WYŚCIG Z Q-DAY

PAŃSTWOWY INSTYTUT BADAWCZY
Instytut Łączności

GLOBALNY STAN PRZYGOTOWAŃ

Standardy, regulacje, strategie migracji do kryptografii postkwantowej

Raport miesięczny o trendach technologicznych

Raport Miesięczny

EDYCJA 3

Maj 2026

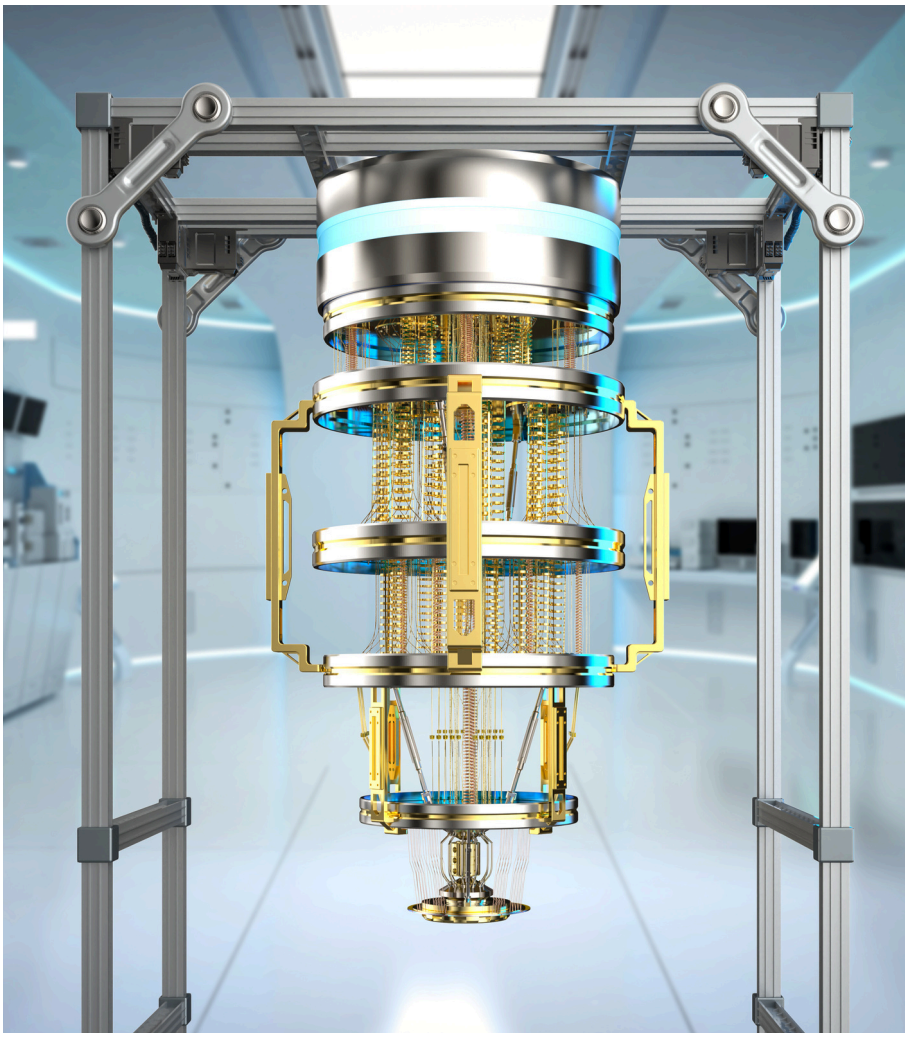
AUTORZY

dr inż. Joanna Kołodziejczyk

Tomasz Melaniuk

Paulina Obara

Zofia Ragankiewicz



Redakcja:

Roman Młodkowski

Opiekun merytoryczny:

Marcin Klepacki

Projekt graficzny:

Kinga Graczyk

Skład:

Kinga Graczyk

Anna Maraszek

Korekta:

Joanna Dubel, Anna Maraszek, Paweł Waszczyk

SPIS TREŚCI

1. WPROWADZENIE

W ostatnich latach ryzyko związane z rozwojem komputerów kwantowych klasy CRQC (Cryptographically Relevant Quantum Computer[1]) o mocy obliczeniowej umożliwiającej złamanie obecnych mechanizmów kryptografii przestało być traktowane jako odległy w czasie problem technologiczny, a stało się jednym z kluczowych wyzwań dla bezpieczeństwa państw, administracji publicznej i sektorów krytycznych.
Wraz z postępem prac rośnie świadomość, że ochrona danych, komunikacji i infrastruktury cyfrowej wymaga przygotowania już dziś - zanim zagrożenie stanie się realne.
Pojawienie się komputerów klasy CRQC umożliwi praktyczne wykorzystanie algorytmu Shora, co doprowadzi do natychmiastowego złamania obecnie stosowanych systemów klucza publicznego (RSA, ECC).

Raport analizuje gotowość m.in. Unii Europejskiej, USA, Chin i Polski do migracji na kryptografię postkwantową - od standardów technicznych po harmonogramy implementacyjne.

Wdrożenie kryptografii postkwantowej (PQC) w 2026 roku przeszło z fazy teoretycznych rozważań do ściśle określonych harmonogramów regulacyjnych. USA mają dziś najbardziej zaawansowany model państwowy: posiadają federalne przepisy, obowiązek inwentaryzacji systemów podatnych na zagrożenia, standardy techniczne Narodowego Instytutu Norm i Technologii (NIST) oraz harmonogram wdrożenia PQC w systemach bezpieczeństwa narodowego. Europa jest na etapie koordynacji, lecz pozostaje nierówna. Na poziomie UE istnieje już wspólna mapa drogowa, ale gotowość wykonawcza poszczególnych państw jest zróżnicowana. Natomiast Chiny prowadzą intensywne działania w obszarze komunikacji odpornej kwantowo i własnej ścieżki standaryzacyjnej, chociaż nie ma publicznie dostępnego dokumentu opisującego migrację do PQC jak w USA czy w Europie.

ZŁAMANIE OBECNYCH MECHANIZMÓW KRYPTOGRAFII PRZESTAŁO BYĆ TRAKTOWANE JAKO ODLEGŁY W CZASIE PROBLEM TECHNOLOGICZNY.

2. DLACZEGO TERAZ

Systemy kryptograficzne, które obecnie zabezpieczają tajemnice państwowe, dane obywateli, dane transakcyjne, globalny handel oraz prywatną komunikację, opierają się na założeniu, że pewne problemy matematyczne są praktycznie nierozwiązywalne dla komputerów klasycznych. Jednak postęp w dziedzinie mechaniki kwantowej, budowy komputerów kwantowych i algorytmiki, jaki dokonał się do roku 2026, wskazuje, że fundamenty te ulegają drastycznym zmianom, większym niż przewidywano jeszcze dekadę temu.

2.1. Q-DAY

Wizja komputera kwantowego zdolnego do łamania współczesnych szyfrów, niegdyś postrzegana jako odległy problem teoretyczny, w połowie obecnej dekady stała się realnym punktem odniesienia w planowaniu zmian w zabezpieczeniach kryptograficznych. Ważnym terminem w tym kontekście jest Q-Day – moment, w którym komputer kwantowy o odpowiedniej mocy obliczeniowej (CRQC) będzie w stanie złamać powszechnie stosowane klucze kryptograficzne.

2.2. EWOLUCJA OD NISQ DO CRQC: PRÓG ZAGROŻENIA KRYPTOGRAFICZNEGO

Dzisiejsze maszyny kwantowe znajdują się w erze Noisy Intermediate-Scale Quantum (NISQ[2]). Systemy tej generacji dysponują od kilkudziesięciu do ponad tysiąca fizycznych kubitów, jednak ich działanie ograniczone jest przez wysoki poziom szumu, dekoherencję oraz brak pełnej korekcji błędów. W praktyce uniemożliwia to realizację długich, odpornych na błędy obliczeń kwantowych wymaganych do przeprowadzenia zaawansowanych operacji kryptograficznych.

Ze względu na ograniczoną stabilność obliczeń algorytmy wykonywane na urządzeniach typu NISQ muszą być relatywnie krótkie i wyspecjalizowane, co pozwala na demonstrację tzw. przewagi kwantowej (quantum advantage) w wybranych problemach obliczeniowych[3], nie stanowiąc jeszcze praktycznego zagrożenia dla współczesnych systemów kryptografii asymetrycznej.

Za próg realnego zagrożenia kryptograficznego uznaje się dopiero pojawienie się komputerów typu CRQC (Cryptographically Relevant Quantum Computer). Systemy te wymagałyby tysięcy logicznych kubitów wyposażonych w mechanizmy korekcji błędów oraz bardzo niskiego poziomu błędów operacyjnych[4]. Dopiero taka architektura umożliwiłaby praktyczne uruchomienie algorytmu Shora w skali pozwalającej na łamanie kluczy RSA-2048, kryptografii krzywych eliptycznych (ECC) oraz mechanizmów opartych na problemie logarytmu dyskretnego[5].

2.3. MATEMATYCZNE SŁABOŚCI OBECNEJ KRYPTOGRAFII: ALGORYTMY SHORA I GROVERA

Nie wszystkie algorytmy kryptograficzne są w równym stopniu zagrożone przez komputery kwantowe. Najwyższy poziom ryzyka dotyczy algorytmów kryptografii asymetrycznej (z kluczem publicznym i kluczem prywatnym), które stanowią fundament dzisiejszej infrastruktury zabezpieczeń cyfrowych. Bezpieczeństwo kluczy RSA, DSA, ECDSA, Diffie-Hellmana i ECDH opiera się na trudności faktoryzacji dużych liczb całkowitych oraz obliczania logarytmu dyskretnego. Algorytm Shora (1994 r.) rozwiązuje oba te problemy w czasie wielomianowym przy użyciu komputera kwantowego o wystarczająco dużej mocy obliczeniowej. W praktyce oznacza to, że CRQC zdezaktualizuje współczesną kryptografię klucza publicznego - PKI, podpis elektroniczny, TLS, VPN, SSH, protokoły bezpiecznej poczty.

W przeciwieństwie do systemów asymetrycznych, kryptografia symetryczna (np. AES) oraz funkcje skrótu (np. SHA-256) są mniej podatne na całkowite złamanie, ale ich efektywny poziom bezpieczeństwa ulega zmniejszeniu. Algorytm Grovera (zaproponowany w 1996 r.[6]) przyspiesza wyszukiwanie elementu w niestrukturalnych bazach danych poprzez przeszukanie przestrzeni możliwych kluczy o połowie długości klucza, który jest obiektem ataku. Teoretycznie obniża to efektywny poziom bezpieczeństwa szyfru o połowę, dlatego jako środek ostrożności rekomenduje się przejście z AES-128 na AES-256 dla danych o długim horyzoncie poufności. Teoretycznie algorytm Grovera umożliwia komputerom kwantowym przyspieszenie ataków metodą „brute-force" i sprawdzenie wszystkich możliwych kombinacji w celu odkrycia prawidłowego hasła lub klucza, jednak jest to mniej groźne niż użycie algorytmu kryptoanalizy o wykładniczym współczynniku obliczeniowym jak algorytm Shora[7].

2.4. TEMPO REDUKCJI SZACUNKÓW

Ryzyko związane z CRQC rośnie szybciej niż przewidywano. W maju 2025 r. Craig Gidney (Google Quantum AI) wykazał, że złamanie RSA-2048 wymaga mniej niż milion kubitów fizycznych - co stanowi około 20-krotną redukcję liczby kubitów względem wspólnego szacunku Gidney–Ekerå z 2019 r. (wówczas mowa była o 20 mln)[8]. Co istotne, redukcja ta dotyczy liczby kubitów, nie czasu obliczeń: szacowany czas ataku wzrósł z 8 godzin (2019) do mniej niż tygodnia (2025).

Cytat z abstraktu: „*W Gidney+Ekerå 2019 opublikowaliśmy szacunek, według którego 2048-bitowe liczby RSA można sfaktoryzować w 8 godzin na komputerze kwantowym z 20 milionami zaszumionych kubitów. W tej pracy znacząco redukuję liczbę wymaganych kubitów. Szacuję, że 2048-bitową liczbę RSA można sfaktoryzować w mniej niż tydzień na komputerze kwantowym z mniej niż milionem zaszumionych kubitów.*”

Jeszcze głębszą redukcję zaproponował w lutym 2026 r. zespół Iceberg Quantum (Sydney) w architekturze Pinnacle - poniżej 100 000 kubitów fizycznych[9].

Najnowsze plany wiodących dostawców (stan na maj 2026) wskazują na dostępność systemów odpornych na błędy (fault-tolerant) z 200 kubitami logicznymi w 2029 r. - system IBM Quantum Starling - oraz trajektorię do 2000 kubitów logicznych w systemie Blue Jay około 2033 r. [10]

Należy jednak wyraźnie odróżnić te wartości od szacunków ataku: praca Gidneya mówi o mniej niż 1 milionie kubitów fizycznych, co przy obecnych możliwościach korekcji błędów może odpowiadać około 1000 kubitów logicznych[11]. Oznacza to, że 200 kubitów logicznych planowanego systemu Starling pozostaje o rząd wielkości poniżej progu potrzebnego do złamania RSA-2048. Mimo to ogólny kierunek jest jednoznaczny: zasób potrzebny do ataku maleje szybciej, niż przewidywano, a kolejne kamienie milowe sprzętowe wyraźnie skracają horyzont zagrożenia.

2.5. HARVEST NOW, DECRYPT LATER (HNDL)

Najbardziej czarny scenariusz jest już realizowany, ponieważ największym problemem nie jest moment powstania kryptologicznie istotnego komputera kwantowego (CRQC), lecz zjawisko Harvest Now, Decrypt Later (HNDL). W istocie oznacza to, że przeciwnik może dziś przechwytywać zaszyfrowane dane i odszyfrować je w przyszłości, gdy będą dostępne komputery klasy CRQC. Jest to szczególnie krytyczne dla danych, które wymagają długoletniej ochrony z uwagi na swoją wrażliwość, np. dokumenty niejawne państwa, dane wywiadowcze, informacje bankowe, dane medyczne, własność intelektualna, tajemnice handlowe, dane geopolityczne. Dlatego państwa nie czekają na Q-Day, tylko rozpoczynają migrację do kryptografii postkwantowej już teraz. Holenderski AIVD, brytyjski NCSC i rekomendacje Komisji Europejskiej wskazują wprost, że dla części danych i systemów ryzyko już dziś ma charakter strategiczny, a nie wyłącznie hipotetyczny.

2.6. RYZYKO OPÓŹNIONEJ MIGRACJI

Złożone systemy, takie jak infrastruktura zarządzania kluczami publicznymi czy urządzenia o długim cyklu życia, wymagają wieloletnich okresów przejściowych. Nawet w sytuacji braku bieżących ataków, zbyt późne rozpoczęcie procesu przejścia na kryptografię postkwantową może uniemożliwić jego terminowe zakończenie, co w konsekwencji może zagrozić poufności oraz autentyczności komunikacji.

2.7. REGUŁA MOSCA

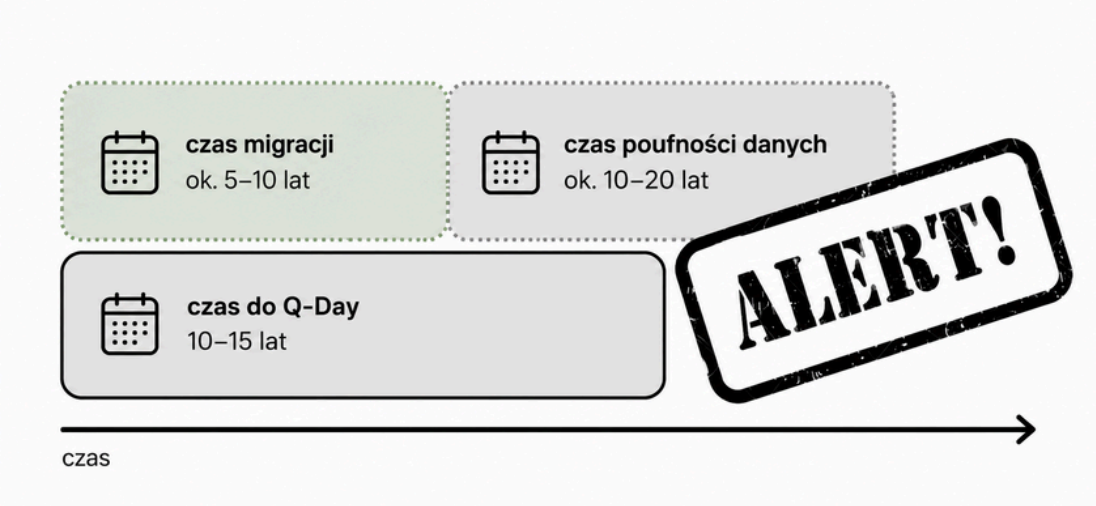
Podstawowym narzędziem oceny ryzyka jest tzw. formuła pilności Mosca[11], która identyfikuje sytuację kryzysową dotyczącą cyberbezpieczeństwa za pomocą trzech zmiennych:

$$X + Y \geq Z$$

gdzie: X to czas, przez który dane muszą pozostać poufne; y to czas potrzebny na migrację; z to czas do Q-Day.

„Jeżeli X + Y ≥ Z, mamy dziś poważny problem, ponieważ informacje chronione przez narzędzia podatne na ataki kwantowe pod koniec następnych y lat mogą zostać złamane przez ataki kwantowe w ciągu mniej niż x lat od tego momentu”[12].

Dla danych państwowych w Polsce: X ≥ 20–30 lat, Y = 5–10 lat (typowy horyzont dużej migracji kryptograficznej), Z = 2029-2040 rok (szacunkowo) gdy pojawi się komputer klasy CRQC, dlatego prace nad migracją powinny rozpocząć się natychmiast.



2.8. PQC CZY QKD?

W międzynarodowej debacie nad architekturą bezpieczeństwa ery komputerów kwantowych zarysowały się dwa technologicznie odmienne podejścia do ochrony przed zagrożeniem kwantowym:

- Kryptografia postkwantowa (PQC): nowe, klasyczne algorytmy matematyczne (np. oparte na kratach), które są odporne na ataki przy użyciu zarówno współczesnych komputerów klasycznych, jak i przyszłych komputerów kwantowych o dużej mocy obliczeniowej klasy CRQC. Algorytmy mogą być uruchamiane na obecnych komputerach i przesyłane przez istniejącą infrastrukturę sieciową.
- Kwantowa Dystrybucja Klucza (QKD): systemy sprzętowe wykorzystujące zjawiska mechaniki kwantowej, umożliwiające bezpieczne uzgodnienie losowego klucza symetrycznego między dwoma węzłami sieci i uniemożliwiające podsłuch bez zostawienia śladów.

Wiodące zachodnie organy cyberbezpieczeństwa - w tym amerykański NIST, francuska ANSSI, oraz brytyjskie NCSC - wypracowały doktrynę opartą niemal wyłącznie na kryptografii postkwantowej (PQC) jako głównym filarze ochrony. Organy te zachowują daleko idący sceptycyzm wobec wdrażania systemów sprzętowych QKD (Kwantowej Dystrybucji Klucza).

Odmienną strategię reprezentują kluczowi gracze w Azji (np. Chiny, Japonia, Korea Południowa czy Singapur) wdrażając podejście hybrydowe: intensywnie inwestują w wielkoskalowe sieci komunikacji kwantowej, instalując sprzętowe systemy QKD do fizycznego uzgadniania bezpiecznych kluczy symetrycznych między węzłami sieci, a równolegle implementując własne algorytmy PQC w warstwie oprogramowania i punktów końcowych.

3. STANDARDY I GOTOWOŚĆ TECHNOLOGICZNA

Aby skutecznie chronić się przed zagrożeniem ze strony komputerów kwantowych, świat nauki i technologii musiał stworzyć nowe narzędzia kryptograficzne.

Proces ten został zapoczątkowany przez amerykański NIST w 2016 roku globalnym naborem wniosków, w ramach którego międzynarodowe zespoły badawcze zgłosiły 82 projekty kryptograficzne.
Przez kolejne lata, w ramach transparentnej i publicznej oceny, eksperci z całego świata rygorystycznie testowali i analizowali nadesłane rozwiązania.
Proces standaryzacji uległ ostatecznej krystalizacji 13 sierpnia 2024 roku, kiedy NIST opublikował pierwsze, oficjalne normy FIPS (Federal Information Processing Standards).
Standardy te stanowią formalną algorytmiczną bazę dla migracji w systemach w USA i stały się punktem odniesienia dla wdrożeń postkwantowych na całym świecie.

Skuteczne zabezpieczenie systemów przed zagrożeniem kwantowym wymaga elastyczności projektowej, czyli tzw. krypto-zwinności (crypto-agility), oraz unikania opierania ochrony tylko na jednym typie zabezpieczeń. Współczesna architektura PQC nie wykorzystuje bowiem jednego, uniwersalnego algorytmu. Zamiast tego bazuje na kilku odmiennych fundamentach matematycznych, z których każdy oferuje inne zalety i wiąże się z kompromisami.

3.1. ALGORYTMY OPARTE NA KRATACH (LATTICE-BASED) - GŁÓWNY NURT WDROŻENIOWY

Jest to obecnie najważniejsza i najbardziej uniwersalna rodzina algorytmów, stanowiąca fundament nowych standardów bezpieczeństwa. Zostały wytypowane przez amerykański NIST jako podstawowe algorytmy ogólnego przeznaczenia ze względu na balans pomiędzy bezpieczeństwem, rozmiarem kluczy a wydajnością obliczeniową.

- **ML-KEM (dawniej CRYSTALS-Kyber)**. Został opublikowany jako FIPS 203 w sierpniu 2024 roku, jako podstawowy standard enkapsulacji klucza (Key Encapsulation Mechanism). W przeciwieństwie do klasycznych metod współdzielenia (jak Diffie-Hellman), KEM polega na wygenerowaniu bezpiecznego klucza symetrycznego przez jedną stronę i przesłaniu go w zabezpieczonej "kapsule" do drugiej. Stanowi docelowy standard dla modernizacji protokołów sieciowych, w tym: połączeń TLS 1.3 (HTTPS), wirtualnych sieci prywatnych (VPN) oraz bezpiecznej komunikacji w tranzycie. Znaczenie ML-KEM wynika z tego, że zastępuje on funkcjonalnie te obszary, w których obecnie wykorzystywane są RSA, Diffie-Hellman lub ECDH. To właśnie te mechanizmy są najbardziej narażone na złamanie przez komputer klasy CRQC wykorzystujący algorytm Shora. NIST wskazuje trzy poziomy parametrów: ML-KEM-512, ML-KEM-768 oraz ML-KEM-1024, które różnią się poziomem bezpieczeństwa i kosztami wydajnościowymi[14]. W praktyce ML-KEM stanie się głównym kandydatem do masowej migracji protokołów komunikacyjnych w administracji publicznej, sektorze finansowym, telekomunikacji i usługach cyfrowych.

- **ML-DSA (dawniej CRYSTALS-Dilithium)**. Został opublikowany przez NIST jako FIPS 204 i stanowi podstawowy standard podpisu cyfrowego w nowej architekturze PQC[15]. Zastępuje w systemach klasyczne schematy RSA i ECDSA. ML-DSA ma szczególne znaczenie dla infrastruktury zaufania publicznego, ponieważ podpis cyfrowy jest fundamentem administracji elektronicznej, odpowiada za: podpisywanie dokumentów, uwierzytelnianie użytkowników i systemów, podpisywanie certyfikatów, podpisywanie kodu, autoryzację oprogramowania (software signing), podpisywanie aktualizacji oraz zapewnienie integralności komunikatów. W praktyce migracja do ML-DSA będzie jednym z najbardziej złożonych etapów transformacji postkwantowej. Wymaga bowiem nie tylko wymiany algorytmu, ale także dostosowania certyfikatów, bibliotek kryptograficznych, urządzeń HSM, procedur walidacji podpisów, archiwizacji dokumentów oraz systemów długoterminowego potwierdzania ważności podpisu.

- **FN-DSA (Falcon)**: Algorytm ma być zestandaryzowany jako FIPS 206 – projekt przedłożono do zatwierdzenia 28 sierpnia 2025 r., a finalizacja jest spodziewana na przełomie 2026/2027[16]. Alternatywny algorytm podpisu cyfrowego, który charakteryzuje się znacznie mniejszym rozmiarem niż ML-DSA[17] i bardzo szybką jego weryfikacją[18]. Ponieważ proces składania podpisu wymaga złożonych operacji zmiennoprzecinkowych (ang. constant-time 64-bit floating-point arithmetic), algorytm ten nie nadaje się do generowania podpisów na słabych urządzeniach brzegowych (IoT)[19]. Jest jednak idealny do scenariuszy asymetrycznych, gdzie potężny serwer podpisuje dane, a weryfikacja odbywa się w sieciach o niskiej przepustowości lub na prostych urządzeniach końcowych.

3.2. STANDARDY REZERWOWE I STANOWE OPARTE NA FUNKCJACH SKRÓTU (HASH-BASED):

- **LMS oraz XMSS:** Stanowe schematy podpisów cyfrowych (ang. stateful hash-based signatures), formalnie ustandaryzowano w NIST SP 800-208[20]. Ich główną zaletą jest oparcie na matematyce, którą kryptolodzy doskonale znają i badają od dziesięcioleci. Dzięki temu posiadają silne i pewne zaplecze bezpieczeństwa, wykazując odporność zarówno na ataki klasyczne, jak i kwantowe. Francuska agencja cyberbezpieczeństwa (ANSSI) wskazała, że ze względu na ich wyjątkową stabilność i dojrzałość, algorytmy te mogą być wdrażane samodzielnie, bez konieczności stosowania mechanizmów hybrydowych[21]. Ich uniwersalność jest jednak ograniczona przez architekturę „stanową". Wymagają one rygorystycznego zarządzania licznikiem użyć – dana para kluczy pozwala na wygenerowanie jedynie z góry określonej, skończonej liczby podpisów. Co więcej, utrata synchronizacji stanu (np. w wyniku nieodpowiedniego przywrócenia serwera z kopii zapasowej) i ponowne użycie tego samego klucza jednorazowego skutkuje całkowitą kompromitacją bezpieczeństwa.
- Z tego względu implementacja LMS i XMSS wymaga wyspecjalizowanych modułów sprzętowych chroniących stan licznika. Czyni to z nich standard dla zamkniętych, bardzo kontrolowanych środowisk technologicznych. Idealnie sprawdzają się w niszowych, ale krytycznych dla infrastruktury zadaniach, takich jak weryfikacja przy starcie systemu (secure boot), cyfrowa autoryzacja oprogramowania układowego (firmware) oraz bezpieczne dostarczanie aktualizacji dla sprzętu przemysłowego (OT/IoT).

- **SLH-DSA (dawniej SPHINCS+):** Zaawansowany, bezstanowy podpis cyfrowy oparty na funkcjach skrótu (ang. hash-based), wystandaryzowany przez NIST jako FIPS 205[22]. Chociaż proces generowania podpisu jest wolniejszy, a jego rozmiar znacznie większy niż w przypadku algorytmów opartych na kratach, stanowi on kluczową technologię rezerwową (ang. fallback). Jego bezpieczeństwo nie opiera się na nowych założeniach matematycznych, lecz na dekadach badań nad kryptograficznymi funkcjami skrótu. Ponadto jego bezstanowość eliminuje ryzyko błędu ponownego użycia klucza, co gwarantuje najwyższy poziom odporności na wypadek nieoczekiwanego załamania standardów bazujących na kryptografii kratowej. W przypadku odkrycia w przyszłości nowych metod kryptoanalizy wpływających na bezpieczeństwo konstrukcji kratowych, SLH-DSA może pełnić funkcję niezależnej alternatywy dla systemów państwowych, wojskowych oraz infrastruktury krytycznej.

3.3. ALTERNATYWNE ŚCIEŻKI I KONSERWATYWNA DYWERSYFIKACJA (KEM)

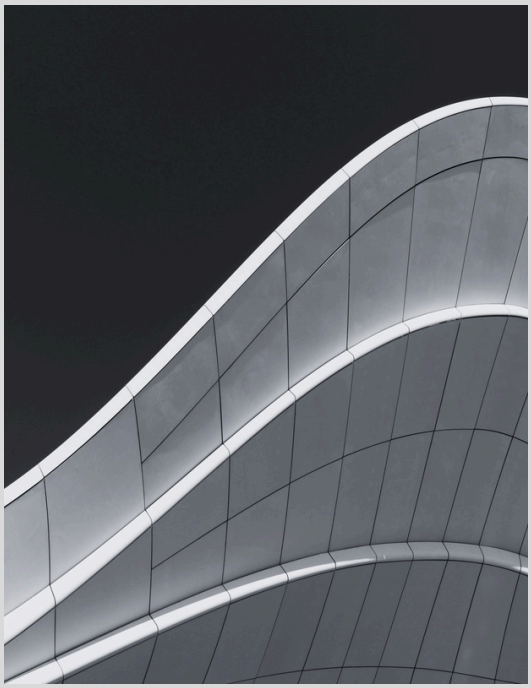
Jednym z najważniejszych wyzwań ery postkwantowej jest ryzyko nadmiernego uzależnienia całej infrastruktury bezpieczeństwa od jednej rodziny matematycznej.

Obecnie większość podstawowych standardów PQC rekomendowanych przez NIST - w szczególności ML-KEM (Kyber), ML-DSA (Dilithium) oraz Falcon - opiera się na kryptografii kratowej (ang. lattice-based cryptography). Z perspektywy bezpieczeństwa państwowego i infrastruktury krytycznej oznacza to ryzyko tzw. monokultury kryptograficznej. W przypadku odkrycia w przyszłości nowych metod kryptoanalizy wpływających na bezpieczeństwo konstrukcji kratowych, potencjalne skutki mogłyby objąć jednocześnie znaczną część światowej infrastruktury cyfrowej. Dlatego doktryna bezpieczeństwa dla systemów najwyższego ryzyka (ang. high-security systems) wymusza stosowanie krypto-zwinności oraz rozwijanie ścieżek alternatywnych, pełniących rolę rozwiązań rezerwowych:

- **FrodoKEM**: Algorytm służący do enkapsulacji klucza, stanowiący bezpośrednią alternatywę dla ML-KEM. O ile ML-KEM (Kyber) wykorzystuje ustrukturyzowane kraty (ang. module lattices) dla maksymalizacji wydajności i zmniejszenia rozmiaru kluczy. FrodoKEM opiera się na czystym, nieustrukturyzowanym problemie LWE (ang. Learning with Errors). Brak dodatkowej struktury matematycznej oznacza większe klucze i wyższe zapotrzebowanie na zasoby obliczeniowe, ale zapewnia znacznie wyższy margines bezpieczeństwa. Mimo to, zgodnie z oficjalnymi rekomendacjami niemieckiego BSI[23], jest to algorytm o znaczeniu krytycznym dla administracji publicznej i sieci rządowych. Wytyczna BSI wprost wymienia i rekomenduje warianty FrodoKEM-976 oraz FrodoKEM-1344. W praktyce FrodoKEM pełni rolę mechanizmu rezerwowego, którego głównym celem nie jest maksymalizacja wydajności, lecz zwiększenie odporności na potencjalne przyszłe przełomy kryptograficzne.

- **Classic McEliece (code-based)**: Algorytm oparty na kodach korekcyjnych, którego podstawy matematyczne pozostają niezłamane od blisko pięciu dekad. Chociaż generuje ogromne klucze publiczne (często liczone w megabajtach), sam proces szyfrowania i deszyfrowania jest bardzo szybki. Z tego względu algorytm ten nie jest optymalny dla urządzeń mobilnych, środowisk IoT, systemów o ograniczonej przepustowości ani masowych wdrożeń. Doskonale sprawdza się w specyficznych przypadkach użycia, takich jak tunele VPN typu site-to-site czy szkieletowa infrastruktura komunikacyjna, gdzie rozmiar klucza nie stanowi problemu. Classic McEliece jest również ważnym elementem strategicznej dywersyfikacji kryptograficznej. W przypadku osłabienia bezpieczeństwa algorytmów kratowych mógłby pełnić funkcję alternatywnej warstwy bezpieczeństwa dla infrastruktury państwowej i obronnej.

HQC: Nowocześniejszy algorytm oparty na kodach (code-based), który w marcu 2025 r. został wybrany przez NIST do standaryzacji jako dodatkowy, rezerwowy mechanizm KEM - niezależny matematycznie od rodziny kratowej[24]. HQC wyłoniono spośród kandydatów czwartej rundy (obok m.in. BIKE, który nie został wybrany). W przeciwieństwie do Classic McEliece, algorytm ten posiada znacznie mniejsze klucze publiczne; jego głównym zadaniem jest zapewnienie alternatywy chroniącej ekosystem przed ewentualną kompromitacją matematyki opartej na kratach (lattice-based). Finalny standard HQC jest spodziewany w kolejnych latach (NIST przewiduje publikację około 2026–2027 r.).



3.4. IZOGENIE KRZYWYCH ELIPTYCZNYCH I LEKCJA Z UPADKU ALGORYTMU SIKE

Kryptografia oparta na izogeniach krzywych eliptycznych (ang. Isogeny-based cryptography) przez lata stanowiła jedną z najbardziej obiecujących gałęzi w badaniach nad bezpieczeństwem postkwantowym. Jej zaletą, wyróżniającą ją na tle schematów opartych na kratach czy kodach, był niezwykle mały rozmiar kluczy publicznych, zbliżony do klasycznej kryptografii krzywych eliptycznych (Elliptic Curve Cryptography - ECC). Najbardziej zaawansowanym reprezentantem tej rodziny był algorytm **SIKE** (Supersingular Isogeny Key Encapsulation), który pomyślnie dotarł do czwartej rundy procesu standaryzacyjnego amerykańskiego instytutu NIST i był powszechnie uważany za silnego kandydata do wdrożeń w środowiskach o rygorystycznych ograniczeniach przepustowości[25].

W 2022 roku SIKE został złamany przez klasyczny atak kryptograficzny opracowany przez zespół kierowany przez Woutera Castrycka i Thomasa Decru[26]. Badacze z belgijskiego uniwersytetu KU Leuven opublikowali pracę naukową, w której zaprezentowali skuteczny atak na SIDH – podstawowy problem matematyczny, na którym opierał się schemat SIKE. Atak nie wykorzystywał komputera kwantowego, lecz był to klasyczny atak, który znacząco obniżył złożoność łamania schematu i doprowadził do kompromitacji bezpieczeństwa algorytmu SIKE. Wydarzenie to miało ogromne znaczenie dla całego środowiska kryptografii postkwantowej z kilku powodów. Po pierwsze, SIKE przez lata był uznawany za jedną z najbardziej zaawansowanych matematycznie konstrukcji PQC. Złamanie algorytmu pokazało, że wysoki poziom matematycznej złożoności nie oznacza automatycznie długoterminowego bezpieczeństwa kryptograficznego. Po drugie, kompromitacja SIKE nastąpiła bardzo szybko w porównaniu z wieloletnią historią analizy innych rodzin kryptograficznych, takich jak funkcje skrótu czy systemy kodowe McEliece. Pokazało to fundamentalne ryzyko związane z „młodymi" schematami kryptograficznymi, które nie przeszły jeszcze dekad intensywnej analizy kryptograficznej. W praktyce wiele zachodnich agencji bezpieczeństwa - w tym NIST, BSI, ANSSI oraz NCSC - zaczęło po 2022 roku jeszcze mocniej podkreślać znaczenie crypto-agility, hybrydyzacji, oraz utrzymywania alternatywnych rozwiązań matematycznych. Przypadek SIKE stał się bowiem dowodem na to, że nawet bardzo obiecujące i szeroko analizowane konstrukcje mogą zostać niespodziewanie osłabione przez nowe metody kryptograficzne.

4. RAMY REGULACYJNE UNII EUROPEJSKIEJ I JEJ CZŁONKÓW

4.1 SKOORDYNOWANA MAPA DROGOWA EUROPY

11 kwietnia 2024 r. Komisja Europejska wydała rekomendację w sprawie skoordynowanego planu wdrożenia dotyczącego przejścia na kryptografię postkwantową („*Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography*")[27], a rok później 23 czerwca 2025 r.[28] państwa członkowskie, wspierane przez KE, opublikowały wspólną mapę wdrożeniową „*Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography*"[29]. Dokument nie jest aktem prawnie wiążącym w rozumieniu prawa UE. Jest to wysokopoziomowy dokument strategiczny (ang. high-level paper) skierowany do państw członkowskich.

Kluczowy zwrot nastąpił w styczniu 2026 r., gdy Komisja Europejska zaproponowała poprawki do dyrektywy **NIS2** (projekt COM(2026) 13), w których przejście do kryptografii postkwantowej zostaje wprost wpisane do dyrektywy:

” (…)W CELU PRZEJŚCIA NA KRYPTOGRAFIĘ POSTKWANTOWĄ, BIORĄC POD UWAGĘ HARMONOGRAMY PRZEJŚCIA I ODPOWIEDNIE WYMOGI OKREŚLONE W OBOWIĄZUJĄCYCH AKTACH PRAWNYCH I POLITYKACH UNII.(…).”[30]

W praktyce oznacza to, że mapa drogowa KE z czerwca 2025 r. przejdzie od statusu rekomendacji do statusu obowiązku w momencie przyjęcia poprawek do NIS2 co ma nastąpić jeszcze w 2026 lub w 2027 roku. Do tej pory gotowość PQC w ramach NIS2 była kwestią interpretacji, przyjęcie COM(2026) 13 zniweluje tę lukę. Polityki przejściowe PQC staną się obowiązkowym elementem krajowej strategii cyberbezpieczeństwa każdego państwa członkowskiego.

Europejska mapa przygotowana przez NIS Cooperation Group[31] powstała na bazie dokumentów i doświadczeń przygotowanych przez agencje rządowe takich krajów jak Niemcy BSI[32] (niem. *Bundesamt für Sicherheit in der Informationstechnik* tłum. Federalny Urząd ds. Bezpieczeństwa Informacji), Francja ANSSI[33] (franc. *Agence nationale de la sécurité des systèmes d'information* w tłum. Narodowa Agencja Bezpieczeństwa Systemów Informatycznych) czy Holandia AIVD[34] (*Algemene Inlichtingen- en Veiligheidsdienst* w tłum. Główna Służba Wywiadu i Bezpieczeństwa Królestwa Niderlandów).

Rekomendacje Komisji Europejskiej służą trzem celom:
- Zapewnienie zsynchronizowanej implementacji PQC we wszystkich państwach członkowskich
- Ustanowienie wspólnego języka ryzyka (klasyfikacja: wysokie, średnie i niskie zagrożenie kwantowe).
- Wprowadzenie środków informacyjno-edukacyjnych dla zapewnienia, że wszyscy interesariusze rozumieją zagrożenie kwantowe.

Wyznaczając wspólne ramy czasowe dla całej Unii Europejskiej ustanowiono trzy wiążące kierunkowo kamienie milowe podzielone na etapy „First Steps", „Next Steps" oraz pełna implementacja[35]:

- **31 grudnia 2026 r.** - wszystkie państwa członkowskie muszą ukończyć wdrażanie tzw. Pierwszych Kroków („*First Steps*"). Wymagane jest formalne ustanowienie początkowych krajowych migracyjnych map drogowych oraz uruchomienie planowania i programów pilotażowych dla przypadków użycia o wysokim i średnim poziomie ryzyka.

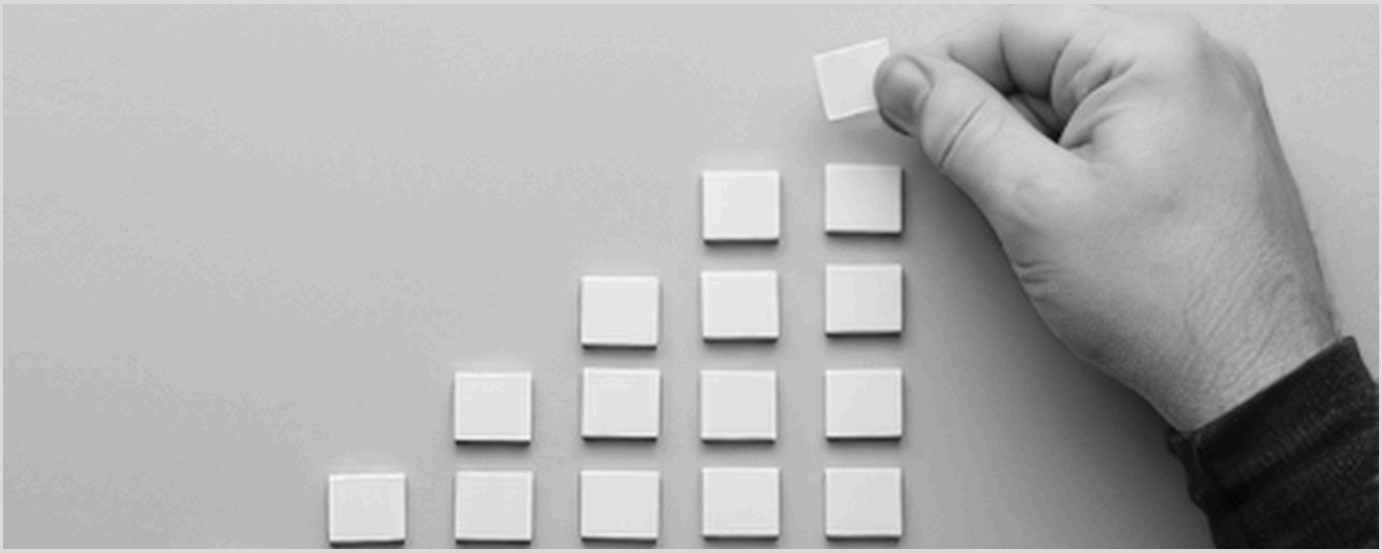
- **31 grudnia 2030 r.** - obowiązkowe sfinalizowanie Kolejnych Kroków („*Next Steps*") przez wszystkie kraje UE. Następuje całkowite zakończenie migracji do PQC dla wszystkich obszarów sklasyfikowanych jako wysokie ryzyko. Muszą zostać ukończone procesy planowania i pilotaże dla średniego ryzyka, a bezpieczne kwantowo mechanizmy aktualizacji oprogramowania (również wbudowanego w urządzenie sprzętowe tzw. firmware'u) muszą być domyślnie włączone (ang. enabled by default). Od tego momentu tradycyjne, podatne na ataki przy użyciu komputerów klasy CRQC, asymetryczne mechanizmy klucza publicznego (np. RSA) nie mogą być stosowane samodzielnie w obszarach wysokiego ryzyka.

- **31 grudnia 2035 r.** - pełne zakończenie transformacji systemów o średnim poziomie ryzyka. Szyfrowanie asymetryczne oparte na tradycyjnych metodach klucza publicznego przestaje być dopuszczane samodzielnie dla średniego ryzyka. Migracja systemów niskiego ryzyka musi zostać zrealizowana w stopniu, w jakim jest to technicznie i praktycznie wykonalne. Taki horyzont czasowy zapewnia spójność z ekosystemem międzynarodowym – w tym z wytycznymi USA (NIST IR 8547 oraz celami rządowymi redukcji ryzyka kwantowego do 2035 r. zapisanymi w NSM-10) oraz oficjalną mapą drogową brytyjskiego NCSC.

PIERWSZE KROKI WDROŻENIOWE “FIRST STEPS” REALIZACJA DO KOŃCA 2026 R.

Stanowią działania typu „no-regret” i podnoszą ogólny poziom dojrzałości operacyjnej wspierając zgodność z dyrektywą NIS2. Obejmują osiem kluczowych obszarów zadaniowych:

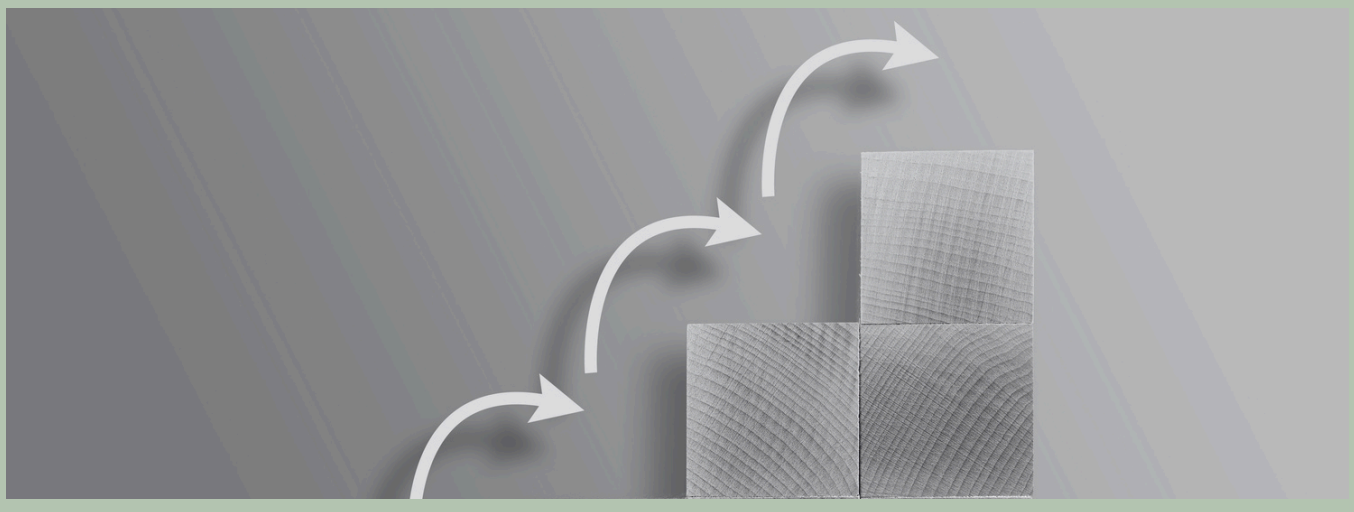
- Identyfikacja i zaangażowanie interesariuszy: ze względu na ogromny zakres oraz złożoność transformacji postkwantowej, kluczowe znaczenie ma włączenie do procesu decyzyjnego istotnych podmiotów krajowych już od samego początku, a także strukturalne i strategiczne zarządzanie ich doradztwem. Interesariusze ci powinni ściśle współpracować z organem lub organami administracji państwowej odpowiedzialnymi za wdrażanie krajowej mapy drogowej PQC[36].
- Inwentaryzacja kryptograficzna: wdrożenie rejestrów zasobów kryptograficznych (on-premise oraz w chmurze) z wykorzystaniem automatycznego wykrywania i ustandaryzowanego formatu CBOM (ang. Cryptographic Bill of Materials). Państwa Członkowskie powinny promować i wspierać tworzenie i utrzymywanie użytecznych wykazów kryptograficznych.
- Mapowanie zależności: identyfikacja powiązań wewnętrznych i zewnętrznych (od dostawców trzecich) w celu ochrony transgranicznego łańcucha dostaw w UE.
- Ewaluacja ryzyka: formalne włączenie zagrożenia kwantowego do rejestrów ryzyka na szczeblu zarządczym (board level) oraz do krajowych raportów bezpieczeństwa.
- Nadzór nad dostawcami: uruchomienie dialogu z rynkiem IT w celu wymuszenia stosowania algorytmów PQC w planach rozwojowych produktów (roadmaps).
- Szkolenia i budowa świadomości: budowa krajowego programu budowania świadomości, opartego na spersonalizowanych profilach szkoleń osobno dla kadry zarządzającej (C-level) oraz personelu inżynieryjnego (IT/OT).
- Synchronizacja z UE: aktywna wymiana doświadczeń w ramach dedykowanej grupy roboczej ds. PQC przy Grupie Współpracy NIS (NIS CG).
- Krajowa mapa wdrożenia kryptografii postkwantowej: sformułowanie krajowych ram czasowych i priorytetów

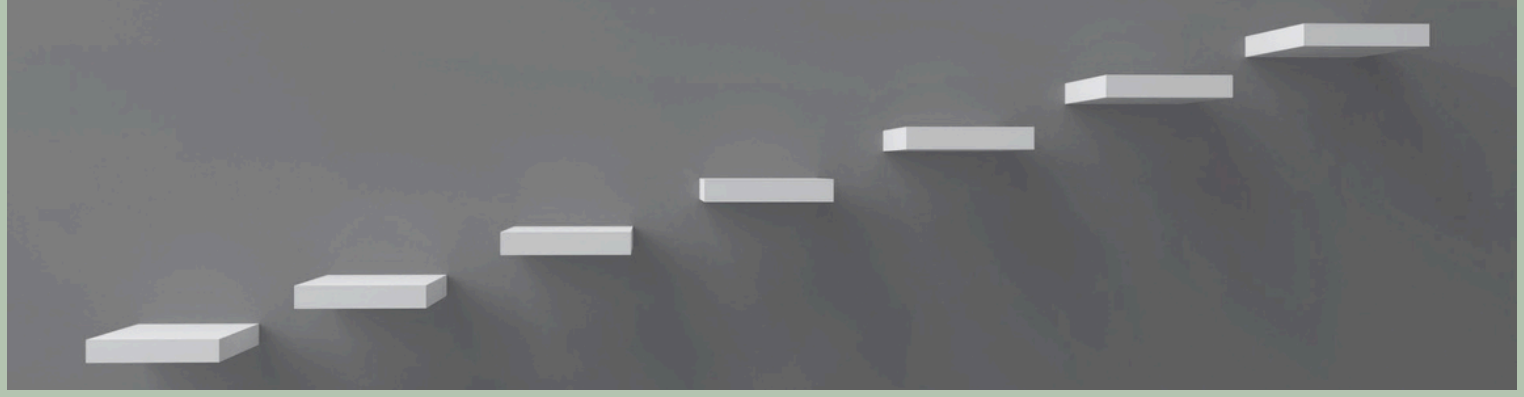


KOLEJNE KROKI “NEXT STEPS” PERSPEKTYWA DO 2030 R.

Zaawansowane działania migracyjne realizowane równolegle do etapu pierwszego “First Steps”, skupione wokół głębokiej transformacji technologicznej, dostosowania przepisów oraz procedur zakupowych i certyfikacji.

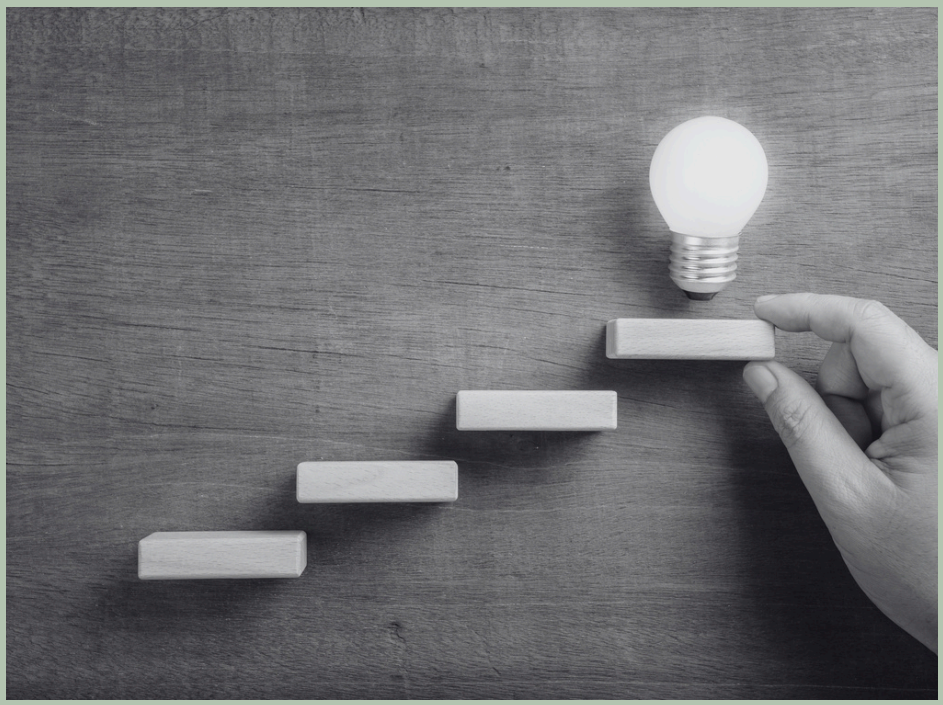
- Krypto-zwinność (crypto-agility): projektowanie protokołów w celu łatwej wymiany szyfrów bez przepisywania kodu (wymóg CRA od grudnia 2027 r.). Kluczowe jest zapewnienie ścieżki bezpiecznych kwantowo uaktualnień.
- Wdrożenie schematów hybrydowych (PQC + klasyczny algorytm) w celu uniknięcia regresu bezpieczeństwa.
- Bezpieczne aktualizacje: Wprowadzenie obowiązku zabezpieczania startu urządzeń (funkcja secure boot) oraz fabrycznego oprogramowania (firmware) nowymi, postkwantowymi podpisami cyfrowymi. Dzięki temu systemy te zyskają gwarancję, że instalowane aktualizacje oraz oprogramowanie rozruchowe są autentyczne, bezpieczne i nie zostały zmodyfikowane przez hakerów dysponujących dostępem do komputerów kwantowych.
- Finansowanie i zasoby: zabezpieczenie dedykowanych budżetów, rekrutacja personelu oraz nakaz tworzenia rezerw finansowych na migrację w cyklu życia produktu.
- Certyfikacja i audyt: integracja wymagań kwantowych z unijnymi schematami certyfikacji (w tym Europejskim Programem Certyfikacji Cyberbezpieczeństwa w oparciu o Common Criteria zgodnie z wytycznymi Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa ECCG). Uczestnicy branży certyfikacji muszą być konsultowani i zaangażowani w proces przejścia na kryptografię postkwantową.





- Przepisy i zamówienia publiczne: systematyczna aktualizacja krajowych przepisów prawnych zgodnie z najnowszymi zaleceniami dotyczącymi PQC, oraz integracja wymogów PQC do procedur zamówień publicznych.
- Współpraca w ramach ekosystemu: połączenie sił interesariuszy (podobnie jak w Kroku Pierwszym) będzie kluczem do płynnego i globalnego przejścia. Współpraca ma angażować sektor prywatny, publiczny oraz programy finansowania w celu uświadamiania (szkolenia, podnoszenie kompetencji) oraz rozwijania dedykowanych programów akademickich i doktoratów (PhD).
- Współpraca międzynarodowa: udział ekspertów państwowych w globalnej standaryzacji (NIST, ETSI, ISO), angażowanie w grupy robocze zajmujące się normalizacją PQC.

- Rozwijanie krajowych kompetencji eksperckich: państwa członkowskie powinny powoływać krajowe centra eksperckie oraz aktywnie wykorzystywać nadchodzącą unijną infrastrukturę testową finansowaną z programu Digital Europe. Działania te umożliwią precyzyjne dopracowanie modeli zagrożeń oraz ułatwią przeprowadzanie testów koncepcyjnych przed ostatecznym wdrożeniem systemów.



4.2 ENISA I ECCG - REKOMENDACJE TECHNICZNE

Proces adaptacji nowych rozwiązań postkwantowych zyskał na poziomie Unii Europejskiej ramy certyfikacyjne dzięki działaniom European Cybersecurity Certification Group (ECCG), wspieranej przez agencję ENISA. Przełomowym etapem było opublikowanie wiosną 2025 roku zaktualizowanego dokumentu „Agreed Cryptographic Mechanisms" v2.0 (ACM v2.0)[37]. Jest to pierwszy ogólnoeuropejski zbiór wytycznych, który oficjalnie włączył zatwierdzone schematy kryptografii postkwantowej do rekomendowanych rozwiązań.

Zasadniczą różnicą między mechanizmami wdrożenia kryptografii postkwantowej nakreślonymi przez ECCG a podejściem amerykańskim (bazującym głównie na standardach NIST) jest ostrożne zarządzanie ryzykiem implementacji algorytmów PQC w fazie przejściowej. Dokument wprowadza wymóg podejścia hybrydowego, nakazując łączenie nowych algorytmów postkwantowych z klasycznymi, które zostały już szeroko przebadane[38]. Architektura hybrydowa ma na celu celową dywersyfikację ryzyka kryptoanalitycznego. Europejscy regulatorzy – powołując się na wieloletnie stanowiska wyspecjalizowanych agencji krajowych, w tym francuskiej ANSSI oraz niemieckiego BSI – wychodzą z założenia, że pomimo imponującej odporności schematów kratowych na moc obliczeniową maszyn kwantowych, fundamenty ich bezpieczeństwa spoczywają na wciąż niedostatecznie długo badanych założeniach matematycznych. Połączenie warstwy kwantowej i klasycznej (tzw. zasada defense-in-depth) gwarantuje utrzymanie szczelności systemów; nawet w przypadku kompromitacji matematycznej lub odkrycia krytycznej podatności w młodym algorytmie PQC, dane chronione są nadal warstwą tradycyjną, uniemożliwiając napastnikowi pełen odczyt poufnych informacji.

4.3 REGULACJE SEKTOROWE I HORYZONTALNE

Kształtujące się podstawy prawne Unii Europejskiej sprawiają, że wdrażanie kryptografii postkwantowej przestaje być wyłącznie kwestią rekomendacji technicznych, a staje się twardym i egzekwowalnym obowiązkiem regulacyjnym. Najważniejsze europejskie regulacje - zarówno horyzontalne, jak i sektorowe - nie zawsze wymieniają wprost kryptografię postkwantową, jednak ich konstrukcja prawna, wymogi zarządzania ryzykiem oraz obowiązek stosowania środków odpowiadających „stanowi techniki" (tzw. state-of-the-art cryptography) powodują, że w praktyce wymuszają przygotowanie organizacji do ery komputerów kwantowych klasy CRQC.

Poniżej przedstawiono analizę kluczowych aktów prawnych, które bezpośrednio wymuszają na organizacjach transformację kryptograficzną.

- **Dyrektywa NIS2** oraz Ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC): Unijna dyrektywa NIS2 (Directive (EU) 2022/2555) oraz implementujące ją przepisy krajowe KSC nakładają na podmioty kluczowe i ważne prawny wymóg stosowania środków bezpieczeństwa odpowiadających aktualnemu stanowi techniki. Wraz z postępem prac standaryzacyjnych (m.in. przez NIST), to algorytmy PQC definiują nowy „stan techniki". W konsekwencji dla operatorów usług kluczowych i infrastruktury krytycznej migracja do PQC stanowi obligatoryjny wymóg prawny, a nie opcjonalne podniesienie poziomu bezpieczeństwa. Najnowsza (styczeń 2026 r.) nowelizacja do NIS2, COM(2026)13[39] (art. 7(2)(k)) znajdująca się na etapie unijnej ścieżki legislacyjnej, wymusza wręcz dodanie „polityki migracyjnej PQC" do krajowej strategii i dostosowanie krajowych wytycznych do wymogów unijnych.

- **DORA** (w mocy od stycznia 2025 r.)[40]Jeśli NIS2 jest szeroko rozumianą cyberhigieną, mechanizmem zarządzania i egzekwowania prawa, to DORA (Digital Operational Resilience Act) jest precyzyjnym instrumentem – skoncentrowanym głównie na sektorze finansowym – odnoszącym się do zmieniającego się krajobrazu zagrożeń. Choć samo rozporządzenie DORA nie wymienia wprost kryptografii postkwantowej w swoim pierwotnym tekście, to jego ramy prawne i wymogi technologiczne bezpośrednio wymuszają na sektorze finansowym przygotowanie się do ery postkwantowej. Rozporządzenie DORA, analogicznie do dyrektywy NIS2, nakłada na instytucje finansowe prawny obowiązek wdrożenia zaawansowanych środków zarządzania ryzykiem ICT, co obejmuje stosowanie najnowocześniejszych rozwiązań kryptograficznych (state-of-the-art). W momencie oficjalnego finalizowania standardów PQC przez NIST, klasyczne szyfrowanie asymetryczne przestaje spełniać kryterium "najnowocześniejszego"
- w kontekście ochrony długoterminowej. Innym aspektem jest okres przetwarzania danych. Podmioty podlegające DORA muszą przetwarzać dane finansowe i transakcyjne, których horyzont poufności często przekracza 10 lat. Brak wdrożenia krypto-zwinności oraz ochrony przed atakami typu HNDL stanowi naruszenie unijnych zasad ciągłości działania i odporności operacyjnej. W kontekście unijnej strategii, podmioty objęte zakresem DORA powinny dostosować swoje plany do oficjalnych kamieni milowych Unii Europejskiej.

- **Rozporządzenie eIDAS 2.0**[41] Nowe przepisy dotyczące identyfikacji elektronicznej i usług zaufania będą wymagały dużych zmian technologicznych. Oznacza to, że narzędzia używane dziś do potwierdzania tożsamości i autentyczności dokumentów - takie jak kwalifikowany podpis elektroniczny, pieczęcie cyfrowe czy europejski portfel tożsamości cyfrowej (EUDI) - będą musiały zostać zabezpieczone nową generacją kryptografii odpornej na komputery klasy CRQC. Bez migracji
- do PQC mogłoby dojść w przyszłości do sytuacji, w której podpisane dziś dokumenty utraciłyby swoją wiarygodność i moc prawną, ponieważ obecne mechanizmy kryptograficzne mogą zostać złamane.

- **Akt o Cyberodporności (Cyber Resilience Act – CRA)**[42] Regulacja ta wprowadza bezwzględne wymogi bezpieczeństwa w fazie projektowania (security-by-design) dla produktów z elementami cyfrowymi – PDE. Kluczowe znaczenie ma fakt, że CRA wymaga uwzględniania cyberbezpieczeństwa w całym cyklu życia tych produktów oraz wdrażania mechanizmów umożliwiających bezpieczne aktualizacje. Producenci urządzeń i oprogramowania będą musieli udowodnić stosowanie aktualnego stanu wiedzy technicznej (state-of-the-art), a ten stan wiedzy zaczyna obejmować algorytmy PQC. W praktyce oznacza to, że będą musieli przygotować swoje produkty do przyszłej migracji kryptograficznej, wymiany algorytmów, wdrażania krypto-zwinności, oraz integracji mechanizmów PQC, pod rygorem niedopuszczenia ich do obrotu na jednolitym rynku unijnym. W rezultacie od grudnia 2027 CRA stanie się jednym z najważniejszych regulatorów wymuszających praktyczne wdrażanie crypto-agility oraz „PQC-readiness" w europejskim sektorze technologicznym.

- **Ogólne Rozporządzenie o Ochronie Danych (RODO/GDPR) - Art. 32**[43] Zgodnie z wymogami zapewnienia bezpieczeństwa przetwarzania danych, administratorzy muszą wdrażać odpowiednie środki techniczne, uwzględniając aktualny stan wiedzy oraz ryzyko naruszenia praw osób fizycznych. Ignorowanie implementacji PQC w perspektywie lat 2028 i kolejnych może stanowić argument dla organów nadzorczych do uznania stosowanych zabezpieczeń za nieodpowiednie, co otwiera drogę do nałożenia kar finansowych.

4.4 MODELOWE PODEJŚCIE NIEMIECKIEGO BSI

Bundesamt
für Sicherheit in der
Informationstechnik

Niemiecki Federalny Urząd ds. Bezpieczeństwa Informacji (BSI) uznawany jest za jednego z kluczowych unijnych i globalnych liderów w obszarze wdrażania kryptografii bezpiecznej kwantowo. Oficjalne stanowisko BSI jednoznacznie odcina się od czysto akademickich dyskusji na temat precyzyjnego momentu stworzenia pierwszego komputera typu CRQC. Agencja deklaruje, że kwestia „czy" lub „kiedy" powstaną komputery kwantowe nie znajduje się już na pierwszym planie – kryptografia postkwantowa bezwzględnie stanie się nowym standardem, co wymusza natychmiastowe wdrożenie rozważnego zarządzania ryzykiem w strukturach państwa i biznesu[44]. Niemiecki model opiera się przede wszystkim na: wczesnym rozpoczęciu migracji, podejściu hybrydowym, zasadzie crypto-agility, oraz długoterminowym planowaniu dla infrastruktury krytycznej i systemów wysokiego bezpieczeństwa.

W przeciwieństwie do wielu krajów europejskich opierających się na miękkich zaleceniach, Niemcy wprowadziły precyzyjne ramy czasowe i konkretne daty graniczne dla poszczególnych sektorów gospodarki:

- **Rok 2030 – Infrastruktura Krytyczna (KRITIS):** To ostateczny termin wyznaczony przez BSI na zakończenie pełnej migracji systemów kryptograficznych dla operatorów infrastruktury krytycznej oraz instytucji rządowych przetwarzających informacje niejawne. Harmonogram ten jest ściśle skorelowany z egzekwowaniem krajowych przepisów implementujących unijną dyrektywę NIS2. Do końca 2030 roku najbardziej wrażliwe obszary rządowe muszą być bezwzględnie zabezpieczone przed atakami typu HNDL
- **Rok 2032 – Sektor Komercyjny i Pozostałe Organizacje:** Od tego punktu klasyczne metody kryptografii asymetrycznej (takie jak powszechnie stosowane RSA-2048 czy ECDSA) zostają oficjalnie uznane przez niemieckie instancje nadzorcze za niewystarczająco bezpieczne. Wszystkie podmioty komercyjne operujące na rynku niemieckim muszą do tego czasu zmigrować swoje systemy do standardów bezpiecznych kwantowo.

Zgodnie z zaktualizowaną Wytyczną Techniczną BSI TR-02102-1[45], niemiecki plan wdrożenia nakłada na inżynierów i producentów systemów dwa kluczowe obowiązki technologiczne:

- Obligatoryjna hybrydyzacja: każde nowe wdrożenie systemów kryptograficznych musi łączyć tradycyjne algorytmy klasyczne z nowymi algorytmami PQC. Zapobiega to regresowi bezpieczeństwa w przypadku wykrycia nieznanych dotąd podatności w młodych strukturach postkwantowych.
- Wymóg krypto-zwinności: nowo rozwijane produkty i systemy IT muszą posiadać modułową architekturę, umożliwiającą szybką wymianę algorytmów lub zmianę długości kluczy bez modyfikacji kodu źródłowego. BSI zaznacza, że krypto-zwinność musi stać się standardowym kryterium projektowym, ponieważ klasyczne metody ataków również ewoluują.

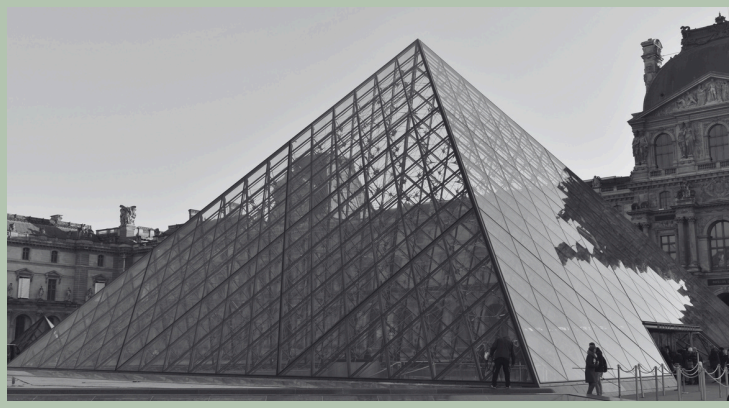
Mimo twardych ram regulacyjnych, badania rynkowe przeprowadzone w 2023 r. wspólnie przez BSI oraz firmę audytorską KPMG[46], ujawniły poważną lukę w gotowości operacyjnej biznesu. Zagrożenie kwantowe w Niemczech jest wciąż powszechnie niedoceniane – mniej niż 5% przedsiębiorstw posiada formalny, zatwierdzony plan migracji do PQC. BSI alarmuje, że czas potrzebny na pełną transformację kryptograficzną jest lekceważony przez kadrę zarządzającą. Jak wskazuje BSI, statystycznie migracja w małych organizacjach zajmuje od 5 do 7 lat, w średnich od 8 do 12 lat, natomiast w dużych korporacjach i złożonych infrastrukturach państwowych proces ten trwa od 12 do 15 lat. Oznacza to, że podmioty, które chcą osiągnąć zgodność z prawem i pełne bezpieczeństwo przed terminami 2030/2032, muszą uruchomić procedury audytowe i inwentaryzację zasobów natychmiast.

4.5 SUWERENNOŚĆ I AGRESYWNY HARMONOGRAM FRANCJI

Podczas gdy większość państw członkowskich Unii Europejskiej dostosowuje swoje działania do ogólnego unijnego horyzontu migracji wyznaczonego na rok 2035, Francja narzuca swoim instytucjom jeden z najbardziej rygorystycznych i agresywnych harmonogramów na świecie. Głównym motorem tych zmian jest państwowa Agencja Bezpieczeństwa Systemów Informacyjnych (ANSSI), która traktuje zagrożenie atakami typu HNDL jako bezpośrednie, krytyczne ryzyko dla ciągłości funkcjonowania państwa i integralności danych.

Francja należy do pierwszych państw UE, które zaczęły przekładać temat PQC na konkretne cele administracyjne. Najważniejszy dokument wykonawczy to: *„Feuille de route des efforts prioritaires en matière de sécurité numérique de l'État 2026–2027”*[47], opublikowany przez ANSSI w kwietniu 2026 r. wskazuje: rozpoczęcie pierwszych etapów inwentaryzacji kryptograficznej w latach 2026–2027, oraz cele wdrożeniowe dla administracji państwowej z perspektywą do 2030 r. Francuski plan transformacji nakłada na resorty rządowe oraz podmioty zarządzające infrastrukturą krytyczną precyzyjne i nieprzekraczalne terminy operacyjne:

- **Koniec 2026 roku – obowiązkowa inwentaryzacja danych trwałych:** Wszystkie francuskie ministerstwa zostały zobligowane do sfinalizowania do końca tego roku pełnego audytu i skatalogowania tzw. danych trwale wrażliwych (données durablement sensibles). To właśnie te zasoby informacyjne, ze względu na swój długi cykl życia (powyżej 10 lat), muszą zostać bezwzględnie objęte priorytetem migracyjnym w celu ochrony przed retroaktywnym odszyfrowaniem przez komputery kwantowe.
- **Koniec 2027 roku – wybór bloków technologicznych:** Do tego momentu administracja rządowa musi precyzyjnie zdefiniować i zatwierdzić komponenty techniczne, biblioteki oraz standardy implementacji, które posłużą do przebudowy architektury cyfrowej. Choć Francuzi w dużej mierze adaptują algorytmy standaryzowane przez amerykański NIST, ANSSI zastrzega sobie prawo do narzucania własnych kryteriów oceny ich dojrzałości.
- **Koniec 2030 roku – pełna odporność kwantowa systemów wrażliwych:** Rok 2030 to dla ANSSI wiążący termin dla Q-Day. Wszystkie systemy rządowe obsługujące informacje niejawne i strategiczne muszą w pełni zmigrować na szyfrowanie postkwantowe. Po tym terminie państwo będzie dopuszczać do użytku wyłącznie produkty bezpieczeństwa posiadające oficjalną certyfikację potwierdzającą zdolność do odparcia ataku kwantowego.



Francja jest zwolennikiem kryptografii hybrydowej. ANSSI oficjalnie uznaje, że samodzielne algorytmy PQC są jeszcze zbyt młode, by ufać im w 100%, dlatego wymaga, by każda implementacja PQC była "opakowana" w klasyczny algorytm (np. RSA lub ECC)[48].

Francja traktuje krypto-zwinność jako jeden z fundamentów odporności cyfrowej państwa. W oficjalnych wytycznych z początku 2026 roku ANSSI przypomina, że jest to bardzo skuteczny sposób na zapewnienie długoterminowej żywotności systemów w warunkach dynamicznie zmieniających się standardów międzynarodowych.

Francuski plan nie jest jedynie zapisem obowiązków – stoi za nim silne zaplecze finansowe i naukowe. Narodowa Strategia Akceleracji Technologii Kwantowych (uruchomiona z budżetem rzędu 1,8 miliarda euro) traktuje PQC jako jeden z sześciu priorytetów suwerennościowych kraju. Fundusze te zasilają m.in. program PEPR Quantum, który finansuje zarówno zaawansowane badania akademickie nad kryptoanalizą, jak i rozwój rodzimego, francuskiego przemysłu dostawców rozwiązań cyberbezpieczeństwa. Dzięki temu unijny Akt w sprawie Cyberodporności (CRA) zastanie francuski rynek z gotową podażą komercyjnych produktów spełniających najwyższe kryteria odporności.

4.6 HOLENDERSKA ŚWIADOMOŚĆ ZAGROŻEŃ

Holandia, choć mniejszy gracz, wyróżnia się systemowym podejściem do edukowania sektora publicznego i prywatnego. Holenderski rząd w 2023 opublikował podręcznik operacyjny „The PQC Migration Handbook", który został zaktualizowany w 2024 roku[49].

Podręcznik krok po kroku instruuje, jak przeprowadzić inwentaryzację kryptograficzną i stanowi jeden z najbardziej dojrzałych, metodycznych i przejrzystych wzorców w Unii Europejskiej. Charakteryzuje się wczesnym budowaniem świadomości zagrożeń oraz ścisłą współpracą państwowych organów bezpieczeństwa z sektorem naukowo-badawczym. Podręcznik stanowi ważne narzędzie dla organizacji rządowych i komercyjnych wdrażających procedury migracyjne. Za opracowanie odpowiada konsorcjum złożone z Holenderskiej Organizacji Zastosowań Nauki Społecznej (TNO), agencji AIVD oraz Centrum Matematyki i Informatyki (CWI).

Holenderski plan wdrożenia PQC kładzie nacisk na promowanie i techniczne egzekwowanie krypto-zwinności w nowo powstających aplikacjach oraz systemach teleinformatycznych. Pozwala ona na sprawną, natychmiastową wymianę poszczególnych komponentów kryptograficznych w sytuacji, gdy dotychczasowy algorytm przestanie gwarantować pożądany poziom bezpieczeństwa (np. w wyniku ewolucji klasycznych metod ataku lub postępu w budowie komputerów kwantowych). Holenderskie ramy wdrożeniowe traktują krypto-zwinność jako kluczowy element zarządzania cyklem życia zasobów IT w administracji państwowej.

Holandia należy do państw, które najwcześniej i najmocniej zaakcentowały zagrożenie: HNDL. Wspólne stanowisko AIVD i NCSC wskazuje, że najbardziej wrażliwe informacje powinny zostać zabezpieczone przed zagrożeniem HNDL najpóźniej do końca 2030 r.

Jednym z ważniejszych elementów holenderskiego modelu jest nacisk na inwentaryzację kryptograficzną (cryptographic inventory). AIVD podkreśla, że organizacje często nie wiedzą, gdzie dokładnie używana jest kryptografia, jakie algorytmy są wdrożone, oraz które systemy są zależne od klasycznych mechanizmów kryptograficznych. Dlatego holenderski model migracji rozpoczyna się od pełnej inwentaryzacji kryptografii, mapowania zależności, oceny długości życia danych, oraz klasyfikacji ryzyka.

Podobnie jak Niemcy i Francja, Holandia rekomenduje rozwiązania hybrydowe. Pełne przejście do wyłącznie PQC będzie procesem wieloletnim, dlatego konieczne jest zachowanie interoperacyjności i odporności operacyjnej. Holenderski model jest bardzo silnie zintegrowany z polityką UE, oraz stanowi jeden z fundamentów europejskiego podejścia do migracji postkwantowej. Jednak nie definiuje jednego scentralizowanego „deadline'u narodowego", ale bardzo wyraźnie wskazuje konieczność rozpoczęcia migracji natychmiast, oraz zabezpieczenia najbardziej krytycznych elementów infrastruktury państwa do końca 2030 r.

Pomimo wcześniejszych, zaawansowanych prac koncepcyjnych (takich jak opracowanie przez konsorcjum TNO, AIVD i CWI kompendium „The PQC Migration Handbook"), realne wdrożenia w sektorze publicznym są wciąż znikome. Opublikowany w maju 2026 roku raport Holenderskiego Trybunału Obrachunkowego (Algemene Rekenkamer) zatytułowany „Focus on quantum technology in central government" przyniósł bezwzględną ocenę gotowości tamtejszej administracji państwowej. Opóźnienia są szczególnie alarmujące w kontekście oficjalnych ostrzeżeń holenderskich służb wywiadowczych (AIVD). Agencja AIVD szacuje, że Q-Day – moment, w którym komputery typu CRQC będą zdolne do łamania klasycznych szyfrów asymetrycznych – może nadejść już w 2030 roku. Biorąc pod uwagę ramy czasowe (połowa 2026 r.), administracji rządowej pozostało niespełna 4 lata na przeprowadzenie transformacji systemów o krytycznym znaczeniu, takich jak system tożsamości cyfrowej DigiD, rejestry paszportowe czy systemy kontroli infrastruktury przeciwpowodziowej. W odpowiedzi na kryzys zarysowany przez raport Trybunału Obrachunkowego, Ministerstwo Spraw Gospodarczych Holandii przygotowuje nową, ogólnokrajową Strategię Kwantową (Quantum Strategy), której przedłożenie przed parlamentem zaplanowano na drugi kwartał 2026 roku[50]. Strategia ta ma na celu zdefiniowanie konkretnych celów budżetowych i czasowych dla PQC.

4.7 HISZPAŃSKA „PRYWATNOŚĆ POSTKWANTOWA”

Hiszpania nie ma jeszcze szczegółowej, publicznie komunikowanej państwowej ścieżki migracji PQC, jak Niemcy czy Francja, ale w swojej pierwszej krajowej strategii technologii kwantowych 2025–2030 wprost wpisuje priorytety strategiczne państwa: prywatność i ochronę poufności informacji w świecie postkwantowym[51]. Dokument wyznacza cztery główne cele strategiczne, z których jeden wprost dotyczy przygotowania społeczeństwa i infrastruktury na nadejście ery kwantowej poprzez zabezpieczenie systemów kryptograficznych oraz wprowadza koncepcję „prywatności postkwantowej” jako nowe prawo cyfrowe. Kwestia ta jest centralnym elementem operacyjnym Priorytetu 5 hiszpańskiej strategii („Prywatność i poufność informacji w świecie postkwantowym”), który ma na celu przygotowanie narodowych ram prawnych na utratę skuteczności obecnych algorytmów.

4.8 POLSKA GOTOWOŚĆ

Polska weszła w fazę formalizacji polityki postkwantowej później niż Niemcy czy Francja. Uchwałą Rady Ministrów nr 92 z 10 marca 2026 r. przyjęto Strategię Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025-2029[52]. Dokument, opracowany przez Ministerstwo Cyfryzacji, zastąpił poprzednią strategię wygasłą z końcem 2024 r. i - co istotne dla niniejszej analizy - wprost wymienia wśród kierunków działań „plan migracji do kryptografii postkwantowej oraz rozwój krajowej kryptografii i technologii kwantowych".

„W CELU ZWIĘKSZENIA ODPORNOŚCI SYSTEMÓW INFORMACYJNYCH BĘDZIE ROZWIJANY KRAJOWY POTENCJAŁ KRYPTOGRAFICZNY, UWZGLĘDNIAJĄCY WYZWANIA KRYPTOGRAFII POSTKWANTOWEJ (…)”[53].

W załączniku do Strategii „Plan działań na rzecz wdrożenia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej” w sekcji 3 „Podniesienie poziomu odporności systemów informacyjnych w sferze publicznej (w tym militarnej) oraz prywatnej” jako jedno z zadań wymienia się opracowanie planu migracji do kryptografii postkwantowej, za co mają być odpowiedzialne: MC jako jednostka wiodąca, Instytut Łączności-PIB, DK-WOC, NASK, ABW, MON, MRiT, SKW[54].

Najważniejszym dokumentem strategicznym regulującym ramy implementacji kryptografii postkwantowej na szczeblu krajowym są zaktualizowane „Założenia do krajowej polityki rozwoju technologii kwantowych”, opublikowane przez Ministerstwo Cyfryzacji 13 marca 2026 roku[55]. W rozdziale zatytułowanym „Bezpieczeństwo postkwantowe” dokument jednoznacznie diagnozuje konieczność natychmiastowej adaptacji systemów bezpieczeństwa do nadchodzących zagrożeń kryptograficznych generowanych przez rozwój komputerów kwantowych.

Zaproponowane w założeniach rekomendacje w pkt. 1 proponują *„Wdrożenie do 2030 roku przez administrację publiczną oraz wybrane sektory gospodarki (np. energetyka, bankowość, zdrowie) algorytmów postkwantowych (PQC) zgodnie z rekomendacjami Europejskiej Strategii Kwantowej, NIST i ETSI, celem ochrony danych przed atakami HNDL (z ang. „Harvest Now, Decrypt Later”)”.*

Wyznacznikiem zmian jest również nowelizacja ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC), będąca bezpośrednią implementacją dyrektywy NIS2. Przekłada ona ogólne unijne wytyczne na zbiór obowiązków dla podmiotów uznanych za kluczowe i ważne. Wraz z nowelizacją przepisów stosowanie nowoczesnych, aktualnych środków kryptograficznych przestaje być jedynie dobrą praktyką, a staje się wymogiem ustawowym, zwłaszcza po przyjęciu projektu poprawek COM(2026)13 do NIS2, co ma nastąpić najpóźniej w 2027 r.

Atutem Polski jest istniejące zaplecze naukowo-techniczne, które może realnie wesprzeć wdrożenie PQC, zamiast pozostawiać je wyłącznie w gestii dostawców komercyjnych. Kompetencje w obszarze kryptografii, technologii kwantowych i bezpiecznej łączności są rozproszone m.in. pomiędzy instytuty badawcze oraz wojskowe struktury cyberbezpieczeństwa. Strategia Cyberbezpieczeństwa explicite akcentuje suwerenność technologiczną - rozumianą jako ograniczanie zależności od dostawców wysokiego ryzyka i wzmacnianie rodzimego zaplecza - co tworzy przestrzeń dla krajowych ośrodków rozwijających kryptografię odporną na ataki z użyciem komputerów typu CRQC oraz komponenty kwantowo-odporne. To pozycjonuje Polskę bliżej francuskiego modelu „suwerennościowego” niż czystej adaptacji przepisów, choć bez porównywalnego zaplecza budżetowego (francuska narodowa strategia kwantowa dysponuje budżetem rzędu 1,8 mld euro, podczas gdy polskie nakłady na ten cel pozostają znacząco niższe i rozproszone).

POWAŻNYM WYZWANIEM JEST BUDOWANIE ŚWIADOMOŚCI WŚRÓD PODMIOTÓW OBJĘTYCH WYMAGANYMI ZMIANAMI.

Obecne działania mają charakter rozproszony i głównie ekspercki. Tematyka kryptografii postkwantowej pojawia się w środowisku akademickim, wybranych instytutach badawczych, sektorze telekomunikacyjnym oraz w części administracji odpowiedzialnej za cyberbezpieczeństwo. Analiza sygnałów rynkowych wskazuje na niepokojąco powolne tempo przygotowań krajowych organizacji do wdrożenia kryptografii postkwantowej. Stan ten jest w dużej mierze bezpośrednim następstwem niskiej świadomości na temat skali i pilności nadchodzących zagrożeń technologicznych. Sektorem szczególnie eksponowanym jest bankowość: polskie instytucje finansowe podlegają jednocześnie reżimowi DORA (obowiązuje od stycznia 2025 r.) i NIS2, przetwarzają dane transakcyjne o horyzoncie poufności często przekraczającym 10 lat, a przy tym funkcjonują w jednym z najczęściej atakowanych krajów Europy[56].

Połączenie długiego cyklu życia danych z intensywnością zagrożeń czyni z sektora finansowego naturalny priorytet migracyjny - analogicznie do brytyjskich wytycznych The Cross Market Operational Resilience Group (CMORG) z 2025 r.[57] oraz mapy drogowej banków centralnych Grupy G7 ogłoszonej w styczniu 2026 r.[57].

5. BENCHMARKI GLOBALNE - POLITYKI NARODOWE

5.1 WIELKA BRYTANIA – DOJRZAŁOŚĆ WDROŻENIOWA PAŃSTWA

Wielka Brytania jest jednym z najbardziej zaawansowanych państw pod względem operacyjnego planowania migracji do kryptografii postkwantowej. Nie jest to już temat wyłącznie badawczy, ale element narodowej odporności cybernetycznej, obejmujący administrację, operatorów infrastruktury krytycznej, sektor finansowy oraz duże organizacje prywatne. Centralną rolę pełni National Cyber Security Centre – NCSC, czyli brytyjskie centrum cyberbezpieczeństwa, które wyznacza kierunek, publikuje zalecenia techniczne i koordynuje przygotowania organizacji publicznych oraz sektorów krytycznych.

W marcu 2025 r. NCSC opublikowało dokument „Timelines for migration to post-quantum cryptography”[59], w którym określono krajowy harmonogram przejścia na PQC. Dokument jest skierowany przede wszystkim do dużych organizacji, administracji, operatorów infrastruktury krytycznej oraz podmiotów posiadających złożone środowiska IT.

Brytyjski plan zakłada trzy główne kamienie milowe:

- Do 2028 r. organizacje powinny zdefiniować cele migracji, przeprowadzić pełną inwentaryzację użycia kryptografii oraz przygotować pierwszy plan migracji.
- Do 2031 r. powinny zostać wykonane pierwsze migracje dla usług najwyższego priorytetu, a plan migracji powinien zostać dopracowany do poziomu pełnej mapy drogowej.
- Do 2035 r. wszystkie systemy, usługi i produkty powinny zostać zmigrowane do kryptografii postkwantowej. NCSC zaznacza, że część rzadziej używanych technologii może mieć trudności z osiągnięciem tego terminu, ale 2035 r. pozostaje głównym celem krajowym.

NCSC wskazuje, że największe ryzyko dotyczy obecnie kryptografii klucza publicznego, zwłaszcza mechanizmów wymiany kluczy i podpisów cyfrowych. Zagrożenie obejmuje zarówno przyszłe łamanie zabezpieczeń, jak i scenariusz HNDL, w którym dane są przechwytywane dziś, aby odszyfrować je po pojawieniu się komputerów typu CRQC.

Brytyjskie rekomendacje są spójne ze standardami NIST. NCSC wskazuje, że do zastosowań ogólnych odpowiednie są przede wszystkim ML-KEM (FIPS 203) oraz ML-DSA (FIPS 204).

Ważne jest również stanowisko wobec rozwiązań hybrydowych. NCSC dopuszcza schematy łączące tradycyjną kryptografię z PQC, traktując je jako rozwiązanie przejściowe, które powinno umożliwiać późniejsze przejście do architektury wyłącznie postkwantowej.

Sektor finansowy jest jednym z najważniejszych obszarów brytyjskiej migracji PQC. W 2025 r. opublikowano wytyczne The Cross Market Operational Resilience Group[60] (CMORG) dla instytucji finansowych, zgodne z podejściem NCSC i NIST[61]. Dokument ma pomóc bankom i innym instytucjom przygotować się do przejścia na praktyki kryptograficzne odporne na komputery kwantowe. Dodatkowo w styczniu 2026 r. opublikowano dokument przygotowany przez Cyber Expert Group G7 (ekspertów ds. cyberbezpieczeństwa banków centralnych Grupy G7) dotyczący skoordynowanej mapy drogowej dla sektora finansowego[62]. Wskazuje on, że przejście na PQC jest podstawową metodą ograniczenia ryzyka wynikającego z przyszłych komputerów kwantowych zdolnych łamać obecne protokoły kryptograficzne.

5.2 USA JAKO GLOBALNY LIDER INSTYTUCJONALNEJ MIGRACJI DO PQC

Stany Zjednoczone posiadają najbardziej scentralizowany, agresywny i zaawansowany prawnie program migracji do kryptografii postkwantowej (PQC) na świecie. Podejście Waszyngtonu opiera się na traktowaniu odporności kwantowej jako krytycznego elementu nadrzędnej suwerenności technologicznej oraz bezpieczeństwa narodowego. W sferze tej USA przeszło od etapu zaleceń do bezwzględnego planu wykonawczego[63]. Amerykańskie organy bezpieczeństwa zidentyfikowały zagrożenie kwantowe jako priorytet obronny znacznie wcześniej niż większość państw europejskich. Amerykańska Agencja Bezpieczeństwa Narodowego (NSA) już w 2015 roku wydała ostrzeżenie dotyczące bezpośredniego zagrożenia dla obecnych systemów kryptograficznych, wynikającego z rozwoju komputerów kwantowych. Doktryna USA kładzie nacisk na eliminację podatności w sferze ochrony danych rządowych, wojskowych oraz wywiadowczych (SIGINT), uznając, że zaniechanie natychmiastowych działań narazi kraj na skutki długofalowych ataków retrospektywnych typu HNDL.

Podstawą prawną amerykańskiej transformacji kryptograficznej są dwa kluczowe akty o charakterze obligatoryjnym:

- **National Security Memorandum 10 (NSM-10)[64]:** Memorandum prezydenckie ds. bezpieczeństwa narodowego ustanawiające strategiczne wytyczne obronne, zobowiązujące administrację rządową do maksymalnego zredukowania ryzyka kwantowego do 2030–2035 roku. Zgodnie z projektem publicznym NIST IR 8547[65] stosowanie tradycyjnych mechanizmów kryptograficznych klucza publicznego zostanie w Stanach Zjednoczonych formalnie zabronione po 2035 roku. NSM-10 ustanawia także cel strategiczny: USA mają jednocześnie utrzymać przewagę w technologiach kwantowych i ograniczyć ryzyka dla bezpieczeństwa narodowego, gospodarki oraz infrastruktury cyfrowej poprzez przejście na quantum-resistant cryptography.
- **Quantum Computing Cybersecurity Preparedness Act[66]:** Ustawa z 2023 roku nałożyła na wszystkie agencje federalne bezwzględny obowiązek przeprowadzenia szczegółowej inwentaryzacji zasobów informatycznych pod kątem stosowanych algorytmów klucza publicznego. Zobowiązuje ona administrację do priorytetyzacji systemów i przygotowania ich do migracji na standardy zatwierdzone przez NIST.

Najważniejszym terminem w amerykańskiej polityce PQC jest **2035 r.** *„Memorandum For The Heads Of Executive Departments and Agencies”* M-23-02[67] wskazuje, że celem USA jest ograniczenie możliwie największej części ryzyka kwantowego do 2035 r. Dokument nakłada na agencje federalne obowiązek prowadzenia priorytetowej inwentaryzacji systemów kryptograficznych podatnych na komputery typu CRQC.

Głównym architektem standardów matematycznych pozostaje NIST, który odpowiada za m.in. standaryzację algorytmów PQC, publikację federalnych standardów, oraz techniczne wytyczne migracyjne. Publikacja oficjalnych norm FIPS (13 sierpnia 2024 r[68]) zamknęła etap dyskusji akademickich, wprowadzając gotowe algorytmy do systemów rządowych i komercyjnych:

- **FIPS 203 (ML-KEM):** Podstawa wymiany kluczy sieciowych (sukcesor RSA i ECC).
- **FIPS 204 (ML-DSA):** Podstawowy schemat uwierzytelniania i podpisów cyfrowych.
- **FIPS 205 (SLH-DSA):** Bezstanowy podpis oparty na funkcjach skrótu jako technologia rezerwowa.

Najbardziej rygorystyczne wytyczne wdrożeniowe zostały sformułowane przez NSA w dokumencie Commercial National Security Algorithm Suite 2.0[69] (CNSA 2.0). Wyznacza on precyzyjne kamienie milowe migracji dla dostawców i operatorów systemów wojskowych i rządowych (NSS):

- Oprogramowanie i systemy operacyjne (do 2025/2026 r.): Obowiązkowe wsparcie dla PQC w przeglądarkach internetowych, platformach serwerowych i systemach klienckich.
- Sprzęt sieciowy (do 2026/2027 r.): Wymóg natywnej obsługi protokołów sieciowych chronionych przez PQC (np. routery, bramy VPN) w celu unikania fragmentacji pakietów.
- Podpisy firmware i secure boot (do 2030 r.): Wszystkie aktualizacje sprzętowe muszą być autoryzowane postkwantowo, co koresponduje z zalecanym unijnym harmonogramem Grupy NIS.
- Zakaz stosowania tradycyjnych metod klucza publicznego (do 2033–2035 r.): Całkowite zamknięcie struktur opartych na RSA i ECC w sferze systemów krytycznych.

5.3 STRATEGIA SUWERENNOŚCI CHIN I PODEJŚCIE DWUTOROWE (QKD I PQC)

Chiny realizują najbardziej niezależną i scentralizowaną na świecie strategię migracji do ery postkwantowej. W przeciwieństwie do państw zachodnich, które polegają na otwartym, międzynarodowym procesie standaryzacyjnym, strategia Pekinu opiera się na doktrynie „niezależności i pełnej kontroli" (independent and controllable). Technologie kwantowe przestały być w Chinach domeną wyłącznie badawczą, stając się filarem przemysłowym. W najnowszym, 15. Planie Pięcioletnim na lata 2026–2030 chiński rząd oficjalnie zdefiniował technologie kwantowe jako nowy punkt wzrostu gospodarczego i nadrzędny priorytet bezpieczeństwa narodowego[70]. Chiny należą do państw najbardziej zaawansowanych w zakresie komunikacji kwantowej. Państwo chińskie przez wiele lat budowało przewagę przede wszystkim wokół kwantowej dystrybucji klucza (QKD), sieci światłowodowych, satelitów kwantowych i zastosowań sektorowych. Jednocześnie podejście do kryptografii postkwantowej różni się od modelu amerykańskiego i europejskiego.

Najważniejsza różnica polega na tym, że Chiny nie opublikowały jeszcze publicznej, kompletnej mapy migracji PQC porównywalnej z amerykańskim NSM-10/CNSA 2.0 lub brytyjską mapą NCSC. Dostępne źródła wskazują jednak, że Pekin przyspiesza prace nad własnymi standardami postkwantowymi, a priorytetowymi sektorami migracji mają być finanse i energetyka. Według informacji Reutersa z marca 2026 r., chińskie standardy krajowe PQC mogą zostać opracowane w ciągu trzech lat, a najbliższy okres 3–5 lat może być w Chinach fazą szybkiego wzrostu przemysłowej migracji postkwantowej[71].

Chiński model kryptografii jest silnie scentralizowany i podporządkowany bezpieczeństwu państwa. Podstawę stanowi ustawa o kryptografii Chińskiej Republiki Ludowej z 2019 r., która klasyfikuje kryptografię na trzy kategorie: kryptografię podstawową, powszechną i komercyjną. Kryptografia podstawowa i powszechna służy ochronie informacji stanowiących tajemnicę państwową, natomiast kryptografia komercyjna jest przeznaczona do ochrony informacji nieobjętych tajemnicą państwową[72]. W praktyce oznacza to, że chińska migracja do rozwiązań quantum-safe prawdopodobnie nie będzie przyjmować formy rozproszonego, dobrowolnego modelu rynkowego. Bardziej prawdopodobny jest model centralnie sterowany, w którym standardy kryptograficzne, certyfikacja, wdrożenia oraz wymagania wobec dostawców będą rozwijane zgodnie z priorytetami państwa. Chińskie Towarzystwo Badań Kryptograficznych (CACR) we współpracy z rządem od lat prowadzi własne, wyizolowane od Zachodu procesy ewaluacji algorytmów PQC. W lutym 2025 r. Chiński Instytut Standardów Kryptografii Komercyjnej wraz z Komitetem Technicznym ds. Standaryzacji Przemysłu Kryptograficznego (Cryptography Industry Standardization Technical Committee) ogłosiły globalny nabór algorytmów nowej generacji[73]. Celem naboru jest odpowiedź na zagrożenie ze strony komputerów kwantowych oraz przygotowanie standardów nowych algorytmów kryptografii komercyjnej. Nabór obejmuje kolejno algorytmy klucza publicznego, funkcje skrótu oraz szyfry blokowe, oceniane pod kątem bezpieczeństwa, wydajności i cech technicznych. Aktualnie (maj 2026) zbierane są propozycje algorytmów kryptograficznych z kluczem publicznym. Termin składania wniosków upływa 30 czerwca 2026[74].

Najbardziej interesujący element dotyczy wyraźnego dążenia do odrębności technologicznej. W dokumencie dotyczącym wymagań wobec zgłoszeń wskazano, że konkurs nie przyjmuje algorytmów, które są już procedowane lub wystandaryzowane w organizacjach międzynarodowych, państwach lub regionach, ani ich wariantów[75].

OZNACZA TO, ŻE CHINY CHCĄ BUDOWAĆ WŁASNE ALGORYTMY I WŁASNY SYSTEM STANDARDÓW, A NIE TYLKO IMPLEMENTOWAĆ ML-KEM, ML-DSA CZY SLH-DSA JAKO STANDARDY KRAJOWE.

W przeciwieństwie do zachodnich organów ds. cyberbezpieczeństwa, które traktują QKD z pewną rezerwą, Chiny inwestują w infrastrukturę kwantowej dystrybucji klucza. Obok komunikacji satelitarnej (projekt Micius wystrzelony w 2016 r., uznawany za pierwszego na świecie satelitę komunikacji kwantowej) z sukcesem rozbudowano naziemną Chińską Sieć Komunikacji Kwantowej (CN-QCN) na linii Pekin–Szanghaj z ponad 12 000 km światłowodu, 145 węzłami szkieletowymi w 80 miastach w 17 prowincjach, połączoną z dwoma satelitami kwantowymi (Jinan-1 wystrzelony 27 lipca 2022 roku, od 25 stycznia 2026 roku działa sam, ponieważ Micius zakończył misję) i obsługującą setki agencji rządowych, banków i przedsiębiorstw państwowych[76]. Najbardziej nieoczywistym elementem chińskiego podejścia jest to, że QKD i technologie quantum-safe nie są prezentowane wyłącznie jako infrastruktura laboratoryjna lub wojskowa. Chińskie źródła branżowe wskazują na zastosowania w sektorach cywilno-państwowych. Przykłady obejmują[77]:

- połączenie quantum-secure OTN o długości 2000 km między Hefei a Mongolią Wewnętrzną realizowane przez China Telecom Quantum i Huawei,
- system „Quantum Safe Gas Station Tax Control System” do ochrony danych podatkowych w detalicznej sprzedaży paliw,
- szyfrowane usługi China Mobile oparte na kartach Super SIM,
- wykorzystanie QKD przez State Grid w demonstracyjnej stacji elektroenergetycznej 220 kV w Hefei,
- eksperymenty QKD z użyciem dronów oraz mikrosatelity Jinan-1 do międzykontynentalnej dystrybucji klucza.

Te przykłady wskazują, że Chiny testują komunikację bezpieczną kwantowo nie tylko w administracji centralnej, ale również w sektorach infrastrukturalnych: energetyce, telekomunikacji, podatkach, łączności mobilnej i sieciach operatorskich.

Chiny nie powinny być opisywane wyłącznie jako państwo „QKD-first”. Taka charakterystyka jest dziś zbyt uproszczona. Bardziej trafna jest ocena, że Pekin rozwija model podwójnej ścieżki: QKD jako warstwę infrastrukturalno-strategiczną oraz PQC jako konieczny, lecz jeszcze standaryzowany filar ochrony systemów cyfrowych.

5.4 MODEL CYBERBEZPIECZEŃSTWA DLA GOSPODARKI CYFROWEJ SINGAPURU

Singapur należy do państw, które przeszły od ogólnej świadomości zagrożenia kwantowego do budowy praktycznych narzędzi przygotowujących administrację, operatorów infrastruktury krytycznej i sektor finansowy do migracji quantum-safe. Podejście Singapuru jest szczególnie istotne, ponieważ państwo to łączy bardzo wysoki poziom cyfryzacji usług publicznych, status regionalnego centrum finansowego oraz model zarządzania cyberbezpieczeństwem podporządkowany odporności gospodarki cyfrowej.

Centralną rolę pełni Cyber Security Agency of Singapore (CSA), która odpowiada za krajowe funkcje cyberbezpieczeństwa, współpracę z sektorami krytycznymi oraz ochronę cyfrowej infrastruktury krytycznej. CSA wskazuje, że jej misją jest ochrona cyberprzestrzeni Singapuru w celu wsparcia bezpieczeństwa narodowego, gospodarki cyfrowej i cyfrowego sposobu życia obywateli[78].

Najważniejszym krokiem było opublikowanie przez CSA w październiku 2025 r. dwóch dokumentów: Quantum-Safe Handbook oraz Quantum Readiness Index (QRI)[79]. Dokumenty te zostały skierowane do właścicieli infrastruktury krytycznej, administracji publicznej, przemysłu i ekspertów, a ich celem jest przygotowanie organizacji do migracji odpornej na ataki przy użyciu komputerów typu CRQC. CSA poddała je konsultacjom publicznym od 23 października do 31 grudnia 2025 r., co pokazuje, że Singapur buduje model nie tylko ekspercki, lecz również wdrożeniowy. Istotną cechą singapurskiego podejścia jest wyraźne uznanie, że PQC będzie głównym rozwiązaniem migracyjnym.

Zgodnie z projektem „Quantum-Safe Migration Handbook” przyjęto bardzo pragmatyczne podejście do osi czasu, unikając sztywnych, ustawowych terminów, które charakteryzują np. amerykańskie czy europejskie przepisy. Główne założenia czasowe i operacyjne opisane w singapurskim dokumencie przedstawiają się następująco:

- Horyzont Q-Day szacowany na 5–10 lat: Podręcznik wprost stwierdza, że precyzyjne przewidzenie nadejścia Q-Day jest niemożliwe. Dokument przyjmuje jednak za punkt odniesienia szacunki ekspertów, które lokują ten horyzont w perspektywie najbliższych 5 do 10 lat.
- Zastrzeżenie o możliwości nagłego skrócenia czasu: CSA bardzo trzeźwo zakłada, że okno czasowe (5-10 lat) może ulec gwałtownemu skróceniu w wyniku nieprzewidzianych przełomów naukowych, optymalizacji algorytmicznych lub niejawnych osiągnięć zaawansowanych technologicznie aktorów państwowych (covert developments).
- Czasochłonność migracji jako główny czynnik decyzyjny: Z racji tego, że transformacja złożonych systemów do architektury quantum-safe to proces wieloletni (wymagający audytów, budżetowania i przebudowy systemów), CSA rekomenduje, aby organizacje - w szczególności operatorzy infrastruktury krytycznej (CII)- rozpoczęły przygotowania tak wcześnie, jak to tylko praktycznie możliwe. Zwłoka w tym procesie stanowi najwyższe ryzyko.

Singapur zakłada więc dekadę na pełne nadejście zagrożenia, ale traktuje obecny czas (od 2026 r.) jako fazę obowiązkowych przygotowań strategicznych i inwentaryzacyjnych, pozostawiając ostateczne masowe wdrożenia na czas dojrzewania samych technologii.

Singapur rozwija równolegle technologie QKD, ale nie traktuje ich jako zamiennika dla masowej migracji kryptografii stosowanej w systemach cyfrowych. National Quantum-Safe Network (NQSN) - krajowa sieć testowa mająca umożliwiać wdrażanie i ocenę komercyjnych technologii quantum-safe[80]. Celem NQSN jest prowadzenie prób z udziałem organizacji publicznych i prywatnych, ocena funkcjonalności i bezpieczeństwa oraz rozwój wytycznych i standardów dla użytkowników końcowych. Projekt ma więc charakter praktycznej infrastruktury testowej, a nie wyłącznie programu badawczego. Oznacza to, że Singapur buduje ekosystem, w którym QKD pełni rolę infrastrukturalną i testową, natomiast PQC pozostaje główną ścieżką migracji dla szerokiej klasy systemów cyfrowych. W praktyce Singapur rozwija model oparty na czterech założeniach: po pierwsze, PQC jako główna ścieżka migracji; po drugie, QKD jako warstwa testowa i uzupełniająca; po trzecie, budowa gotowości organizacyjnej przez handbook, QRI i konsultacje publiczne; po czwarte, silna koncentracja na sektorze finansowym i infrastrukturze krytycznej.

Singapur powinien być klasyfikowany jako państwo o wysokiej dojrzałości operacyjnej, mimo braku tak twardego harmonogramu migracyjnego jak USA lub Wielka Brytania.

JEGO PRZEWAGĄ NIE JEST FORMALNY „DEADLINE” USTAWOWY, LECZ PRAKTYCZNA INFRASTRUKTURA TESTOWA, JASNE WSKAZANIE ROLI CSA, WSPÓŁPRACA Z SEKTOREM FINANSOWYM ORAZ PRZYJĘCIE STANDARDÓW NIST JAKO PUNKTU ODNIESIENIA DLA MIGRACJI.

5.5 KANADA - ŚCISŁA INTEGRACJA I JEDNOLITA ARCHITEKTURA CERTYFIKACJI

Kanada pozycjonuje się jako lider wdrażania uregulowanych standardów, przyjmując strategię pełnej harmonizacji z ekosystemem bezpieczeństwa Stanów Zjednoczonych. Działania te są napędzane przez National Quantum Strategy z budżetem 360 milionów CAD (styczeń 2023) oraz rygorystycznie ujęte w ramach zaktualizowanej na 2025 rok doktryny National Cyber Security Strategy.

- **Zunifikowany front certyfikacyjny (CMVP):** ważną przewagą rynkową Kanady jest uczestnictwo w Cryptographic Module Validation Program. Program ten, współzarządzany przez kanadyjskie centrum cyberbezpieczeństwa (CCCS) oraz amerykański NIST, oznacza, że kanadyjskie wymogi ewaluacyjne dla oprogramowania i sprzętu IT automatycznie asymilują nowe standardy PQC z USA. Dla dostawców oprogramowania tworzy to spójną, pozbawioną tarć legislacyjnych, północnoamerykańską infrastrukturę walidacji produktów.
- **Ochrona infrastruktury krytycznej (CFDIR):** Organy rządowe i agencje ds. cyberbezpieczeństwa wypracowały rygorystyczne wytyczne dla kluczowych sektorów gospodarki (w tym rozbudowane listy kontrolne i kwestionariusze ewaluacyjne dla dostawców zewnętrznych). Od kanadyjskich operatorów wymaga się obecnie nie tyle pasywnej obserwacji, co bezwzględnego przeprowadzenia audytu aktywów (stworzenia dokumentacji CBOM) oraz zdefiniowania jasnego, budżetowanego harmonogramu uodparnienia łańcucha dostaw na ataki kwantowe

5.6 WIELOPOZIOMOWA OCHRONA I NARODOWA SIEĆ QKD-PQC W JAPONII

Japonia realizuje unikalną, zaawansowaną strategię bezpieczeństwa kwantowego, która w przeciwieństwie do podejścia amerykańskiego stawia na techniczną integrację algorytmów PQC z fizyczną warstwą kwantowej dystrybucji klucza (QKD). Za kształtowanie narodowej polityki odporności kwantowej odpowiadają Ministerstwo Spraw Wewnętrznych i Komunikacji (MIC) oraz National Institute of Information and Communications Technology (NICT)[81]. Japońscy eksperci od bezpieczeństwa wychodzą z założenia, że nawet najbardziej zaawansowane algorytmy oparte na kratach (Lattice-based PQC) mogą w przyszłości ulec nieoczekiwanemu złamaniu, dlatego kluczowe systemy państwowe i finansowe muszą być chronione wielowarstwowo.

Większość wdrożeń opiera się na strukturze testowanej w ramach wielkoskalowej sieci Tokyo QKD Network, rozwijanej intensywnie przez NICT we współpracy z rodzimymi gigantami technologicznymi (Toshiba, NEC, Fujitsu)[82]. Sieć ta, uruchomiona jako platforma testowa już w 2010 roku, służy do fizycznej dystrybucji kluczy symetrycznych dla administracji rządowej, sektora medycznego oraz instytucji bankowych. Klucze generowane drogą kwantową są następnie wykorzystywane jako fundament zabezpieczający dla klasycznych, postkwantowych algorytmów enkapsulacji (KEM). Wokół tej struktury Japonia wypracowała unikalną koncepcję tzw. Quantum Secure Cloud Technology[83]. System ten łączy sieć QKD, bezpieczną architekturę rozproszonego przechowywania danych oraz algorytmy kryptografii warstwy fizycznej (physical layer cryptography). Zapobiega to długoterminowym wyciekom informacji o charakterze krytycznym, takich jak dane medyczne (genetyczne) obywateli czy tajemnice państwowe, których ujawnienie za 20 lub 30 lat mogłoby doprowadzić do poważnych strat strategicznych.

W sektorze komercyjnym i telekomunikacyjnym w obszarze kryptografii postkwantowej Japonia wdraża standardy całkowicie zbieżne z normami NIST (ML-KEM i ML-DSA)[84], kładąc szczególny nacisk na uodpornienie infrastruktury sieciowej 5G/6G oraz systemów bezzałogowych, traktując odporność kwantową jako najważniejszy element obrony strategicznej w regionie Indo-Pacyfiku. Równolegle MIC koordynuje programy badawcze nad integracją segmentu kosmicznego z naziemną infrastrukturą optyczną. Prace te, realizowane poprzez mikrosatelity operujące na niskiej orbicie okołoziemskiej (LEO), mają na celu stworzenie międzykontynentalnych, odpornych na podsłuch kwantowy magistrali telekomunikacyjnych, uniezależniających kraj od fizycznych ograniczeń dystrybucji kluczy w tradycyjnych sieciach światłowodowych[85].

5.7 IZRAEL – PRAKTYCZNE ROZWIĄZANIA BANKOWE

Izrael nie ma dziś tak publicznie rozbudowanej, centralnej mapy migracji PQC jak USA, Wielka Brytania czy UE, ale ma kilka bardzo konkretnych elementów wdrożeniowych. Najważniejsze są: wytyczne Narodowego Dyrektoriatu Cybernetycznego Izraela z 2022 r., sektorowe wymagania Banku Izraela z 2025 r. oraz rozwój zaplecza badawczo-operacyjnego dla integracji PQC i QKD.

Najważniejszym dokumentem bazowym jest opracowanie Israel National Cyber Directorate (INCD): „Best Practices – Organizational Cyber Readiness to the Post-Quantum Age”[86]. Dokument został opublikowany na stronie gov.il w 2022 r. i dotyczy przygotowania organizacji na nadejście komputerów kwantowych typu CRQC. Już sam tytuł oraz opis wskazują, że Izrael wcześnie przeszedł od samego monitorowania technologii kwantowych do rekomendowania praktycznych działań przygotowawczych dla gospodarki. Izraelski model jest bardzo zbliżony do podejścia NIST: najpierw rozpoznanie miejsc użycia kryptografii podatnej na atak kwantowy, potem priorytetyzacja i plan migracji.

Najbardziej precyzyjny i formalny materiał dotyczy sektora bankowego. 7 stycznia 2025 r. Bank of Israel (BOI) skierował do banków i licencjonowanych dostawców usług płatniczych pismo pt. „Banking System Preparedness for Cyber Risks Arising from Quantum Computing Capabilities”[87]. Dokument wprost wskazuje, że silny komputer kwantowy może złamać powszechnie używane algorytmy asymetryczne, zagrozić podpisom cyfrowym, komunikacji szyfrowanej oraz poufności transakcji finansowych i danych w instytucjach finansowych. Bank Izraela odwołuje się bezpośrednio do procesu standaryzacji NIST dla PQC i wskazuje, że standardy te mają chronić dane w istniejących protokołach sieciowych i komunikacyjnych. Jednocześnie regulator zauważa, że równolegle testowane są technologie QKD dla bezpiecznej dystrybucji klucza, co pokazuje, że izraelski model jest pragmatyczny i technologicznie neutralny: głównym narzędziem migracji jest PQC, ale QKD pozostaje opcją dla określonych zastosowań.

BOI bardzo wyraźnie wskazuje ryzyko HNDL, co przesuwa temat z poziomu „przyszłej technologii” do bieżącego ryzyka operacyjnego, szczególnie dla danych długoterminowych w sektorze finansowym. Regulator wymaga od banków budowy świadomości w organizacji, stałego monitorowania rozwoju technologii kwantowych i oceny ryzyk cybernetycznych z nimi związanych. Temat ma być komunikowany zarządom i radom dyrektorów, a przegląd rozwoju technologii oraz stanu przygotowania organizacji ma być omawiany okresowo, co najmniej raz na dwa lata. Wymaga też włączenia ryzyka kwantowego do zarządzania ryzykiem łańcucha dostaw. Banki mają utrzymywać kontakt z podmiotami trzecimi, oceniać wpływ rozwoju komputerów kwantowych na dostawców oraz unikać zależności od producentów i dostawców, którzy nie przygotowują się do ery kwantowej. To bardzo istotny element: Izrael traktuje migrację PQC nie tylko jako wymianę algorytmów, ale jako problem zależności technologicznych i odporności dostawców.

Najbardziej konkretnym wymogiem jest mapowanie zaszyfrowanych zasobów informacyjnych. Banki mają identyfikować typ algorytmu i długość klucza, właściciela informacji, systemy i aplikacje używające danego algorytmu, czas wymaganego utrzymania poufności oraz poziom wrażliwości i krytyczności danych, w tym danych osobowych, medycznych, bezpieczeństwa narodowego i informacji biznesowo poufnych.

Regulator wymaga również mapowania procesów i systemów używających szyfrowania asymetrycznego w komunikacji z podmiotami zewnętrznymi oraz informacji asymetrycznie szyfrowanych poza organizacją, np. w chmurze, backupach, transferach lub danych ujawnionych w przeszłych incydentach.
To podejście jest bardzo dojrzałe, bo obejmuje nie tylko aktywne systemy, ale też dane znajdujące się poza bezpośrednią kontrolą organizacji.

Izrael buduje również zaplecze badawczo-polityczne. Center for Cyber Law & Policy przy Uniwersytecie w Hajfie, utworzone we współpracy z Israel National Cyber Directorate, prowadzi m.in. Subcenter for Quantum Cybersecurity Research[88], którego celem jest praktyczne wdrażanie bezpieczeństwa quantum-safe w środowiskach operacyjnych, w tym integracja QKD i PQC z istniejącą infrastrukturą. Choć algorytmiczne PQC stanowi fundament ochrony masowej, w niszowych, militarnych i strategicznych sieciach rządowych badana jest integracja fizycznych systemów QKD, co ma zapewnić wielowarstwową odporność (Multi-layered Security) na wypadek przyszłych przełomów w kryptoanalizie matematycznej.

IZRAEL NIE PUBLIKUJE SZEROKIEJ STRATEGII WOKÓŁ PQC, JAK TO ROBIĄ USA, WIELKA BRYTANIA CZY UE, LECZ WDRAŻA PODEJŚCIE SEKTOROWE I ZWIĄZANE Z RYZYKIEM. NAJBARDZIEJ ZAAWANSOWANYM OBSZAREM JEST SEKTOR FINANSOWY, A GŁÓWNYM MECHANIZMEM MIGRACJI JEST INWENTARYZACJA KRYPTOGRAFICZNA I PRZYGOTOWANIE ORGANIZACYJNE DO WYMIANY ALGORYTMÓW ZGODNIE Z ROZWOJEM STANDARDÓW NIST.

5.8 TWARDE WYMOGI OPERACYJNE NATO

NATO jest jedyną organizacją bezpieczeństwa zbiorowego na świecie, która opublikowała własną Strategię Technologii Kwantowych z migracją na kryptografię, ustanowiła stałą strukturę koordynacyjną (Transatlantic Quantum Community) łączącą rządy, przemysł i akademię państw członkowskich, uruchomiła akcelerator innowacji obronnych DIANA z wyodrębnioną kategorią technologii kwantowych oraz prowadzi badania techniczne przez Science and Technology Organization nad hybrydowymi rozwiązaniami łączącymi PQC i QKD do zastosowań operacyjnych. NATO nie opublikowało dotąd (jawnego) dokumentu typu mapa wdrożenia PQC z harmonogramem analogicznym do USA, UE czy Wielkiej Brytanii. Publicznie dostępne źródła pokazują jednak jasny kierunek: NATO uznaje migrację do kryptografii odpornej kwantowo za cel strategiczny Sojuszu, a PQC traktuje jako podstawowe narzędzie zabezpieczania komunikacji przed przyszłymi atakami kwantowymi.

W styczniu 2024 r. NATO opublikowało streszczenie swojej „Quantum Technologies Strategy”[89]. Dokument, którego pełna treść pozostaje niejawna, wprost wskazuje, że jednym z pożądanych rezultatów jest przejście ze swoimi systemami kryptograficznymi na kryptografię quantum-safe. To najważniejszy oficjalny zapis dotyczący kierunku migracji kryptograficznej Sojuszu. Strategia zakłada również opracowanie, przyjęcie i wdrożenie ram, polityk oraz standardów dla oprogramowania i sprzętu w celu zwiększenia interoperacyjności między państwami sojuszniczymi. W praktyce oznacza to, że migracja PQC nie jest traktowana wyłącznie jako problem cyberbezpieczeństwa, ale jako element współpracy wojskowej, przemysłowej i komunikacyjnej w ramach NATO.

Dokument Sojuszu stwierdza, że post-quantum cryptography jest obecnie ważnym podejściem do zabezpieczania komunikacji przed atakami wspieranymi przez technologie kwantowe, natomiast QKD może pełnić rolę uzupełniającą[90]. Jednocześnie NATO finansuje i wspiera badania nad integracją obu rozwiązań. Program Science for Peace and Security wskazuje, że będą podejmowane działania badające, jak integrować QKD i PQC w celu jak najbardziej całościowego zabezpieczenia infrastruktury informacyjnej Sojuszu[91].

NATO znajduje się w fazie przejścia od badań i demonstratorów do strategicznego zobowiązania migracyjnego. Sojusz chce, aby jego systemy kryptograficzne zostały przestawione na kryptografię quantum-safe. Nie ma jednak jawnego harmonogramu migracji ani technicznego katalogu algorytmów, które akceptuje NATO. Najbardziej prawdopodobny model wdrożenia zabezpieczeń odpornych na ataki kwantowe to: PQC jako warstwa podstawowa, rozwiązania hybrydowe jako etap przejściowy, QKD jako uzupełnienie dla wybranych scenariuszy wysokiego bezpieczeństwa oraz silna zależność od standardów NIST i interoperacyjności sojuszniczej.

Strategia kwantowa NATO formułuje także wymagania dla łańcucha dostaw: sojusznicy mają być świadomi i zapobiegać wrogim inwestycjom i ingerencji w ekosystemy kwantowe, co może obejmować badanie odpowiednich łańcuchów dostaw.

5.9 WYTYCZNE GRUPY EKSPERTÓW BANKÓW CENTRALNYCH G7 DOTYCZĄCE WDROŻENIA KRYPTOGRAFII POSTKWANTOWEJ W SEKTORZE FINANSOWYM

G7 CEG to grupa ekspertów od cyberbezpieczeństwa działających przy ministrach finansów i prezesach banków centralnych G7. Współprzewodniczą jej Bank Anglii i Departament Skarbu Stanów Zjednoczonych. Najważniejszym stanowiskiem G7 wobec wdrożenia kryptografii odpornej kwantowo jest opublikowany 13 stycznia 2026 r. dokument: „Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector”[92]. Nie jest to formalnie wiążąca regulacja, ale dokument referencyjny dla banków centralnych, nadzorów finansowych, instytucji finansowych, operatorów infrastruktury rynkowej, dostawców krytycznych usług i dostawców technologii kryptograficznych. G7 wyraźnie zaznacza, że dokument nie ustanawia oczekiwań regulacyjnych ani nadzorczych. Ma jednak informować, porządkować działania i wspierać terminową, bezpieczną oraz zharmonizowaną migrację sektora finansowego do PQC. W praktyce jest to tzw. „soft law”: formalnie niewiążące, ale bardzo istotne dla przyszłych działań banków centralnych i nadzorów.

Według ekspertów G7 podstawową odpowiedzią na zagrożenie związane z komputerami typu CRQC jest przejście na kryptografię postkwantową oraz algorytmy odporne kwantowo. Dokument podkreśla, że część organów krajowych już wydała wytyczne, a niektórzy uczestnicy rynku zaczęli przygotowywać plany migracji i wdrażać algorytmy quantum-resistant.

Najważniejszy element praktyczny to horyzont czasowy. G7 wskazuje, że wiele istniejących wytycznych krajowych i międzynarodowych przyjmuje 2035 r. jako ogólną datę docelową migracji do kryptografii odpornej kwantowo. Jednocześnie rekomenduje, aby systemy strategiczne były traktowane priorytetowo, z orientacyjnym oknem migracji 2030–2032. Terminy nie są sztywne, ale mają dać wspólną ramę planowania dla sektora finansowego. Roadmapa odwołuje się do ryzyka, że dane finansowe mogą zostać przechwycone dziś i odszyfrowane w przyszłości (HNDL), gdy pojawi się komputer typu CRQC. To szczególnie ważne dla sektora finansowego, ponieważ dane transakcyjne, dane klientów, dokumentacja rozliczeniowa, dane nadzorcze i tajemnice biznesowe mają długi horyzont poufności. G7 traktuje więc PQC nie jako przyszły problem technologiczny, ale jako obecne ryzyko dla bezpieczeństwa danych.

6. GLOBALNY WYŚCIG Z CZASEM

PRZEDSTAWIONA W RAPORCIE ANALIZA GLOBALNEGO PRZYGOTOWANIA NA ZAGROŻENIE Z UŻYCIEM KOMPUTERA KWANTOWEGO KLASY CRQC DOWODZI, ŻE ŚWIAT WKROCZYŁ W FAZĘ TRANSFORMACJI I DOSTOSOWYWANIA SYSTEMÓW BEZPIECZEŃSTWA DO NAJNOWSZYCH WYMAGAŃ.

ZAGROŻENIE OKREŚLANE MIANEM Q-DAY PRZESTAŁO BYĆ TRAKTOWANE JAKO HIPOTETYCZNY SCENARIUSZ Z OBSZARU TEORII NAUKOWEJ, STAJĄC SIĘ ISTOTNYM ELEMENTEM WYŚCIGU TECHNOLOGICZNEGO.

NINIEJSZE PODSUMOWANIE WSKAZUJE KLUCZOWE WNIOSKI Z MAPOWANIA STANU PRZYGOTOWAŃ, STANDARDÓW ORAZ KIERUNKÓW EWOLUCJI SYSTEMÓW OCHRONY DANYCH NA ŚWIECIE I W POLSCE.

Rok 2026 jest punktem zwrotnym migracji do kryptografii postkwantowej. Pierwsze standardy techniczne zostały sfinalizowane w sierpniu 2024 roku. Harmonogramy regulacyjne są wiążące. Szacunki zasobów potrzebnych do ataku z użyciem komputera kwantowego na obecną kryptografię drastycznie spadły w ciągu ostatnich 12 miesięcy. Czas potrzebny na pełną transformację kryptograficzną przekracza dostępne okno dla organizacji, które zwlekają z decyzją.

ZAGROŻENIE ROŚNIE SZYBCIEJ, NIŻ PRZEWIDYWANO

Wspólny wniosek łączący wszystkie analizowane przez raport środowiska eksperckie - od NIST i NSA, przez BSI i ANSSI, po holenderski AIVD i singapurskie CSA - jest jednoznaczny: tempo redukcji szacunków zasobów potrzebnych do ataku kwantowego na kryptografię RSA-2048 przebiega szybciej niż wynikało z prognoz sprzed pięciu lat.
Nie oznacza to, że komputer kwantowy zdolny do łamania algorytmów kryptograficznych już istnieje. Oznacza jednak, że zasób potrzebny do jego zbudowania kurczy się szybciej niż narasta zdolność obrony. Dla planowania migracji kluczowe jest nie to, kiedy dokładnie nastąpi Q-Day, lecz to, że czas dostępny na przygotowanie jest krótszy niż czas potrzebny na migrację.

Scenariusz Harvest Now, Decrypt Later (HNDL) przesuwa problem z przyszłości w teraźniejszość. Państwowe służby wywiadowcze USA, Wielkiej Brytanii, Holandii i Francji potwierdzają, że przechwytywanie danych z zamiarem późniejszego odszyfrowania jest aktywną praktyką operacyjną.

DLA KAŻDEJ ORGANIZACJI PRZECHOWUJĄCEJ DANE O HORYZONCIE POUFNOŚCI POWYŻEJ 5–10 LAT RYZYKO JEST BIEŻĄCE, NIE HIPOTETYCZNE.

MIGRACJA STAJE SIĘ OBOWIĄZKIEM, NIE OPCJĄ

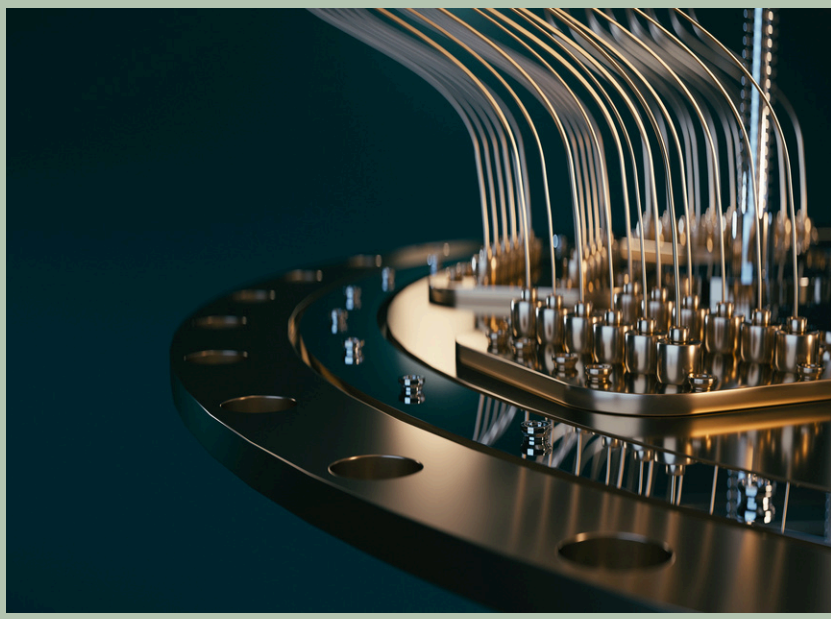
Zmiana statusu PQC w europejskim prawie jest znacząca. Do roku 2023 migracja do kryptografii postkwantowej była interpretowana jako "dobra praktyka" lub "rekomendacja techniczna". W roku 2026 jest to egzekwowalny obowiązek regulacyjny dla rosnącego grona podmiotów. Mapa wdrożeniowa NIS Cooperation Group (23 czerwca 2025 r.), wsparta rekomendacją Komisji Europejskiej i projektem nowelizacji NIS2 (COM(2026)13), ustanawia trzy terminy, które mają stać się wiążące dla członków Unii Europejskiej najpóźniej w 2027 roku.

CO OZNACZA SKUTECZNA MIGRACJA?

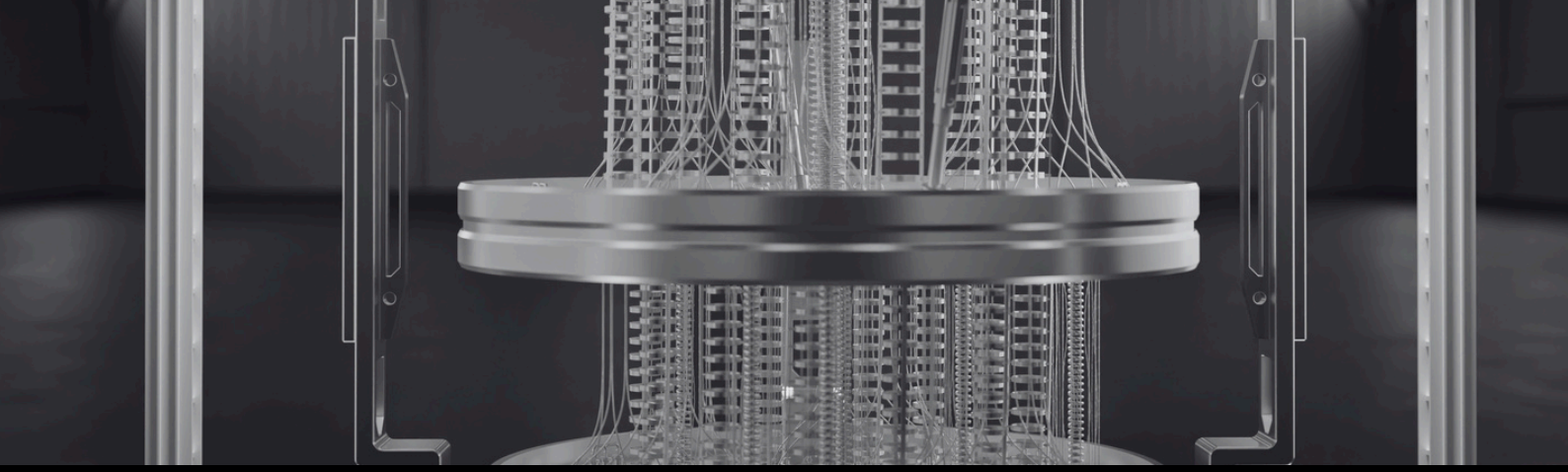
Doświadczenia państw i sektorów, które rozpoczęły migracje, wskazują wspólny mianownik skutecznego działania. Nie zaczyna się od wdrożenia nowych algorytmów, tylko od wiedzy o tym, co się posiada i co należy chronić. Identyfikacja miejsc wykorzystania kryptografii jest najtrudniejszym i najbardziej czasochłonnym etapem migracji.

Równie istotne jest projektowanie systemów umożliwiających wymianę algorytmów kryptograficznych bez konieczności przebudowy całej infrastruktury. W praktyce oznacza to odejście od rozwiązań opartych na pojedynczych technologiach na rzecz architektur zapewniających elastyczność i możliwość reagowania na przyszłe zmiany standardów.

Skuteczna migracja wymaga także podejścia opartego na znajomości ryzyka. Nie wszystkie systemy muszą zostać zmodernizowane w tym samym czasie. W pierwszej kolejności ochroną powinny zostać objęte zasoby o długim okresie poufności, infrastruktura krytyczna, systemy państwowe oraz procesy, których zakłócenie mogłoby mieć wpływ na bezpieczeństwo lub ciągłość działania instytucji.



Najbardziej dojrzałe programy migracyjne traktują kryptografię postkwantową nie jako projekt informatyczny, lecz jako element bezpieczeństwa państwa, odporności gospodarki i zarządzania ryzykiem. Ostatecznym celem nie jest wdrożenie konkretnego algorytmu, ale osiągnięcie stanu, w którym organizacja potrafi skutecznie chronić informacje i usługi niezależnie od zmian zachodzących w technologii.

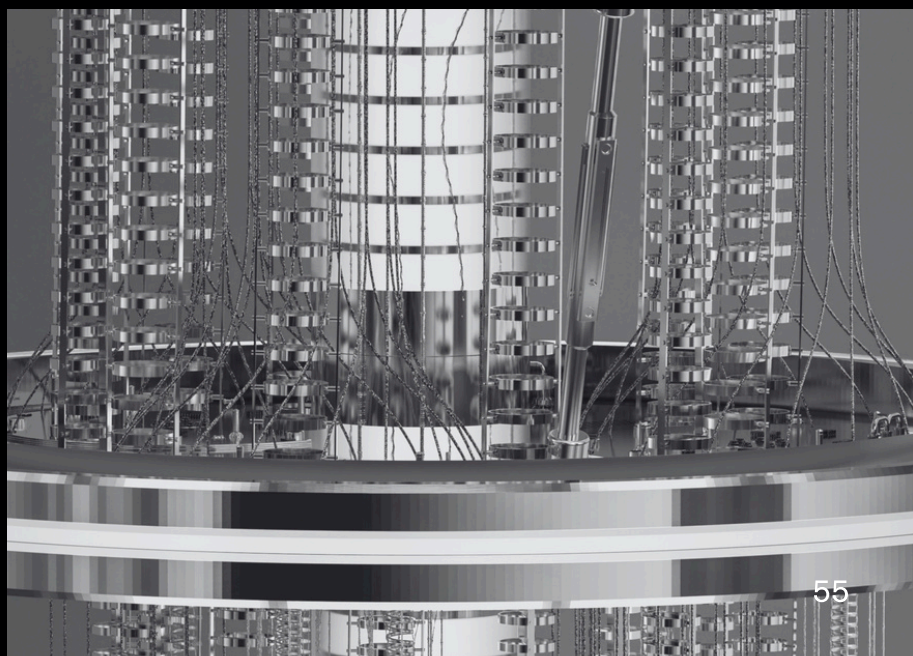


NAJWIĘKSZYM WYZWANIEM NIE JEST WYBÓR ALGORYTMÓW, LECZ SKALA ORGANIZACYJNEJ TRANSFORMACJI, KTÓRA MUSI ZOSTAĆ PRZEPROWADZONA W ADMINISTRACJI, SEKTORZE FINANSOWYM I INFRASTRUKTURZE KRYTYCZNEJ.

POLSKA DYSPONUJE KOMPETENCJAMI NAUKOWYMI I TECHNOLOGICZNYMI POZWALAJĄCYMI AKTYWNIE UCZESTNICZYĆ W TEJ ZMIANIE.

O POWODZENIU ZADECYDUJE TEMPO PRZEJŚCIA OD PLANOWANIA DO REALIZACJI ORAZ ZDOLNOŚĆ DO PROWADZENIA DZIAŁAŃ W SPOSÓB SKOORDYNOWANY NA POZIOMIE PAŃSTWA.

NAJBLIŻSZE LATA POKAŻĄ, KTÓRE KRAJE POTRAKTOWAŁY MIGRACJĘ POSTKWANTOWĄ JAKO ELEMENT DŁUGOTERMINOWEGO BEZPIECZEŃSTWA, A KTÓRE UZNAŁY JĄ ZA PROBLEM PRZYSZŁOŚCI.



7. SŁOWNIK POJĘĆ:

- ACM v2.0 (Agreed Cryptographic Mechanisms) – ogólnoeuropejskie wytyczne opublikowane w kwietniu 2025 roku przez ECCG i ENISA, które oficjalnie włączyły zatwierdzone schematy PQC do kategorii rozwiązań rekomendowanych, stawiając na hybrydyzację kryptograficzną.
- AIVD (Algemene Inlichtingen- en Veiligheidsdienst) – Główna Służba Wywiadu i Bezpieczeństwa Królestwa Niderlandów; holenderska agencja rządowa wskazująca na operacyjny charakter ryzyka kwantowego.
- ANSSI (Agence nationale de la sécurité des systèmes d'information) – Narodowa Agencja Bezpieczeństwa Systemów Informatycznych we Francji; wiodący unijny organ ds. cyberbezpieczeństwa, propagator doktryny suwerenności technologicznej, twardych harmonogramów migracji oraz obowiązkowej hybrydyzacji.
- BSI (Bundesamt für Sicherheit in der Informationstechnik) – Federalny Urząd ds. Bezpieczeństwa Informacji w Niemczech; kluczowy unijny i globalny lider wdrażania kryptografii kwantowo odpornej, autor wytycznych technicznych narzucających ramy czasowe dla sektora KRITIS i komercyjnego.
- CACR (Chinese Association for Cryptologic Research) – Chińskie Towarzystwo Badań Kryptograficznych; organizacja prowadząca niezależne od struktur zachodnich procesy ewaluacji krajowych algorytmów PQC.
- CBOM (Cryptographic Bill of Materials) – Spis wszystkich prymitywów, algorytmów, bibliotek, certyfikatów i protokołów kryptograficznych wykorzystywanych w danym systemie, aplikacji lub w całej organizacji, generowany w ustandaryzowanym formacie w celu zarządzania podatnościami.
- CCCS (Canadian Centre for Cyber Security) – Kanadyjskie Centrum Cyberbezpieczeństwa; rządowa agencja współzarządzająca programem CMVP i odpowiedzialna za krajową strategię odporności kwantowej.
- CMVP (Cryptographic Module Validation Program) – Program Walidacji Modułów Kryptograficznych współzarządzany przez USA (NIST) i Kanadę (CCCS), stanowiący zunifikowany front certyfikacji oprogramowania i sprzętu IT w Ameryce Północnej.
- CNSA 2.0 (Commercial National Security Algorithm Suite 2.0) – Zbiór wytycznych wdrożeniowych wydany przez amerykańską NSA, określający rygorystyczne i precyzyjne kamienie milowe migracji do PQC dla systemów bezpieczeństwa narodowego.
- COM(2026) 13 – Projekt poprawek do unijnej dyrektywy NIS2 zaproponowany przez Komisję Europejską w styczniu 2026 roku, wpisujący polityki migracji do PQC jako bezwzględny, obligatoryjny element krajowych strategii cyberbezpieczeństwa.

SŁOWNIK POJĘĆ:

- CRA (Cyber Resilience Act) – Unijny Akt o Cyberodporności; regulacja wprowadzająca bezwzględne wymogi bezpieczeństwa na etapie projektowania (security-by-design) oraz wymóg wdrażania krypto-zwinności i bezpiecznych aktualizacji.

- CRQC (Cryptographically Relevant Quantum Computer) – Wielkoskalowy, odporny na błędy komputer kwantowy (posiadający tysiące logicznych kubitów z korekcją błędów), zdolny do uruchamiania złożonych algorytmów kwantowych w celu złamania powszechnie stosowanych systemów klucza publicznego.

- Crypto-agility (Krypto-zwinność) – Architektoniczna i projektowa zdolność systemu informatycznego do szybkiej i łatwej wymiany algorytmów lub parametrów kryptograficznych (np. długości kluczy) bez konieczności modyfikacji kodu źródłowego aplikacji czy przepisywania infrastruktury.
- DORA (Digital Operational Resilience Act) – Unijne rozporządzenie o operacyjnej odporności cyfrowej sektora finansowego, nakładające na instytucje finansowe prawny obowiązek zarządzania ryzykiem ICT i stosowania najnowocześniejszych zabezpieczeń.

- ECCG (European Cybersecurity Certification Group) – Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa; unijny organ ekspercki złożony z przedstawicieli krajowych organów ds. certyfikacji cyberbezpieczeństwa, powołany na mocy Aktu o Cyberbezpieczeństwie (Cybersecurity Act) 2019/881

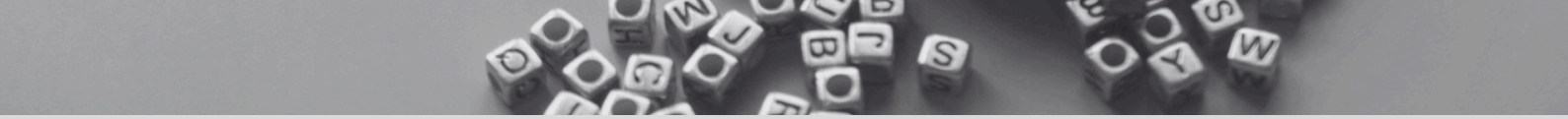
- eIDAS 2.0 – (Rozporządzenie UE 2024/1183) , które weszło w życie 20 maja 2024 roku, to nowelizacja unijnych ram prawnych dotyczących tożsamości cyfrowej i usług zaufania.

- ENISA (European Union Agency for Cybersecurity) – Agencja Unii Europejskiej ds. Cyberbezpieczeństwa; ma za zadanie zapewnić jednakowy poziom bezpieczeństwa cybernetycznego w całej Europie. Buduje zaufanie do produktów, usług i procesów cyfrowych dzięki projektowaniu systemów certyfikacji cyberbezpieczeństwa. Współpracuje z krajami i organami UE oraz pomaga przygotować się na wyzwania związane z cyberbezpieczeństwem.

- FIPS (Federal Information Processing Standards) – Oficjalne federalne standardy przetwarzania informacji publikowane przez amerykański NIST, stanowiące globalny punkt odniesienia dla procedur migracyjnych.

- HNDL (Harvest Now, Decrypt Later) – Model zagrożenia polegający na masowym przechwytywaniu i gromadzeniu zaszyfrowanych danych w teraźniejszości przez adwersarza w celu ich następczej deszyfracji w przyszłości, kiedy dostępne będą komputery kwantowe typu CRQC.

- INCD (Israel National Cyber Directorate) – Narodowy Zarząd Cyberbezpieczeństwa Izraela; organ odpowiedzialny za strategię odporności kwantowej i wymuszanie agresywnej krypto-zwinności w systemach strategicznych.



SŁOWNIK POJĘĆ:

- KNF (Komisja Nadzoru Finansowego) – Polski organ nadzoru nad sektorem finansowym, odpowiedzialny za wdrażanie rekomendacji i wymuszanie ścieżek audytowych zgodnych z reżimami NIS2 i DORA.
- LWE (Learning with Errors) – Trudny problem matematyczny polegający na rozwiązywaniu układów równań liniowych zawierających celowo wprowadzone błędy szumu, stanowiący fundament bezpieczeństwa wielu algorytmów postkwantowych (np. FrodoKEM).
- Monokultura kryptograficzna – Ryzyko nadmiernego uzależnienia całej globalnej infrastruktury cyfrowej od jednej rodziny matematycznej (obecnie od struktur kratowych), co w przypadku jej potencjalnego złamania mogłoby doprowadzić do jednoczesnego paraliżu większości zabezpieczeń.
- Michele Mosca (Formuła Mosca) – Profesor i kryptolog, twórca matematycznego narzędzia oceny ryzyka (X+Y>Z), gdzie kryzys cyberbezpieczeństwa występuje wtedy, gdy suma czasu wymaganej poufności danych (X) oraz czasu potrzebnego na migrację (Y) przewyższa czas pozostały do powstania komputerów typu CRQC.
- NCSC (National Cyber Security Centre) – Narodowe Centrum Cyberbezpieczeństwa w Wielkiej Brytanii; kluczowy organ odpowiedzialny za publikację oficjalnych harmonogramów migracji, doradztwo techniczne i koordynację odporności operacyjnej.
- NCIA (NATO Communications and Information Agency) – Agencja NATO ds. Informacji i Komunikacji; podmiot odpowiedzialny za wdrażanie wytycznych technicznych, zapewnienie interoperacyjności sojuszniczej oraz wdrażanie bezpiecznych kwantowo tuneli taktycznych.
- NICT (National Institute of Information and Communications Technology) – Narodowy Instytut Technologii Informacyjnych i Komunikacyjnych w Japonii; instytut odpowiedzialny za budowę i operacyjny rozwój wielkoskalowych sieci kwantowych (np. Tokyo QKD Network).
- NIS Cooperation Group (Grupa Współpracy NIS) – Unijny organ koordynacyjny odpowiedzialny za opracowanie wspólnej, europejskiej mapy drogowej migracji do PQC oraz wymianę doświadczeń operacyjnych między państwami członkowskimi.
- NIS2 (Directive (EU) 2022/2555) – Unijna dyrektywa nakładająca na podmioty kluczowe i ważne wymóg stosowania zabezpieczeń odpowiadających "stanowi techniki".
- NISQ (Noisy Intermediate-Scale Quantum) – Obecna era rozwoju maszyn kwantowych; urządzenia tej generacji zawierają od kilkudziesięciu do kilkuset zaszumionych kubitów fizycznych i charakteryzują się wysokim wskaźnikiem błędów oraz brakiem mechanizmów korekcji.

SŁOWNIK POJĘĆ:

- NIST (National Institute of Standards and Technology) – Amerykański Narodowy Instytut Norm i Technologii; agencja rządowa odpowiedzialna za prowadzenie globalnego procesu selekcji i standaryzacji algorytmów PQC oraz publikację norm FIPS.
- NQSN (National Quantum-Safe Network) – Singapurska krajowa sieć testowa, zarządzana przez CSA, służąca do prowadzenia prób technicznych, oceny funkcjonalności rozwiązań rynkowych oraz rozwoju standardów quantum-safe dla użytkowników końcowych.
- NSM-10 (National Security Memorandum 10) – Prezydencki dekret Joe Bidena z 2022 roku, ustanawiający strategiczne wytyczne obronne USA i zobowiązujący administrację federalną do maksymalnego zredukowania ryzyka kwantowego i wycofania podatnej kryptografii do lat 2030–2035.
- PKI (Public Key Infrastructure) – Infrastruktura Klucza Publicznego; systemy zarządzania certyfikatami, kluczami i podpisami elektronicznymi, stanowiące fundament dzisiejszego zaufania cyfrowego, bezpośrednio zagrożone przez algorytm Shora.
- PQC (Post-Quantum Cryptography) – Kryptografia Postkwantowa; nowe, klasyczne algorytmy matematyczne (np. oparte na kratach euklidesowych, funkcjach skrótu lub kodach), które mogą być wykonywane na dotychczasowych, klasycznych komputerach i przesyłane przez istniejące sieci, wykazując pełną odporność na ataki przy użyciu maszyn klasycznych i kwantowych typu CRQC.
- Q-Day – Krytyczny punkt zwrotny w osi czasu cyberbezpieczeństwa; hipotetyczny moment, w którym technologie komputerów kwantowych osiągną skalę i stabilność (typ CRQC) pozwalającą na łamanie w czasie rzeczywistym powszechnie stosowanych klasycznych kluczy asymetrycznych (RSA, ECC).
- QKD (Quantum Key Distribution) – Kwantowa Dystrybucja Klucza; sprzętowe systemy telekomunikacyjne wykorzystujące fundamentalne zjawiska mechaniki kwantowej do bezpiecznego generowania i współdzielenia symetrycznego tajnego klucza wyłącznie między dwoma fizycznymi punktami połączenia.
- QRI (Quantum Readiness Index) – Singapurski indeks gotowości kwantowej opublikowany przez CSA w październiku 2025 r., stanowiący narzędzie audytowe ułatwiające organizacjom samoocenę i planowanie faz transformacji kryptograficznej.

8. DODATEK: MIESIĘCZNY PRZEGLĄD TRENDÓW TECHNOLOGICZNYCH – MAJ 2026

Opracowano na podstawie cyklicznych raportów monitoringu trendów technologicznych Instytutu Łączności – Państwowego Instytutu Badawczego

Maj był kolejnym miesiącem, który potwierdził, że era fascynacji sztuczną inteligencją bezpowrotnie przeminęła. Po fazie krytycznego spojrzenia (która nastąpiła po fazie bezkrytycznej fascynacji) oraz poszukiwania optymalizacji kosztowej nadszedł czas zarządzania suwerennością cyfrową oraz bezpieczeństwem narodowym nie tylko w kontekście AI. Skala oraz tempo wdrażania rozwiązań o podwójnym zastosowaniu (dual-use) wymusiły na państwach odejście od pasywnej obserwacji na rzecz aktywnego kształtowania własnych architektur technologicznych. Bezpieczeństwo narodowe, stabilność demokratyczna oraz odporność łańcuchów dostaw zależą dziś także bezpośrednio od stopnia kontroli nad systemami obliczeniowymi, fizyczną produkcją półprzewodników i algorytmami kryptograficznymi.

Najważniejsze wydarzenia z rynku technologicznego zostały pogrupowane w cztery główne trendy wymienione poniżej:

1. Militarna i ofensywna ewolucja Sztucznej Inteligencji (AI). *Sztuczna inteligencja przestała być postrzegana jako narzędzie optymalizacji biznesowej, stając się kluczowym komponentem działań kinetycznych, wywiadowczych i operacji psychologicznych (PSYOPS).*

Integracja sektora prywatnego i przemysłu obronnego. Najlepszym dowodem na militaryzację rynku AI są rekordowe kontrakty Departamentu Obrony USA z wiodącymi dostawcami technologii komercyjnych – konsorcjum obejmującym firmy OpenAI, Google, Microsoft, Amazon Web Services (AWS), NVIDIA oraz SpaceX. Zastosowanie zaawansowanych modeli poznawczych w sieciach niejawnych o najwyższym rygorze bezpieczeństwa (Impact Levels 6 i 7) odbywa się przy radykalnym skróceniu cyklu wdrożeniowego do zaledwie trzech miesięcy. Co istotne, Pentagon zdecydował o zniesieniu standardowych mechanizmów ograniczających bezpieczeństwo w systemach niejawnych, przedkładając autonomię decyzyjną i szybkość reakcji nad deterministyczną przewidywalność algorytmów. Ta decyzja może sprawić, że systemy AI działające samodzielnie zaczną zachowywać się w nieprzewidywalny i trudny do kontrolowania sposób.

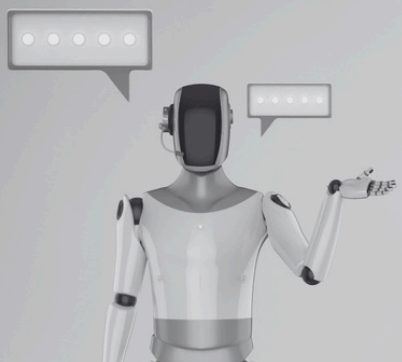
AI napędza cyberataki na skalę przemysłową. Firma Google zaraportowała w maju 2026 roku gwałtowne skrócenie cyklu eksploatacji podatności systemowych (wektorów zero-day). Dzięki generatywnym modelom agentowym, procesy hakerskie zostały zindustrializowane na masową skalę. Systemy automatycznie generują kod i wykorzystują zidentyfikowane luki w zabezpieczeniach. Powoduje to, że tradycyjne, reaktywne paradygmaty ochrony oparte na interwencji ludzkiej (centra SOC) i statycznych regułach stają się całkowicie niewydolne, gdyż czas na aplikację łat (patching) skurczył się do poziomu uniemożliwiającego manualną reakcję

Zagrożenia dla Procesów Demokratycznych. Wpływ halucynacji modeli językowych na sferę publiczną został precyzyjnie zmierzony przez organizację Demos. W symulacji przeprowadzonej przed majowymi wyborami do szkockiego parlamentu, zadano 75 pytań dotyczących trzech okręgów wyborczych pięciu darmowym narzędziom AI (ChatGPT, Google Gemini, Grok i Replika). Wyniki okazały się alarmujące: narzędzia podały błędne informacje w aż 34% odpowiedzi. Skala błędów wahała się od 9% (Grok) do aż 56% (Replika). Wśród wygenerowanych halucynacji znalazły się:

- całkowicie wymyślone skandale obyczajowe i korupcyjne,
- błędne daty wyborów,
- fałszywe instrukcje prawne (np. informacja o nieistniejącym obowiązku okazania konkretnych dokumentów tożsamości),
- wprowadzenie do bazy danych fikcyjnych, nieistniejących kandydatów.

Skalę problemu potęguje fakt, że z sondażu Demos wynika, iż 20% brytyjskich dorosłych (ok. 10 milionów obywateli) czerpało wiedzę o procesie wyborczym bezpośrednio z chatbotów AI.

Geopolityczna ekspansja zaplecza inżynieryjnego. Najwięksi dostawcy AI odchodzą od modelu czysto chmurowego na rzecz budowy fizycznych przyczółków innowacji w regionach strategicznych. Przykładem jest inicjatywa "OpenAI for Singapore". OpenAI podpisało memorandum z singapurskim Ministerstwem Rozwoju Cyfrowego i Informacji, deklarując inwestycję rzędu 300 mln dolarów singapurskich. W jej ramach powstanie pierwsze poza USA laboratorium Applied AI Lab, zatrudniające ponad 200 wysokiej klasy specjalistów, dedykowane wdrażaniu AI w administracji, ochronie zdrowia i finansach Singapuru.



2. Kwantowa rywalizacja o bezpieczeństwo. *W obszarze technologii kwantowych uwaga przesunęła się z badań na wdrożenia rozwiązań przygotowujących systemy architektury cyberbezpieczeństwa państw przed nadejściem Q-Day (momentu, w którym komputer kwantowy typu CRQC będzie mógł złamać klasyczne klucze kryptografii asymetrycznej).*

Więcej informacji, w raporcie głównym na początku opracowania.

3. Poszukiwanie wydajności: Fotonika i przetasowania w łańcuchach dostaw. *Wzrost złożoności modeli AI doprowadził do zderzenia branży informatycznej z fizycznymi barierami architektury krzemowej, zużycia energii i przepustowości pamięci. Tradycyjne procesory i pamięci przestają nadążać za złożonością modeli kognitywnych. Konieczność przełamania ograniczeń termicznych i przepustowości wymusza rewolucję: odejście od monopolu GPU na rzecz systemów heterogenicznych oraz zastępowanie elektronów światłem. Kto pierwszy opanuje tę zmianę, zdobędzie sprzętową dominację na kolejne dekady.*

Kryzys niedoboru pamięci. Rynek komponentów pamięciowych znalazł się w stanie głębokiego strukturalnego niedoboru. Ceny pamięci DRAM wzrosły o ok. 172% rok do roku. Sytuację zaostrza fakt, że giganci technologiczni agresywnie zabezpieczają podaż na lata w przód – OpenAI wykupiło na pniu około 40% globalnej produkcji pamięci DRAM na potrzeby swojego monumentalnego projektu budowy centrum danych Stargate. Masowe przesunięcie mocy produkcyjnych w stronę pamięci wysokoprzepustowej (HBM) dla akceleratorów AI drastycznie ograniczyło dostępność
i podniosło koszty standardowych kości (np. DDR5). Koszt pamięci stanowi obecnie od 15-25% do nawet ponad 35% całego kosztu produkcji urządzeń (BOM), co zmusza producentów do sprzętowej kompresji danych i ograniczania wydajności systemów.

Powrót CPU jako fundamentu infrastruktury AI. Infrastruktura AI odchodzi od monolitycznego modelu „GPU-only" na rzecz architektur heterogenicznych. Potwierdzają to doskonałe wyniki finansowe firmy Intel za I kwartał 2026 roku (przychód 13,6 mld USD, wzrost segmentu *Data Center and AI* o 22%). Procesory CPU odzyskują kluczowe znaczenie rynkowe, stając się filarem procesów wnioskowania (*inference*), obsługi systemów agentowych i zarządzania heterogenicznymi przepływami danych. Świadczy o tym wybór procesorów *Intel Xeon 6* jako jednostek nadrzędnych (*host CPU*) dla najnowszego, flagowego systemu NVIDIA DGX Rubin. Jednocześnie rozwój ramienia produkcyjnego *Intel Foundry* wpisuje się w trend regionalizacji łańcuchów dostaw w obliczu napięć geopolitycznych w Azji.

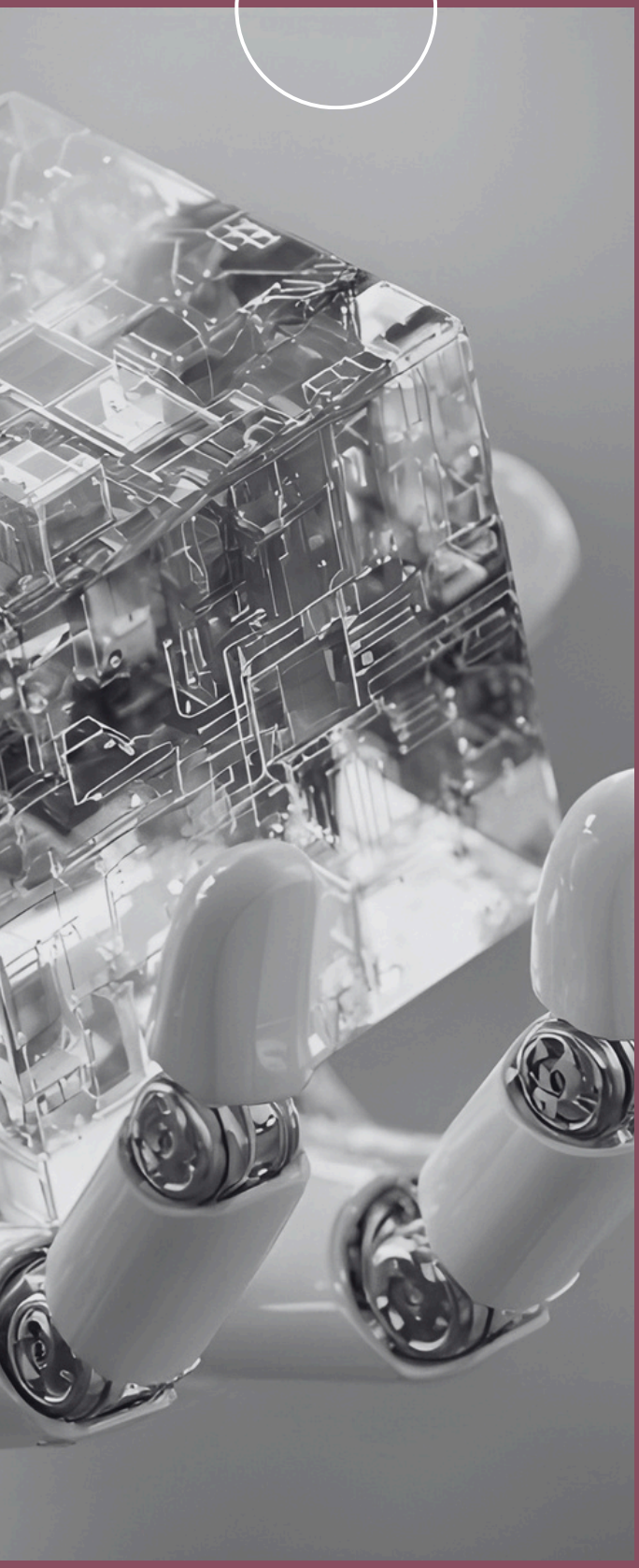
Fotonika komercyjna jako alternatywa energetyczna. Ponieważ dostępność mocy energetycznej w centrach danych stała się głównym hamulcem rozwoju sztucznej inteligencji, świat inwestuje w fotonikę (wykorzystanie światła zamiast elektronów do obliczeń i transferu danych).

- **Chip Lumai Iris:** *Lumai* (spin-off Uniwersytetu Oksfordzkiego) zaprezentował architekturę serwerową z rodziny *Iris*, w której kluczowe operacje AI (mnożenie macierzy o potężnych rozmiarach do 2048×2048) wykonywane są za pomocą fal świetlnych. Pozwala to na eliminację narzutu procesorów graficznych i skutkuje o 90% niższym zużyciem energii w porównaniu z klasycznymi systemami GPU.

- **Inicjatywy Europejskie**: W Leuven w Belgii, w ramach unijnego programu *Chips Joint Undertaking*, uruchomiono SPINS – jedną z sześciu europejskich linii pilotażowych produkcji półprzewodników kwantowych i mikroelektroniki. Z kolei w Hiszpanii przyspieszają inwestycje w ramach projektu PIXEurope o wartości ponad 400 mln euro, nakierowanego na budowę zdolności przemysłowych w zakresie układów fotonicznych.

- **Komercjalizacja w Kanadzie**: Rząd Kanady podjął decyzję o całkowitym wydzieleniu ośrodka *Canadian Photonics Fabrication Centre (CPFC)* ze struktur publicznych i przekształceniu go w komercyjny spin-off rynkowy w celu szybszego przyciągania kapitału prywatnego i skrócenia czasu wdrażania innowacji fotonicznych dla sektorów AI i obronności.

Walka o efektywność zasilania. Rywalizacja technologiczna przeniosła się z czystej mocy obliczeniowej na poziom efektywności dostarczania energii bezpośrednio do struktur krzemowych. Amerykański producent układów analogowych Analog Devices (ADI) ogłosił plan przejęcia startupu *Empower Semiconductor* za gigantyczną kwotę 1,5 mld USD. Powodem transakcji jest unikalna własność intelektualna Empower w obszarze zintegrowanych regulatorów napięcia (IVR). Układy te są montowane bezpośrednio przy procesorze, co eliminuje tradycyjne, rozproszone komponenty zasilania, drastycznie zmniejsza rozmiar systemów zasilających i minimalizuje straty energii w centrach danych AI.



Nowa geopolityka łańcuchów dostaw. Globalne łańcuchy dostaw są redefiniowane w celu ominięcia tradycyjnych centrów w Azji Wschodniej. Przykładem jest m.in. umowa między holenderskim ASML a indyjskim Tata Electronics na budowę fabryki w Indiach. Poniżej wybrane przykłady tych procesów:

- **Sojusz ASML i Indii:** Holenderski lider litograficzny ASML podpisał memorandum z indyjskim koncernem Tata Electronics. Współpraca dotyczy budowy pierwszej w Indiach komercyjnej fabryki półprzewodników (wafli 300 mm) w miejscowości Dholera. Inwestycja opiewa na 11 mld USD i ma osiągnąć wydajność produkcyjną na poziomie 50 tys. wafli miesięcznie. Fabryka celowo skupi się na dojrzałych, lecz krytycznych rynkowo procesach technologicznych (28-110 nm), zaspokajając potrzeby branży motoryzacyjnej, IoT i elektroniki przemysłowej.
- **Oś Seul-Hanoi:** Wietnam i Republika Korei zintensyfikowały partnerstwo strategiczne. Południowokoreańscy liderzy (Samsung, SK Hynix) oferują transfer technologii i wsparcie infrastrukturalne HPC/AI w zamian za stabilną bazę surowcową i produkcyjną w Wietnamie, tworząc nowy biegun technologiczny zdolny rywalizować z Chinami w obszarze pakowania i testowania półprzewodników (ATP).
- **Dywersyfikacja Apple:** Na rynku amerykańskim doszło do wstępnego porozumienia pomiędzy Apple i Intelem. Intel, w ramach swojego biznesu foundry, ma przejąć część zamówień na produkcję chipów projektowanych przez Apple, co pozwoli ograniczyć głębokie uzależnienie korporacji z Cupertino od mocy produkcyjnych tajwańskiego TSMC.

4. Big Tech kontra Państwo: Batalia o Algorytmy i Suwerenność Danych. *Gwałtowna ekspansja systemów analitycznych i kognitywnych w strukturach państwowych wywołuje głębokie napięcia na styku prawa, suwerenności danych i etyki.*

Ryzyko Monopolu Infrastrukturalnego w Służbie Zdrowia. Wielkie kontrowersje wzbudziła decyzja Narodowej Służby Zdrowia (NHS) w Anglii, która rozszerzyła zakres dostępu amerykańskiej korporacji Palantir do strukturyzowanych i niestrukturyzowanych danych medycznych pacjentów w ramach platformy *Federated Data Platform (FDP)*. Przekazanie operacyjnej kontroli nad potokami danych publicznych podmiotowi o rodowodzie wywiadowczo-obronnym wywołało masowy opór społeczny i groźbę masowego wycofywania zgód na przetwarzanie danych (*opt-out*). Eksperci alarmują, że wdrożenie własnościowego oprogramowania uniemożliwia transparentny audyt algorytmów, niesie ryzyko reidentyfikacji pacjentów technikami AI oraz grozi trwałym uzależnieniem strategicznym od dostawcy spoza Europejskiego Obszaru Gospodarczego.

Algorytmy w zarządzaniu a kondycja poznawcza człowieka. Międzynarodowa Organizacja Pracy (ILO) opublikowała raport wykazujący bezpośrednią korelację pomiędzy implementacją systemów AI do nadzoru nad pracownikami a drastycznym obniżeniem ich autonomii decyzyjnej, intensyfikacją tempa pracy i wzrostem obciążenia psychicznego. Algorytmiczna nieprzejrzystość (*opacity*) procesów zarządczych prowadzi do dehumanizacji relacji pracowniczych, generując realne koszty systemowe związane z wypaleniem zawodowym i absencją chorobową.

Transatlantycka asymetria regulacyjna. Na poziomie legislacyjnym pogłębia się przepaść pomiędzy Unią Europejską (wdrażającą restrykcyjny AI Act) a USA.
W Stanach Zjednoczonych Departament Sprawiedliwości USA oraz firma xAI (Elona Muska) oficjalnie zakwestionowały przed sądem przepisy stanowe Kolorado (Senate Bill 205). Przepisy te nakładały na producentów systemów AI wysokiego ryzyka obowiązek technicznej oceny modeli pod kątem uprzedzeń i potencjalnej dyskryminacji. Strona skarżąca argumentuje, że regulacje te bezprawnie ograniczają proces projektowania systemów. Brak jednolitych standardów grozi transferem na rynek europejski modeli o całkowicie niezweryfikowanej strukturze etycznej.

Aktywna rola krajowych regulatorów: Przykład Polski

W odpowiedzi na zagrożenia rynku cyfrowego, polski Urząd Ochrony Konkurencji i Konsumentów (UOKiK) przeszedł od reaktywnej ochrony konsumentów do proaktywnego monitoringu algorytmicznego. Prezes UOKiK wdrożył zaawansowane narzędzia oparte na uczeniu maszynowym i przetwarzaniu języka naturalnego (NLP) do automatycznej identyfikacji zwodniczych interfejsów (dark patterns) w handlu elektronicznym. Systemy te w czasie rzeczywistym analizują strukturę witryn sklepów internetowych, automatycznie wykrywając i flagując manipulacje rynkowe, takie jak fałszywe liczniki czasu czy sztucznie generowane powiadomienia o rzekomym wysokim popycie na dany produkt.

WNIOSKI PŁYNĄCE Z ANALIZY MAJA 2026 ROKU SĄ JEDNOZNACZNE: NOWOCZESNE PAŃSTWO NIE MOŻE BUDOWAĆ STRATEGII BEZPIECZEŃSTWA W OPARCIU O ZAMKNIĘTE, ZAGRANICZNE EKOSYSTEMY. POLSKA MUSI PILNIE DĄŻYĆ DO:

- Zainicjowania krajowego, skoordynowanego planu migracji do kryptografii postkwantowej (PQC) obejmującego m.in. audyt podatności systemów administracji publicznej i sektora finansowego.
- Wyznaczenia instytucjonalnych właścicieli procesów migracji kryptograficznej w każdej kluczowej instytucji państwowej.
- Rozwoju suwerennych, odizolowanych środowisk obliczeniowych oraz własnych, krajowych modeli detekcji anomalii sieciowych w celu uniezależnienia się od silników analitycznych dostawców spoza EOG.

BIBLIOGRAFIA

1. Pojęcie CRQC zostało spopularyzowane przez administrację USA i środowisko bezpieczeństwa narodowego jako sposób odróżnienia eksperymentalnych komputerów kwantowych od systemów zdolnych do realnego przełamywania współczesnej kryptografii.
2. John Preskill, *Quantum Computing in the NISQ era and beyond*, Quantum 2, 79 (2018). *https://doi.org/10.22331/q-2018-08-06-79*.
3. Frank Arute et al. (Google AI), *Quantum supremacy using a programmable superconducting processor*, Nature 574, 505–510 (2019). https://doi.org/10.1038/s41586-019-1666-5.
4. Craig Gidney, Martin Ekerå, *How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits*, Quantum 5, 433 (2021). https://doi.org/10.22331/q-2021-04-15-433 oraz aktualizacja Craig Gidney, „How to factor 2048 bit RSA integers with less than a million noisy qubits", arXiv:2505.15917, 21 maja 2025, s. 1. Abstract https://arxiv.org/abs/2505.15917.
5. ENISA, Post-Quantum Cryptography: Current state and quantum mitigation (2021) https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation.
6. Lov K. Grover. A fast quantum mechanical algorithm for database search. In STOC '96: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pages 212-219, New York, NY, USA, 1996. ACM Press. https://arxiv.org/abs/quant-ph/9605043
7. National Institute of Standards and Technology (NIST). Post-Quantum Cryptography https://csrc.nist.gov/projects/post-quantum-cryptography 2024.
8. Craig Gidney, „How to factor 2048 bit RSA integers with less than a million noisy qubits", arXiv:2505.15917, 21 maja 2025, s. 1. Abstract https://arxiv.org/abs/2505.15917
9. "The Pinnacle Architecture: Reducing the cost of breaking RSA-2048 to 100 000 physical qubits using quantum LDPC codes", arXiv:2602.11457, 12 lutego 2026, s1 abstract https://arxiv.org/abs/2602.11457.
10. https://www.ibm.com/quantum/hardware#roadmap.
11. Stosunek między kubitami fizycznymi a logicznymi zależy od przyjętej architektury korekcji błędów.
12. Michele Mosca, profesor i współzałożyciel Instytutu Quantum Computing na Uniwersytecie w Waterloo.
13. Cybersecurity in an Era with Quantum Computers: Will We Be Ready?"https://ieeexplore.ieee.org/document/8490169.
14. *FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism Standard*, National Institute of Standards and Technology, 13 August 2024, https://csrc.nist.gov/pubs/fips/203/final.
15. *FIPS 204 Module-Lattice-Based Digital Signature Standard*, National Institute of Standards and Technology, 13 August 2024, https://csrc.nist.gov/pubs/fips/204/final.
16. https://csrc.nist.gov/news/2022/pqc-candidates-to-be-standardized-and-round-4.
17. Dla wariantu FN-DSA-512 ok 666 bajtów wobec 2420 bajtów dla ML-DSA-44.
18. Falcon bazuje na starszych, ale doskonale zbadanych kratach typu NTRU (N-th degree Truncated polynomial Ring Units) i wykorzystuje szybką transformatę/transformację Fouriera (FFT) do optymalizacji operacji matematycznych. To właśnie ta specyficzna struktura NTRU w połączeniu z arytmetyką zmiennoprzecinkową pozwala Falconowi na osiągnięcie podpisu niedużych rozmiarów i bardzo krótki czas weryfikacji. Stanowi to jego największą zaletę, ale sam proces generowania podpisu wymaga dużych zasobów.

BIBLIOGRAFIA

19. Falcon posiada bardzo mały podpis i ekstremalnie szybką weryfikację, co pozornie czyni go idealnym dla IoT. Jednakże proces generowania podpisu (signing) wymaga skomplikowanych operacji na liczbach zmiennoprzecinkowych w czasie stałym (constant-time 64-bit floating-point arithmetic). Typowe urządzenia brzegowe (tanie mikrokontrolery, IoT bez jednostek FPU) nie są w stanie tego bezpiecznie i wydajnie policzyć. Próba emulacji naraża je na ataki z kanałów bocznych (side-channel attacks).
20. NIST SP 800-208, Recommendation for Stateful Hash-Based Signature Schemes, National Institute of Standards and Technology, Październik 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-208.pdf.
21. ANSSI views on the Post-Quantum Cryptography transition (2023 follow up) 21 grudnia 2023, https://messervices.cyber.gouv.fr/documents-guides/follow_up_position_paper_on_post_quantum_cryptography.pdf.
22. *FIPS 205, Stateless Hash-Based Digital Signature Standard*, National Institute of Standards and Technology, 13 sierpnia 2024 https://csrc.nist.gov/pubs/fips/205/final.
23. BSI TR-02102-1 "Cryptographic Mechanisms: Recommendations and Key Lengths" Version: 2026-01.
24. NIST PQC Standardization Process | HQC Announced as a 4th Round Selection, National Institute of Standards and Technology, 11 marca 2025, https://csrc.nist.gov/news/2025/hqc-announced-as-a-4th-round-selection.
25. j.w. , https://csrc.nist.gov/news/2025/hqc-announced-as-a-4th-round-selection
26. Wouter Castryck, Thomas Decru, *An Efficient Key Recovery Attack on SIDH*, 2022, https://eprint.iacr.org/2022/975.
27. https://digital-strategy.ec.europa.eu/pl/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography.
28. Uwaga do datacji dokumentu: W publicznej dyskusji o dokumencie krążą dwie daty, które warto rozróżnić: 11 czerwca 2025 - data finalizacji wersji 1.1 dokumentu przez NIS Cooperation Group (NIS CG), wewnątrz Grupy Współpracy. 23 czerwca 2025 - data oficjalnej publikacji dokumentu przez Komisję Europejską na portalu “Shaping Europe’s Digital Future” (digital-strategy.ec.europa.eu) i jednoczesnego komunikatu prasowego “EU reinforces its cybersecurity with postquantum cryptography”. Obie daty są poprawne - odnoszą się do dwóch różnych momentów cyklu wydawniczego.
29. https://digital-strategy.ec.europa.eu/pl/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography.
30. DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive (EU) 2022/2555, 20 styczeń 2026, COM(2026)13 Directive Proposal for simplification measures and alignment with the Cybersecurity Act , art 7(2)(k) str. 12 oraz motyw 8, str. 8, https://digital-strategy.ec.europa.eu/pl/library/proposal-directive-regards-simplification-measures-and-alignment-cybersecurity-act.
31. NIS Cooperation Group to formalna grupa współpracy Unii Europejskiej ds. bezpieczeństwa sieci i systemów informacyjnych, utworzona na mocy dyrektywy NIS (Network and Information Systems Directive). Jej głównym zadaniem jest koordynacja współpracy państw członkowskich UE w obszarze cyberbezpieczeństwa oraz wypracowywanie wspólnego podejścia do ochrony infrastruktury cyfrowej i krytycznej https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group.

BIBLIOGRAFIA

32. BSI. Quantum-safe cryptography – fundamentals, current developments and recommendations. 2021. [Accessed 31.01.2025]. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html.
33. ANSSI. ANSSI views on the Post-Quantum Cryptography transition. 2022. [Accessed 31.01.2025]. URL: https://cyber.gouv.fr/sites/default/files/document/EN_Position.pdf. oraz ANSSI. ANSSI views on the Post-Quantum Cryptography transition (2023 follow up). 2023. [Accessed 31.01.2025]. URL: https://cyber.gouv.fr/sites/default/files/document/follow_up_position_paper_on_post_quantum_cryptography.pdf.
34. AIVD. Informatieblad over quantumcomputers. 2014. [Accessed 31.01.2025].URL: https://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2014/11/20/informatieblad-over-quantumcomputers.
35. A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography Part 1, Version: 1.1, EU PQC Workstream, 11.06.2025, s. 2, 5, 7.
36. Opracowanie polskiej mapy drogowej jest wpisane w Strategię Cyberbezpieczeństwa przyjętą przez KPRM 10 marca 2026, str. 58, tabela, zadanie 3.2.1 https://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20260000309/O/M20260309.pdf .
37. Agreed Cryptographic Mechanisms v2.0 ECCG, Kwiecień 2025, https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
38. j.w. Note 40-Hybridization str. 29, Note 51-Hybridization, str. 33, Note 60-Hybridization, str. 36.
39. DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive (EU) 2022/2555, 20 styczeń 2026, COM(2026)13 Directive Proposal for simplification measures and alignment with the Cybersecurity Act , motyw 8, str. 8, oraz propozycja zmiany zapisu art 7(2) ppkt. k, str 12, https://digital-strategy.ec.europa.eu/pl/library/proposal-directive-regards-simplification-measures-and-alignment-cybersecurity-act.
40. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA) 14 grudnia 2022 r., https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022R2554.
41. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (eIDAS 2.0) https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32024R1183&qid=1779626333601.
42. Rozporządzenie w sprawie horyzontalnych wymogów cyberbezpieczeństwa dla produktów z elementami cyfrowymi (Cyber Resilience Act). https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32024R2847.
43. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO) art. 32 https://gdpr-text.com/pl/read/article-32/?col=1&lang1=pl&lang2=en&lang3=uk.
44. BSI. Quantum-safe cryptography – fundamentals, current developments and recommendations. 2021. [Accessed 31.01.2025]. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html.

BIBLIOGRAFIA

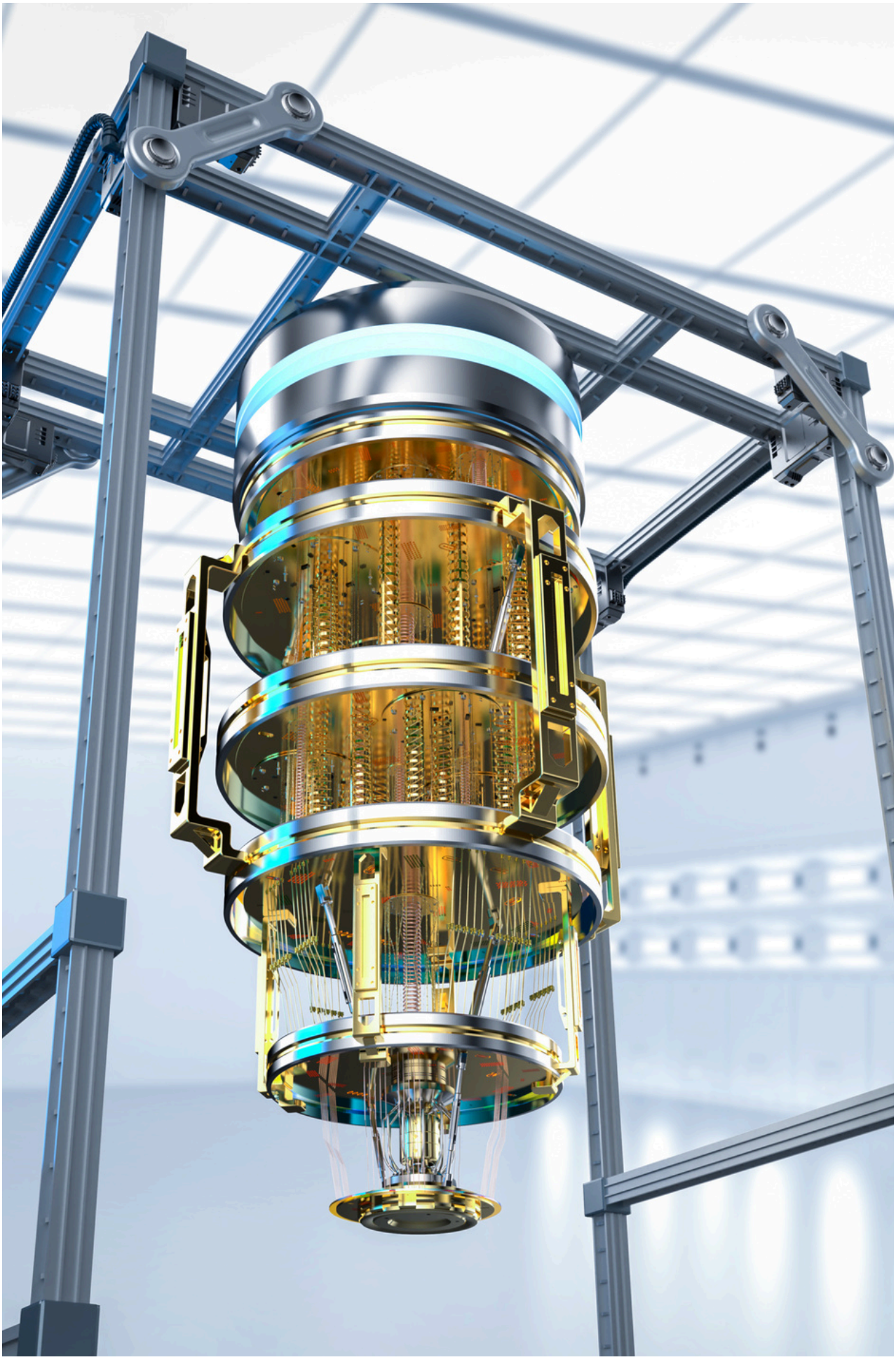
45. BSI TR-02102-1, wersja 2026-01, 23 stycznia 2026.
46. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Marktumfrage_EN_Kryptografie_Quantencomputing.
47. https://cyber.gouv.fr/nous-connaitre/publications/feuilles-de-route-de-la-securite-numerique-de-letat/feuille-de-route-de-securite-numerique-2026-2027/.
48. https://cyber.gouv.fr/enjeux-technologiques/cryptographie-post-quantique/faq-pqc/.
49. https://english.aivd.nl/documents/2024/12/3/the-pqc-migration-handbook.
50. https://english.rekenkamer.nl/documents/2026/02/04/focus-on-quantum-technology-in-central-government
51. https://espanadigital.gob.es/estrategia-de-tecnologias-cuanticas-de-espana
52. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej, Ministerstwo Cyfryzacji, przyjęto 10 marca 2026 r. https://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20260000309/O/M20260309.pdf.
53. J.w. Rozdział 7.2, Rozwój krajowej kryptologii, w tym migracja do kryptografii postkwantowej oraz rozwój technologii kwantowych, str. 28.
54. J.w. zadanie 3.2.1, str. 58.
55. https://www.gov.pl/web/cyfryzacja/rozwoj-technologii-kwantowych-w-polsce--zaktualizowane-zalozenia-polityki.
56. Jak wynika z „Check Point Security Report 2025", aż 1850 ataków tygodniowo kierowanych jest w Polsce wyłącznie w instytucje finansowe. https://www.bankier.pl/wiadomosc/Polska-bankowosc-2026-4-najwazniejsze-trendy-technologiczne-9065120.html; publikacja 8 stycznia 2026.
57. https://www.cmorg.org.uk/artefact/guidance-post-quantum-cryptography.
58. https://assets.publishing.service.gov.uk/media/6966149d8d599f4c09e1ffab/G7-CEG-Quantum-Roadmap.pdf.
59. https://www.ncsc.gov.uk/guidance/pqc-migration-timelines.
60. The Cross Market Operational Resilience Group (CMORG) to kluczowa brytyjska inicjatywa publiczno-prywatna, której zadaniem jest poprawa odporności operacyjnej i cyberbezpieczeństwa całego sektora finansowego. Stanowi ona strategiczne forum współpracy między instytucjami finansowymi, organami regulacyjnymi a władzami państwowymi.
61. https://www.cmorg.org.uk/artefact/guidance-post-quantum-cryptography.
62. https://assets.publishing.service.gov.uk/media/6966149d8d599f4c09e1ffab/G7-CEG-Quantum-Roadmap.pdf .
63. https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.
64. https://www.presidency.ucsb.edu/documents/memorandum-promoting-united-states-leadership-quantum-computing-while-mitigating-risks.
65. https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf.
66. https://www.congress.gov/bill/117th-congress/house-bill/7535/text.
67. https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf

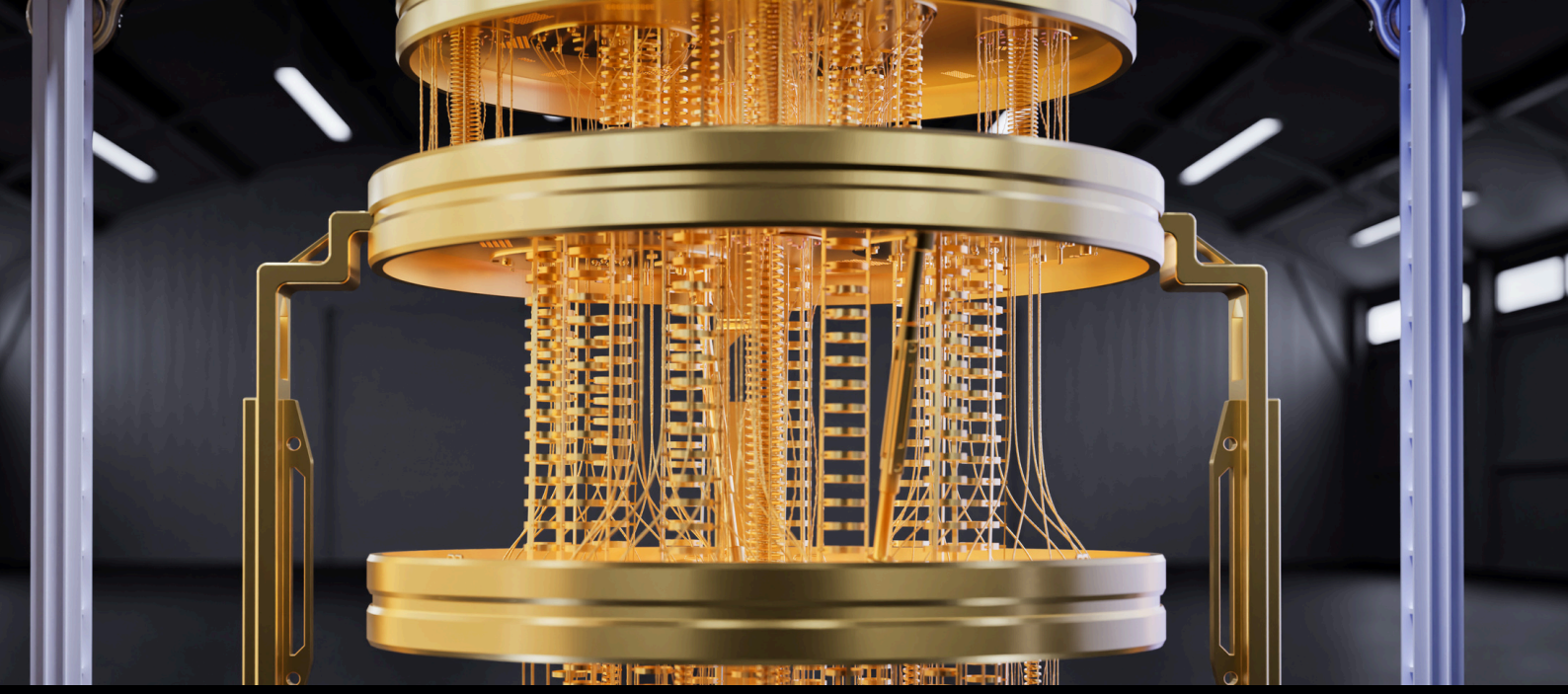
BIBLIOGRAFIA

68. https://csrc.nist.gov/publications/fips.
69. https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF.
70. China's Quantum Technology: The 15th Five-Year Plan's Push from Lab to Market, China Briefing, 26 lutego 2026, https://www.china-briefing.com/news/chinas-quantum-technology-15th-fyp-commercialization/.
71. Reuters, „China likely to have standards for post-quantum cryptography in 3 years, expert says", 19 marca 2026 r., https://www.reuters.com/world/asia-pacific/china-likely-have-standards-post-quantum-crytography-3-years-expert-says-2026-03-19/.
72. Cryptography Law of the People's Republic of China, tłum. China Law Translate27 października 2019 r. https://www.chinalawtranslate.com/en/cryptography-law/.
73. Institute of Commercial Cryptography Standards, Next-generation Commercial Cryptographic Algorithms Program (NGCC), 2 lutego 2025 r. https://www.niccs.org.cn/symmbzyjy/tzgg/pc/content/1937422988373135360/content_1937422988373135360.html.
74. Call for Proposals for the Next-generation Public-Key Cryptographic Algorithms, Institute of Commercial Cryptography Standards (ICCS), 9 października 2025, https://www.niccs.org.cn/niccs/Notice/pc/content/content_1975896137741635584.html.
75. Institute of Commercial Cryptography Standards of China, Submission Requirements for Cryptographic Hash Algorithms, sekcja 1 „ Notes for Algorithm Submitter(s)" pkt.5 , str. 1,: "*Considering algorithms innovation, technology diversity and intellectual property issues, NGCC will not accept the algorithms that are in or have finished the standardization process in international organizations, countries and regions, or related variants with insignificant modifications*."
76. npj Quantum Information, Implementation of carrier-grade quantum communication networks over 10000 km 8 sierpnia 2025, https://www.nature.com/articles/s41534-025-01089-8.
77. China Quantum, Deep dive: 2025 CAICT Quantum Reports State of quantum from China's leading government ICT think tank, Elias X. Huber, 8 lutego 2026 r., https://www.chinaquantum.info/p/deep-dive-2025-caict-quantum-reports.
78. https://www.csa.gov.sg/about-csa/who-we-are/.
79. CSA Releases A Quantum-Safe Handbook And Quantum Readiness Index, 22 października 2025, https://www.csa.gov.sg/news-events/press-releases/csa-releases-a-quantum-safe-handbook-and-quantum-readiness-index/.
80. https://nqsn.sg/.
81. National Institute of Information and Communications Technology (NICT), *Quantum Cryptography and Physical Layer Cryptography*, Online: nict.go.jp
82. Satellite-based QKD for Global Quantum Cryptographic Network Construction, https://ieeexplore.ieee.org/document/9749727.
83. Beginning Joint Verification Tests on Quantum Cryptography Technology to Enhance Cybersecurity in the Financial Sector, 21 grudnia 2020. https://www.global.toshiba/ww/technology/corporate/rdc/rd/topics/20/2012-04.html.

BIBLIOGRAFIA

84. CRYPTREC, Advisory Board for Cryptographic Technology FY 2025 Annual Report, 3.1.1, str.9, https://www.cryptrec.go.jp/report/cryptrec-rp-1000-2025.pdf.
85. *"QKD from a microsatellite: the SOTA experience",* https://arxiv.org/abs/1810.12405.
86. Israel National Cyber Directorate (INCD), Best Practices Organizational Cyber Readiness to the Post-Quantum Age, 2022, https://www.gov.il/BlobFolder/generalpage/quantum_computing/he/Best%20Practices%20-%20Organizational%20Cyber%20Readiness%20to%20the%20Post-Quantum%20Age%20v.1.85.pdf.
87. Banking System Preparedness for Cyber Risks Arising from Quantum Computing Capabilities, Bank of Israel, 7 stycznia 2025 r., https://boi.org.il/media/sm4f1ssu/202501en.pdf.
88. https://cyber.haifa.ac.il/quantum-cybersecurity/.
89. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/01/16/summary-of-natos-quantum-technologies-strategy.
90. j.w. art. 17.
91. https://www.nato.int/en/news-and-events/articles/news/2022/09/27/using-quantum-technologies-to-make-communications-secure.
92. https://assets.publishing.service.gov.uk/media/6966149d8d599f4c09e1ffab/G7-CEG-Quantum-Roadmap.pdf.





PAŃSTWOWY INSTYTUT BADAWCZY
Instytut Łączności

Projekt finansowany ze środków Ministerstwa Cyfryzacji. Publikacja wyraża jedynie poglądy autora/ów i nie może być utożsamiana z oficjalnym stanowiskiem Ministerstwa Cyfryzacji.

Projekt finansowany ze środków Ministerstwa Cyfryzacji