Internet. Cyberodporność

CZĘŚĆ I
Aktualne zagrożenia i ich przezwyciężanie

Krzysztof Gawkowski

Rozdział 1.
Strategiczne działania Ministra Cyfryzacji w przezwyciężaniu cyberzagrożeń

§ 1. Formalne aspekty Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej

Przyjęcie i realizacja Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej stanowi kluczowy obowiązek wynikający z przepisów CyberbezpU. Ze względu na to, że z końcem 2024 r. upłynął okres obowiązywania Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024[1], a także biorąc pod uwagę dynamicznie zmieniające się uwarunkowania w obszarze cyberbezpieczeństwa, konieczne stało się opracowanie nowego dokumentu strategicznego, który odpowie na współczesne zagrożenia[2].

Odpowiedzialność za przygotowanie projektu Strategii[3] spoczywa na ministrze właściwym do spraw informatyzacji, działającym we współpracy z Pełnomocnikiem Rządu do Spraw Cyberbezpieczeństwa[4] oraz z innymi ministrami i kierownikami urzędów centralnych[5]. Projekt nowej Strategii został opracowany w Ministerstwie Cyfryzacji, z uwzględnieniem wyników prekonsultacji przeprowadzonych z partnerami rządowymi i innymi instytu-

[1] Przyjęta uchwałą Nr 125 Rady Ministrów w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 z 22.10.2019 r. (M.P. poz. 1037, nie obowiązuje) – dalej: Strategia na lata 2019–2024.

[2] Ustawa z 5.7.2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2024 r. poz. 1077 ze zm.), art. 45 ust. 1 pkt 1.

[3] Na potrzeby niniejszego opracowania termin „Strategia" będzie używany zgodnie z jego znaczeniem zawartym w art. 45 ust. 1 pkt 1 CyberbezpU.

[4] Zgodnie z art. 4 pkt 19 CyberbezpU: Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa, zwany jest dalej „Pełnomocnikiem".

[5] Art. 70 ust. 1 CyberbezpU.

cjami publicznymi. Strategia zgodnie z CyberbezpU przyjmowana jest w drodze uchwały Rady Ministrów, co wiąże się z przeprowadzeniem uzgodnień i opiniowania w ramach rządowego procesu legislacyjnego. Dokument wpisuje się w ewolucyjny nurt rozwoju polityki cyberbezpieczeństwa, adaptując wcześniejsze rozwiązania do aktualnych realiów technologicznych, prawnych, międzynarodowych oraz krajowych. Uwzględniono w nim m.in. zmiany wynikające z rozwoju technologii (takie jak kryptografia postkwantowa, rozwiązania chmurowe), w tym również przekształcenia, jakie zaszły w środowisku bezpieczeństwa międzynarodowego[6] oraz w funkcjonowaniu Krajowego Systemu Cyberbezpieczeństwa (KSC)[7], i wnioski, jakie zostały wyciągnięte z dotychczasowej praktyki działania tego systemu. Chociaż Strategia została opracowana przy aktualnym stanie prawnym, zawiera również elementy przygotowujące system na wdrożenie dyrektywy NIS 2, której transpozycja do polskiego porządku prawnego wymaga nowelizacji CyberbezpU. Wśród mechanizmów usprawniających wdrożenie i rozliczalność, wprowadzanych przez Strategię, znalazł się załącznik w postaci Planu działań[8], zawierający konkretne zadania i odpowiadające im środki realizacyjne, co sprzyja zarówno wdrożeniu Strategii, jak i kontroli jej wykonania.

Zarówno cele główne, jak i szczegóły dokumentu pozostają pokrewne z tymi zawartymi w Strategii na lata 2019–2024, jednak z tą różnicą, że postawione zadania zostały zaktualizowane i dostosowane do obecnych realiów. W ramach nowej Strategii przewidziano wiele inicjatyw, takich jak:

1) powołanie centralnej instytucji koordynującej cyberbezpieczeństwo na poziomie krajowym (bazującej na Połączonym Centrum Operacyjnym Cyberbezpieczeństwa – PCOC);
2) utworzenie lub rozwój sektorowych zespołów CSIRT;
3) dalsze działania wspierające cyberbezpieczeństwo w samorządach;
4) utworzenie Centrum Cyberbezpieczeństwa NASK.

Ponadto planowane są działania związane z rozwojem bezpiecznej łączności, migracją do kryptografii postkwantowej, wdrażaniem rozwiązań chmurowych dla informacji niejawnych oraz doskonaleniem Systemu S46[9].

Istotną rolę w nowej Strategii odgrywają także przedsięwzięcia ukierunkowane na wzmacnianie bezpieczeństwa łańcucha dostaw, rozwój krajowych technologii oraz zwiększanie suwerenności technologicznej. Szczególną wagę

[6] Sprawozdanie Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa za 2024 rok, s. 16–18, https://www.gov.pl/attachment/42dd5b60-d5b4-41f7-ba1f-20c842070cf0 (dostęp: 16.9.2025 r.).
[7] Tamże, s. 35.
[8] Projekt Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025–2029, s. 45–77, https://mc.bip.gov.pl/fobjects/download/2026757/uzg-_projekt-_strategia-cyberbezpieczenstwa-rp-2025-2029-docx.html (dostęp: 16.9.2025 r.).
[9] Pod pojęciem systemu S46 rozumie się system teleinformatyczny wymieniony w art. 46 ust. 1 CyberbezpU, wspierający działania podmiotów wskazanych w tej ustawie, https://www.gov.pl/web/popcwsparcie/podlaczenie-podmiotow-krajowego-systemu-cyberbezpieczenstwa-do-zintegrowanego-systemu-zarzadzania-cyberbezpieczenstwem-s46-s46-react (dostęp: 16.9.2025 r.).

przywiązano także do wdrażania wymogów cyberbezpieczeństwa w zamówieniach publicznych, a także do dalszego rozwoju centralnie zapewnianej ochrony przed atakami DDoS, którą Ministerstwo Cyfryzacji już obecnie zapewnia dla kilkudziesięciu instytucji administracji publicznej oraz dla Sił Zbrojnych RP. Przewidziano także intensyfikację działań szkoleniowych kierowanych do różnych grup społecznych (w tym do dzieci, seniorów czy pracowników MŚP). Współpraca międzynarodowa, zarówno w ramach UE i NATO, jak i w formatach dwustronnych, została wskazana jako jeden z fundamentów wzmacniania krajowego systemu cyberbezpieczeństwa.

Co warte podkreślenia, przeciwdziałanie i zwalczanie cyberprzestępczości zostało ujęte w projektowanej Strategii jako odrębny cel szczegółowy. W dokumencie wskazano trzy zasadnicze kierunki działań w tym zakresie: tworzenie skuteczniejszych regulacji prawnych, wzmacnianie wyspecjalizowanych struktur oraz rozwijanie zdolności analitycznych organów ścigania, służb specjalnych i wymiaru sprawiedliwości z wykorzystaniem nowych technologii. Zapewnienie bezpieczeństwa w cyberprzestrzeni, w warunkach dynamicznego rozwoju technologii informacyjnych, stanowi jedno z podstawowych zadań państwa. Z raportów Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa wynika, że większość incydentów ma charakter przestępstw motywowanych finansowo, w szczególności oszustw komputerowych[10]. Skala tego zjawiska wskazuje na potrzebę zapewnienia organom ścigania adekwatnych narzędzi prawnych i technicznych do jego zwalczania przez zniesienie ograniczeń obowiązujących regulacji. W odpowiedzi na zidentyfikowane problemy Strategia przewiduje inicjatywy legislacyjne i organizacyjne, których celem jest zwiększenie skuteczności wykrywania i ścigania sprawców przestępstw w cyberprzestrzeni. Wśród proponowanych rozwiązań wymienić można m.in. wprowadzenie obowiązku retencjonowania informacji o portach przypisanych do adresów IP, co umożliwi skuteczniejszą identyfikację sprawców. Ustanowienie kontratypów działań operacyjnych w cyberprzestrzeni, zapewniających ochronę funkcjonariuszom działającym w interesie publicznym i pod nadzorem sądowym. Ponadto dokument zakłada uproszczenie dostępu do danych objętych tajemnicą bankową, co przyspieszy gromadzenie materiału dowodowego w początkowej fazie postępowań oraz stworzenie mechanizmu blokowania stron internetowych wykorzystywanych do działalności przestępczej.

Oprócz Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025–2029 Ministerstwo Cyfryzacji prowadzi równoległe prace nad projektem Strategii Cyfryzacji Państwa do 2035 r., mając na uwadze to, aby w zakresie cyberbezpieczeństwa oba dokumenty strategiczne były spójne. Przy czym

[10] Sprawozdanie Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, s. 42.

Strategia na lata 2025–2029 dla obszaru cyberbezpieczeństwa będzie w naturalny sposób wiodąca i bardziej szczegółowa.

Możliwie szybkie przyjęcie i wdrożenie nowej Strategii na lata 2025–2029 jest warunkiem skutecznego reagowania na zagrożenia oraz wzmacniania odporności państwa na wyzwania w cyberprzestrzeni. Nowa Strategia stanie się drogowskazem dla KSC: usprawni zarządzanie strategiczne i podniesie poziom ochrony obywateli oraz instytucji państwowych.

§ 2. Wyzwania strategiczne dla cyberbezpieczeństwa

W erze globalnych konfliktów informacyjnych i ataków w cyberprzestrzeni Polska aspiruje do stania się wiodącym krajem kształtującym regulacje cyfrowe w ramach wspólnoty euroatlantyckiej – nie tylko z uwagi na swoje położenie geograficzne i sąsiedztwo z Rosją, lecz także ze względu na rosnące znaczenie polityczne oraz tzw. globalne zmiany geopolityczne, w których nasz kraj odgrywa coraz większe znaczenie[11]. Dzięki dynamicznemu rozwojowi kompetencji w zakresie cyberbezpieczeństwa, inwestycjom w infrastrukturę cyfrową oraz aktywnej roli w strukturach NATO i Unii Europejskiej znaczenie Polski w obszarze cyfryzacji uległo na przestrzeni ostatnich kilku lat pozytywnym przeobrażeniom.

W 2024 r. zespoły CSIRT funkcjonujące na poziomie krajowym obsłużyły łącznie ponad 111 tys. incydentów, co stanowi wzrost o 23% względem roku poprzedniego. Sam CSIRT NASK zarejestrował ponad 103 tys. zdarzeń, odnotowując ich wzrost o 29%. Do najczęstszych incydentów należały oszustwa komputerowe (ponad 97 tys. przypadków), wykrycie szkodliwego oprogramowania (ponad 1800 przypadków) oraz podatności usług (ponad 1600 przypadków)[12]. Dane te jednoznacznie wskazują na rosnącą aktywność cyberprzestępców oraz konieczność dalszego doskonalenia systemów ochrony teleinformatycznej.

Nie tylko liczba incydentów, ale także ich charakter wskazuje na pogłębiającą się skalę zagrożeń. Choć wiele ataków ma charakter masowy, jak w przypadku kampanii phishingowych, również tego rodzaju działania wymagają reakcji i przeciwdziałania, ponieważ stanowią realne zagrożenie dla obywateli. Szczególnie niebezpieczne są jednak zaawansowane operacje grup APT[13], powiązanych ze służbami wrogo nastawionych Polsce państw, których celem jest pozyskiwanie wrażliwych danych, zakłócanie działania krytycznych

[11] DIIS – Danish Institute for International Studies, Power moves east: Poland's rise as a strategic European player, https://www.diis.dk/en/research/power-moves-east-polands-rise-as-a-strategic-european-player (dostęp: 16.9.2025 r.).
[12] Sprawozdania Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa.
[13] Advanced Persistent Threat (APT, pol. zaawansowane, trwałe zagrożenie), https://www.cisco.com/site/us/en/learn/topics/security/what-is-an-advanced-persistent-threat-apt.html (dostęp: 16.9.2025 r.).

systemów lub przygotowanie do przyszłych ataków o charakterze strategicznym[14].

Coraz częściej celem ataków są także podmioty odgrywające kluczową rolę w łańcuchach dostaw dla infrastruktury krytycznej oraz instytucje administracji publicznej. Ministerstwo Cyfryzacji, we współpracy z Zespołami Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT), działającymi na poziomie krajowym, prowadzonymi przez: Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy (CSIRT NASK), Szefa Agencji Bezpieczeństwa Wewnętrznego (CSIRT GOV), Ministra Obrony Narodowej (CSIRT MON); Policją, służbami specjalnymi, m.in.: Agencją Bezpieczeństwa Wewnętrznego (ABW), Służbą Kontrwywiadu Wojskowego (SKW) oraz Pełnomocnikiem Rządu do Spraw Cyberbezpieczeństwa (umocowanym w Ministerstwie Cyfryzacji), prowadzi skoordynowane działania mające na celu przeciwdziałanie tym zagrożeniom[15].

Współczesna sytuacja geopolityczna w Europie, zwłaszcza trwająca wojna Rosji przeciwko Ukrainie, znacząco zwiększa ryzyko cyberataków. Polska jako kraj wspierający Ukrainę i pełniący funkcję logistycznego zaplecza, staje się jednym z głównych celów ataków wymierzonych w infrastrukturę transportową i informatyczną. Jednocześnie rośnie aktywność grup haktywistycznych, organizacji przestępczych działających dla zysku, jak również grup sponsorowanych przez obce państwa[16].

Wobec dynamicznie zmieniającego się krajobrazu zagrożeń – wynikającego z postępu technologicznego – konieczne jest ciągłe udoskonalanie KSC. Ministerstwo Cyfryzacji oraz inne instytucje odpowiedzialne za bezpieczeństwo teleinformatyczne na poziomie krajowym podejmują działania o charakterze regulacyjnym, organizacyjnym, technicznym oraz kompetencyjnym. Wśród nich znajdują się te: z zakresu regulacyjno-systemowego – np. projekt nowelizacji CyberbezpU, mający na celu wdrożenie dyrektywy NIS 2; z zakresu szkoleniowo-kompetencyjnego – np. programy szkoleniowe dla społeczeństwa, specjalistów i administracji publicznej czy inicjatywy takie jak Fundusz Cyberbezpieczeństwa, umożliwiający sektorowi publicznemu konkurowanie o ekspertów z sektorem prywatnym; z zakresu organizacyjnego – np. wzmocnienie roli Kolegium do Spraw Cyberbezpieczeństwa oraz operacyjne zarządzanie incydentami przez Połączone Centrum Operacyjne Cyberbezpieczeństwa; z zakresu rozwiązań technicznych – np. system rozpoznawania zagrożeń w cyberprzestrzeni (CTI), zapewniany przez Ministerstwo Cyfryzacji, środki bezpiecznej łączności: Komunikator i SKR-Z, system

[14] Raport roczny 2024 z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu, Państwowy Instytut Badawczy NASK, Warszawa 2025, s. 33–38, https://cert.pl/uploads/docs/Raport_CP_2024.pdf (dostęp: 16.9.2025 r.).
[15] Sprawozdanie Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, s. 20.
[16] Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2024 r., s. 53–78, https://csirt.gov.pl/download/3/221/RaportostaniebezpieczenstwacyberprzestrzeniRPw2024.pdf (dostęp: 16.9.2025 r.).

AntyDDoS, którym Ministerstwo Cyfryzacji zapewnia osłonę przed atakami DDoS dla kilkudziesięciu instytucji, w tym dla Sił Zbrojnych RP, system zarządzania cyberbezpieczeństwem S46. Wśród inicjatyw, które wzmacniają bezpieczeństwo Polski, należy wymienić również programy wsparcia dla poszczególnych sektorów, np. Cyberbezpieczny Samorząd, Cyberbezpieczny Rząd, Cyberbezpieczne Wodociągi.

§ 3. Przewidywania dotyczące rozwoju cyberzagrożeń

Prognozy odnoszące się do rozwoju cyberzagrożeń jednoznacznie wskazują na utrzymanie trendu wzrostowego zarówno w zakresie liczby incydentów, jak i ich złożoności. W nadchodzących latach przewiduje się dalsze wykorzystywanie luk bezpieczeństwa o różnym poziomie skomplikowania i krytyczności w systemach instytucji publicznych i podmiotów prywatnych. Szczególnie niebezpieczne są ataki na łańcuchy dostaw, które – choć pośrednie – mogą wywoływać równie poważne skutki, jak bezpośrednie uderzenia w systemy docelowe.

Utrzymującym się zagrożeniem pozostaje brak wdrożenia wieloskładnikowego uwierzytelniania (MFA) przez wiele instytucji, w tym operatorów infrastruktury krytycznej oraz jednostki administracji publicznej. Zjawisko to stanowi istotne ryzyko w kontekście rosnącej liczby ataków sponsorowanych przez obce państwa, w tym prowadzonych przez zaawansowane grupy APT.

Coraz częściej wykorzystywanym wektorem ataku stają się podatności w oprogramowaniu i urządzeniach brzegowych, wypierając tym samym klasyczne techniki, takie jak phishing czy złośliwe oprogramowanie przesyłane drogą mailową. Jednocześnie obserwuje się wzrost liczby cyberataków wymierzonych w elementy przemysłowej infrastruktury krytycznej dostępnej z poziomu sieci, a także w urządzenia Internetu Rzeczy (IoT) oraz systemy autonomiczne. Skalę zagrożeń potęguje fakt, że wiele z tych urządzeń nie posiada odpowiednich mechanizmów ochronnych lub jest nieprawidłowo skonfigurowanych.

W sferze zagrożeń dla obywateli prognozuje się dalszy rozwój technik socjotechnicznych. Oszustwa będą stawać się coraz bardziej wyrafinowane i trudniejsze do rozpoznania. Wzrośnie liczba kampanii, w których wykorzystana zostanie generatywna sztuczna inteligencja, służąca do tworzenia fałszywego głosu, wizerunku czy narracji medialnej. Tego typu ataki będą miały na celu nie tylko oszustwa finansowe, lecz także dezinformację, wpływ na opinię publiczną czy destabilizację społeczną.

Wobec złożoności i nieprzewidywalności zagrożeń niezbędne jest wzmocnienie współpracy pomiędzy podmiotami KSC, w tym wymiana informacji, tworzenie wspólnych platform i forum wymiany wiedzy eksperckiej.

Tylko w ten sposób możliwe będzie odpowiednio wczesne wykrywanie zagrożeń i skuteczne reagowanie na incydenty.

Szczególne znaczenie w nadchodzących latach zyska rozwój technologii kwantowych. Komputery kwantowe, choć obecnie jeszcze na wczesnym etapie rozwoju, mogą w przyszłości doprowadzić do przełamania aktualnie stosowanych zabezpieczeń kryptograficznych. Dlatego już dziś konieczne jest wdrażanie kryptografii postkwantowej (PQC) w systemach szyfrowania i transmisji danych oraz rozwijanie krajowego potencjału w zakresie kryptografii i łączności kwantowej.

§ 4. Inwestycje w cyberbezpieczeństwo realizowane przez Polskę

Inwestycje w cyberbezpieczeństwo stanowią jeden z filarów strategicznego podejścia państwa do ochrony przed zagrożeniami w przestrzeni cyfrowej. W ostatnich latach Polska podjęła wiele działań o charakterze systemowym i infrastrukturalnym, których celem jest trwałe zwiększenie odporności instytucji publicznych i gospodarki narodowej na cyberataki.

Jednym z kluczowych przedsięwzięć jest budowa Centrum Cyberbezpieczeństwa NASK (CCN), które obejmuje utworzenie Krajowego Centrum Odzyskiwania Danych, Krajowego Centrum Operacyjnego Cyberbezpieczeństwa, Laboratorium Bezpieczeństwa AI, Laboratorium Fuzzingu i Badania Złośliwego Oprogramowania oraz Ośrodka Modelowania Certyfikacji Cyberbezpieczeństwa. Prace nad realizacją projektu rozpoczęły się w trzecim kwartale 2023 r., a planowany termin ich zakończenia to 2029 r. CCN odegra kluczową rolę w usprawnieniu systemu cyberbezpieczeństwa państwa, w szczególności w kontekście wdrażania przepisów dyrektywy NIS 2. Całkowita wartość inwestycji to 310 mln zł, częściowo finansowanych ze środków unijnych[17].

Ministerstwo Cyfryzacji finansuje również usługę AntyDDoS, realizowaną przez NASK na rzecz podmiotów publicznych i istotnych z punktu widzenia bezpieczeństwa narodowego. W 2024 r. usługa ta była kluczowa w ochronie przed atakami typu DDoS, które mogłyby zakłócić funkcjonowanie kluczowych usług publicznych[18].

W ramach realizacji przedmiotowego zadania w latach 2022–2024 objętych ochroną zostało 75 podmiotów realizujących zadania publiczne oraz podmiotów istotnych z punktu widzenia bezpieczeństwa RP, w tym m.in. Siły Zbrojne RP, służby specjalne oraz urzędy centralne. Systematycznie wzrasta liczba podmiotów objętych ochroną[19].

[17] Zob. https://www.gov.pl/web/cyfryzacja/przelom-w-projekcie-centrum-cyberbezpieczenstwa-nask (dostęp: 16.9.2025 r.)
[18] Sprawozdanie Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, s. 135–136.
[19] Tamże.

Istotne nakłady inwestycyjne przeznaczono również na modernizację infrastruktury lokalnej i wsparcie jednostek samorządu terytorialnego. Programy takie jak „Cyberbezpieczny Rząd”[20] i „Cyberbezpieczne Wodociągi” [21], stanowiące uzupełnienie programu „Cyberbezpieczny Samorząd”, umożliwiły wsparcie centralnych organów administracji rządowej i przedsiębiorstw wodociągowo-kanalizacyjnych w zakresie rozwoju infrastruktury IT. Łączna wartość środków przeznaczonych na te cele przekroczyła 2,25 mld zł.

Równolegle realizowane są inne długofalowe programy infrastrukturalne, takie jak rozwój nowych centrów operacyjnych oraz modernizacja istniejących systemów ochrony. Do przykładów należą: „Bezpieczny Komunikator”[22], zapewniający bezpieczną komunikację dla administracji publicznej; „Platforma CTI”[23], zakupiona dla najważniejszych instytucjach państwowych odpowiedzialnych za cyberbezpieczeństwo; projekt „SecureV”[24], obejmujący specjalistyczne szkolenia z zakresu bezpieczeństwa cyfrowego dla najważniejszych decydentów państwowych. W tym miejscu warto również wspomnieć o mechanizmach wyrównujących wynagrodzenia specjalistów IT w administracji publicznej względem sektora prywatnego[25] – dzięki czemu zwiększa się konkurencyjność sektora publicznego na rynku pracy.

Znaczący impuls inwestycyjny zapewnił również Krajowy Plan Odbudowy (KPO), w ramach którego realizowane są cztery strategiczne przedsięwzięcia o łącznej wartości 864,6 mln zł[26]. Obejmują one: ustanowienie pięciu sektorowych zespołów CSIRT odpowiedzialnych za reagowanie na incydenty bezpieczeństwa komputerowego w różnych sektorach gospodarki; podłączenie 385 podmiotów krajowego systemu cyberbezpieczeństwa do zintegrowanego systemu zarządzania bezpieczeństwem; wsparcie modernizacji infrastruktury cyberbezpieczeństwa w 500 instytucjach publicznych; stworzenie wojewódzkiej sieci specjalistów wspierających obsługę incydentów i odzyskiwanie danych, w tym wzmocnienie kompetencji jednostek Policji w tym zakresie.

Dodatkowo podjęto działania mające na celu wsparcie sektora MŚP, w tym wdrożenie e-usług zwiększających poziom ochrony danych oraz jako-

[20] Zob. https://www.gov.pl/web/cyfryzacja/cyberbezpieczny-rzad--wszystkie-umowy-juz-podpisane (dostęp: 16.9.2025 r.).
[21] Zob. https://www.gov.pl/web/cyfryzacja/cyberbezpieczne-wodociagi--rusza-nabor-wnioskow-o-wsparcie-na-ochrone-przed-cyberatakami (dostęp: 16.9.2025 r.).
[22] Sprawozdanie Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, s. 133.
[23] Tamże, s. 141–142.
[24] Zob. https://www.gov.pl/web/cyfryzacja/komunikat-pelnomocnika-rzadu-ds-cyberbezpieczenstwa-w-sprawie-oszustw-w-komunikacji-z-osobami-publicznymi (dostęp: 16.9.2025 r.).
[25] Zob. https://www.gov.pl/web/baza-wiedzy/przypominamy-zasady-ubiegania-sie-o-srodki-z-funduszu-cyberbezpieczenstwa (dostęp: 16.9.2025 r.).
[26] Sprawozdanie Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, s. 129–130.

ści usług cyfrowych. Dzięki tym inicjatywom MŚP mogą skuteczniej zabezpieczać swoje zasoby i dane klientów[27].

§ 5. Plany zwiększające cyberodporność

W 2025 r. planowane jest też uruchomienie platformy Cyber.gov.pl, nowoczesnego serwisu rządowego zintegrowanego z krajowym węzłem identyfikacji elektronicznej[28]. Platforma ta umożliwi obywatelom, instytucjom i przedsiębiorstwom zgłaszanie incydentów, dostęp do monitoringu zagrożeń, korzystanie z narzędzi takich jak Artemis[29], S46[30] czy aplikacji Moje.cert.pl, a także zdobywanie wiedzy i śledzenie alertów. Jej celem jest uproszczenie dostępu do narzędzi ochrony cyfrowej i wsparcie w codziennym funkcjonowaniu w środowisku online.

Kluczowym czynnikiem skutecznego funkcjonowania KSC pozostaje współpraca międzysektorowa. Koordynację tych działań zapewnia Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa, który integruje wysiłki administracji rządowej, służb, sfery cywilnej i wojskowej oraz innych instytucji. Regularne spotkania koordynacyjne PCOC pozwalają na skuteczne zarządzanie incydentami i szybkie reagowanie w sytuacjach kryzysowych. Ministerstwo Cyfryzacji ściśle współpracuje z CSIRT NASK, CSIRT GOV i CSIRT MON, a także z sektorowymi zespołami cyberbezpieczeństwa – CSIRT CeZ (Centrum e-Zdrowia) i CSIRT KNF (Komisji Nadzoru Finansowego) oraz Centralnym Biurem Zwalczania Cyberprzestępczości (CBZC), podejmując działania minimalizujące skutki zagrożeń cyfrowych.

Równolegle prowadzone są prace legislacyjne, takie jak nowelizacja CyberbezpU, której celem jest wdrożenie dyrektywy NIS 2 oraz tzw. Toolbox 5G[31]. Nowe przepisy przewidują m.in. rozwiązania wzmacniające koordynację i współpracę w zakresie cyberbezpieczeństwa, co w sposób zasadniczy usprawni zarządzanie bezpieczeństwem w polskiej cyberprzestrzeni.

Streszczenie

Rozdział prezentuje założenia i kontekst nowej „Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej 2025–2029". Strategia, przyjmowana uchwałą Rady Ministrów, kontynuuje i aktualizuje cele dokumentu z lat 2019–2024, uwzględniając

[27] Zob. https://www.gov.pl/web/cppc/zakonczenie-oceny-wniosku-o-objecie-przedsiewzieciawsparciem (dostęp: 16.9.2025 r.).
[28] Krajowy węzeł identyfikacji elektronicznej to centralny system, który umożliwia bezpieczne logowanie się do różnych usług publicznych i biznesowych online za pomocą jednego zestawu danych uwierzytelniających, takich jak: Profil Zaufany, mObywatel, e-Dowód lub bankowość elektroniczna (mojeID), https://www.coi.gov.pl/realizacje/rozwoj-cyfrowej-tozsamosci (dostęp: 16.9.2025 r.).
[29] Raport roczny 2024 z działalności CERT Polska, s. 70.
[30] Sprawozdanie Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, s. 75.
[31] Zob. https://ec.europa.eu/newsroom/dae/redirection/document/64596 (dostęp: 16.9.2025 r.).

wyzwania związane z dyrektywą NIS 2 (Network and Information Systems Directive 2) oraz zmiany technologiczne (kryptografia postkwantowa, chmura obliczeniowa i inne przełomowe rozwiązania stosowane w cyberbezpieczeństwie). Strategia wprowadza Plan Działań jako załącznik operacyjny z mierzalnymi zadaniami. Diagnoza zagrożeń wskazuje dynamiczny wzrost incydentów (w tym operacji APT – profesjonalnych grup powiązanych ze strukturami państwowymi), rosnącą wrażliwość łańcuchów dostaw, administracji publicznej i infrastruktury krytycznej, a także intensyfikację kampanii przestępczych i haktywistycznych w kontekście wojny Rosji przeciwko Ukrainie. Prognozy zakładają dalszy wzrost skali i złożoności ataków, szersze wykorzystywanie podatności na brzegu sieci, IoT/OT (Internet Rzeczy/Technologie Operacyjne) oraz technik socjotechnicznych wspieranych przez generatywną sztuczną inteligencję; wskazano pilność wdrażania MFA (uwierzytelniania wieloskładnikowego) i kryptografii postkwantowej. Warstwa wykonawcza Strategii obejmuje m.in. powołanie krajowej instytucji koordynującej (na bazie Połączonego Centrum Operacyjnego Cyberbezpieczeństwa – PCOC), rozwój sektorowych Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT-ów sektorowych), centralne usługi ochronne (zabezpieczenia przed atakami typu DDoS – AntyDDoS, system rozpoznawania zagrożeń w cyberprzestrzeni – CTI, bezpieczna łączność), programy wsparcia jednostek samorządu terytorialnego oraz budowę Centrum Cyberbezpieczeństwa NASK. Strategię uzupełniają projekty Krajowego Plany Odbudowy i uruchomienie platformy Cyber.gov.pl. Dla wzmacniania krajowego systemu cyberbezpieczeństwa kluczowe są: międzysektorowa koordynacja, wzmocnienie wymogów w zamówieniach publicznych, rozwój krajowych technologii i suwerenności technologicznej oraz stała współpraca międzynarodowa w formatach Unii Europejskiej i Organizacji Traktatu Północnoatlantyckiego.

Abstract

The chapter presents the assumptions and context of the new „Cybersecurity Strategy of the Republic of Poland for 2025–2029". The strategy, adopted by a resolution of the Council of Ministers, continues and updates the objectives of the 2019–2024 document, integrating the requirements of the Network and Information Systems Directive 2 and technological changes (Post-quantum cryptography, cloud computing, and other disruptive solutions in cybersecurity). The strategy introduces an Action Plan as an operational annex with measurable tasks. The threat assessment points to a dynamic increase in incidents (including APT – Advanced Persistent Threat operations), growing vulnerability of supply chains, public administration, and critical infrastructure, as well as an intensification of criminal and hacktivist campaigns in the context of Russia's war against Ukraine. Forecasts predict a further increase in the scale and complexity of attacks, wider use of network edge vulnerabilities, IoT/OT (Internet of Things/Operational Technology), and social engineering techniques supported by generative artificial intelligence; the urgency of implementing MFA (Multi-Factor Authentication) and post-quantum cryptography has been highlighted. The executive layer of the Strategy includes, among other things, the establishment of a national coordinating institution (based on PCOC – Joint Cybersecurity Operational Centre), the development of sectoral CSIRTs, cen-

tral protection services (against DDoS attacks – Anti-DDoS, Cyber Threat Intelligence – CTI, secure communications), local government support programs, and the establishment of the Cybersecurity Centre at NASK – National Research Institute. The strategy is complemented by projects under the National Recovery Plan and the launch of the Cyber.gov.pl platform. Key factors in strengthening the national cybersecurity system include cross-sector coordination, strengthening public procurement requirements, developing national technologies and technological sovereignty, and ongoing international cooperation within the European Union and North Atlantic Treaty Organization.

Dominika Kasprowicz

Rozdział 2.
Zagrożenia dla cyberodporności w czasie wojny kognitywnej

„Problemy państw demokracji zachodniej z dezinformacją wynikają po części z nieznajomości rosyjskiej strategii, po części z «przekładania» jej na własny system pojęć i język interpretacji. Tymczasem rosyjski model refleksji na ten temat jest zasadniczo odmienny od zachodniego" – *J. Darczewska*

§ 1. Wstęp

Współczesne konflikty międzynarodowe przybierają niemilitarne formy, wśród których kluczowe miejsce zajmują operacje hybrydowe i – bardziej szczegółowo – operacje kognitywne. Termin ten rozumiany jest jako działania ukierunkowane na percepcję, emocje i zachowania społeczne prowadzące do długofalowej destabilizacji państwa bez użycia sił zbrojnych. W niniejszym rozdziale celem Autorki było zwrócenie uwagi na dwie kwestie, a mianowicie charakterystykę rosyjskiej operacji kognitywnej i jej wpływu na bezpieczeństwo polskiej przestrzeni informacyjnej oraz wyzwań społecznych wymagających systemowych rozwiązań na polu szeroko rozumianej cyberodporności. Operacja kognitywna toczy się ona w sposób systematyczny, zaplanowany i wieloaspektowy, wywołując pytania o poziom bezpieczeństwa przestrzeni informacyjnej polskiego państwa, jego gotowości oraz odporności i cyberodporności polskiego społeczeństwa. Cyberodporność to termin ważny w kontekście bezpieczeństwa, jednocześnie wymagający podejścia zintegrowanego, które wykracza poza tradycyjne ramy cyberbezpieczeństwa. Bo choć komponenty techniczne i organizacyjne są fundamentem ochrony cyfrowej, to komponenty społeczne w coraz większym stopniu decydują o skuteczności reakcji na współczesne zagrożenia.