom na Szkodę Małoletnich na lata 2023–2026.

Efektom prac było przyjęcie stanowiska Rady, zawierającego rekomendacje działań systemowych. W szczególności wskazano na konieczność pilnego wdrożenia rozwiązań przewidzianych w Krajowym Planie, w tym utworzenia Krajowej Bazy Hash CSAM oraz Krajowej Bazy CSAM jako odrębnych systemów teleinformatycznych. Zarekomendowano również wprowadzenie jednolitej klasyfikacji materiałów CSAM zgodnej ze standardami międzynarodowymi, rozwój narzędzi opartych na sztucznej inteligencji do identyfikacji i analizy treści nielegalnych, a także zapewnienie odpowiedniego wsparcia szkoleniowego i psychologicznego dla służb zaangażowanych w prowadzenie tego typu spraw. Rekomendacje Rady zostały uwzględnione i zaowocowały podjęciem prac nad projektem ustawy o krajowym systemie przetwarzania, analizy i klasyfikacji treści przedstawiających seksualne wykorzystywanie małoletnich (UD306, [Projekt ustawy o krajowym systemie przetwarzania,](#)

analizy i klasyfikacji treści przedstawiających seksualne wykorzystywanie małoletnich - Kancelaria Prezesa Rady Ministrów - Portal Gov.pl).

Działania zespołu w 2025 r. obejmowały ponadto analizę raportów dotyczących aktywności dzieci w Internecie i ich dobrostanu psychicznego, opiniowanie projektów legislacyjnych (w tym ustawy o ochronie małoletnich przed treściami szkodliwymi), wspieranie wdrażania rozwiązań technicznych oraz współpracę z interesariuszami.

- Kompetencje cyfrowe, edukacja cyfrowa

Ważnym elementem aktywności Państwa na rzecz wzmocnienia odporności państwa i odporności obywateli jest walka z dezinformacją w przestrzeni cyfrowej. W swym stanowisku z czerwca 2025 r. Rada podkreśla między innymi istotną rolę mechanizmu ISAC – Centrum Wymiany i Analizy Informacji jako instrumentu dobrowolnej współpracy na zasadzie partnerstwa, podmiotów z danego obszaru (sektora, branży, ale także jako inicjatywa dziedzinowa) dla zapewnienia cyberbezpieczeństwa, który to instrument mógłby zostać stworzony w kraju, w celu skuteczniejszej walki z dezinformacją.

W ramach zespołu podjęto działania obejmujące analizę problematyki zjawiska dezinformacji, w szczególności zmierzające do identyfikacji kluczowych zagrożeń informacyjnych (krajowych i międzynarodowych), analizy współpracy z platformami internetowymi, jak również analizy wyzwań w zakresie budowania odporności społecznej.

W pierwszym półroczu 2025 r. zespół:

- współpracował z administracją rządową oraz ośrodkami analitycznymi,
 - identyfikował luki w systemie reagowania na dezinformację,
 - formułował rekomendacje dotyczące edukacji cyfrowej i komunikacji strategicznej państwa.
- Rejestry referencyjne, otwarcie danych

W ramach prac zespołu podjęto analizę inicjatywy Europejskiej Przestrzeni Danych w Zdrowiu (EHDS) i przygotowania Polski do wdrożenia unijnych regulacji w obszarze danych zdrowotnych, jak również dyskutowano nad możliwościami, szansami oraz wyzwaniami związanymi z przetwarzaniem danych w sektorze publicznym.

[Dokumenty Rady ds. Cyfryzacji V kadencji 2025 r.](#)

Informacje dotyczące działalności Rady są zamieszczane w wydzielonej części [Biuletynu Informacji Publicznej](#)¹ na stronach ministra właściwego do spraw informatyzacji oraz na [stronie internetowej](#). Dostępne są tam protokoły ze wszystkich posiedzeń Rady oraz stanowiska/opinie RdC, tj.

¹ od 16 lutego 2026 r. Biuletyn Informacji Publicznej Ministerstwa Cyfryzacji funkcjonuje w ramach witryny www.gov.pl/cyfryzacja

- [Stanowisko Rady do Spraw Cyfryzacji dotyczące konieczności systemowego wsparcia cyberbezpieczeństwa sektora naukowo-badawczego w Polsce.](#)
- [Stanowisko Rady do Spraw Cyfryzacji w sprawie cyberbezpieczeństwa w sektorze medycznym.](#)
- [Stanowisko Rady do Spraw Cyfryzacji dotyczące systemu dystrybucji czasu urzędowego w Rzeczypospolitej Polskiej – eCzasPL.](#)
- [Stanowisko Rady do Spraw Cyfryzacji w sprawie rozwoju technologii przełomowych.](#)
- [Stanowisko Rady do Spraw Cyfryzacji w sprawie działań na rzecz zwalczania dezinformacji.](#)
- [Stanowisko Rady do Spraw Cyfryzacji wraz z rekomendacjami w zakresie działań niezbędnych do podjęcia w celu ochrony małoletnich przed wykorzystaniem seksualnym w sieci.](#)