



# QT szansa czy zagrożenie ?



**QT wymaga poważnego traktowania i metodycznego podejścia**



Włodzimierz Nowak  
Gen.Bryg.(Rez.)



# Quantum Technologie

- **Komputery kwantowe i kryptografia kwantowa to dwie różne rzeczy.**
- Mają wspólny mianownik - w obu z nich używa się efektów kwantowych, żeby coś zrobić z informacją.
- **Komputery kwantowe** mają na celu przetwarzanie informacji w sposób bardziej efektywny.
- **Kwantowa kryptografia** jest odpowiedzią na zagrożenie jakie stwarzają komputery kwantowe.





# Zagrożenia

- Zmierzch rozwiązań bazujących na teorii wielkich liczb;
- Algorytm DES – złamany w 1997r.;
- Algorytm AES - 2015 ?;
- W roku 2025 algorytm klucza publicznego RSA zostanie złamany przez komputer kwantowy;
- Po 2025r. każdy klucz pseudolosowy będzie mógł być rozszyfrowany.



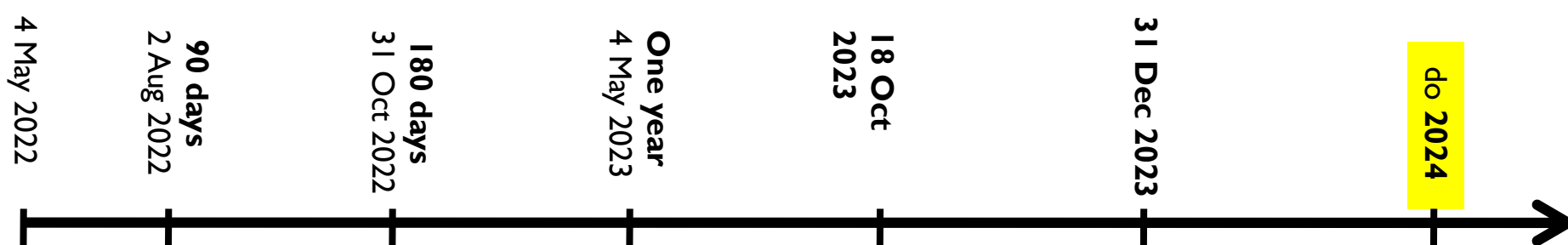


# Dlaczego nasze dane są zagrożone ?

Zaszyfrowana wiadomość z użyciem algorytmu RSA z 2048 bitowym kluczem:

- komputer konwencjonalny potrzebuje na rozszyfrowanie **300 mln lat**;
- komputer kwantowy zasilany 4099 kubitów będzie potrzebował na to **10 sekund**.





Memorandum

Plan Narodowej Strategii QIS (2.f)

Open WG (I)

Plan migracji do post quantum cryptography (II)

Pierwszy raport o ryzykach dla IK. Potem co roku (III)

Inwentaryzacja komercyjnych systemow krypto. (bez NSS) (IV)

Inwentaryzacja komercyjnych systemów IT (V)

NSA, wytyczne do migracji i implementacji syst. krypto odpornych na QC w NSS (X)

Szefowie NSS mają zidentyfikować wszystkie systemy podatne na QDekryptarz. (XI)

Pierwszy raport o migracji syst IT do „QC resist” (bez NSS) (VI)

Szefowie NSS wdrożą zabezpieczenia klucza symetrycznego (np. HAIPE) zapewniając dodatkowa ochronę syst. wymiany kluczy, za wyjątkiem „VPN symertic key solution”. (XIV)

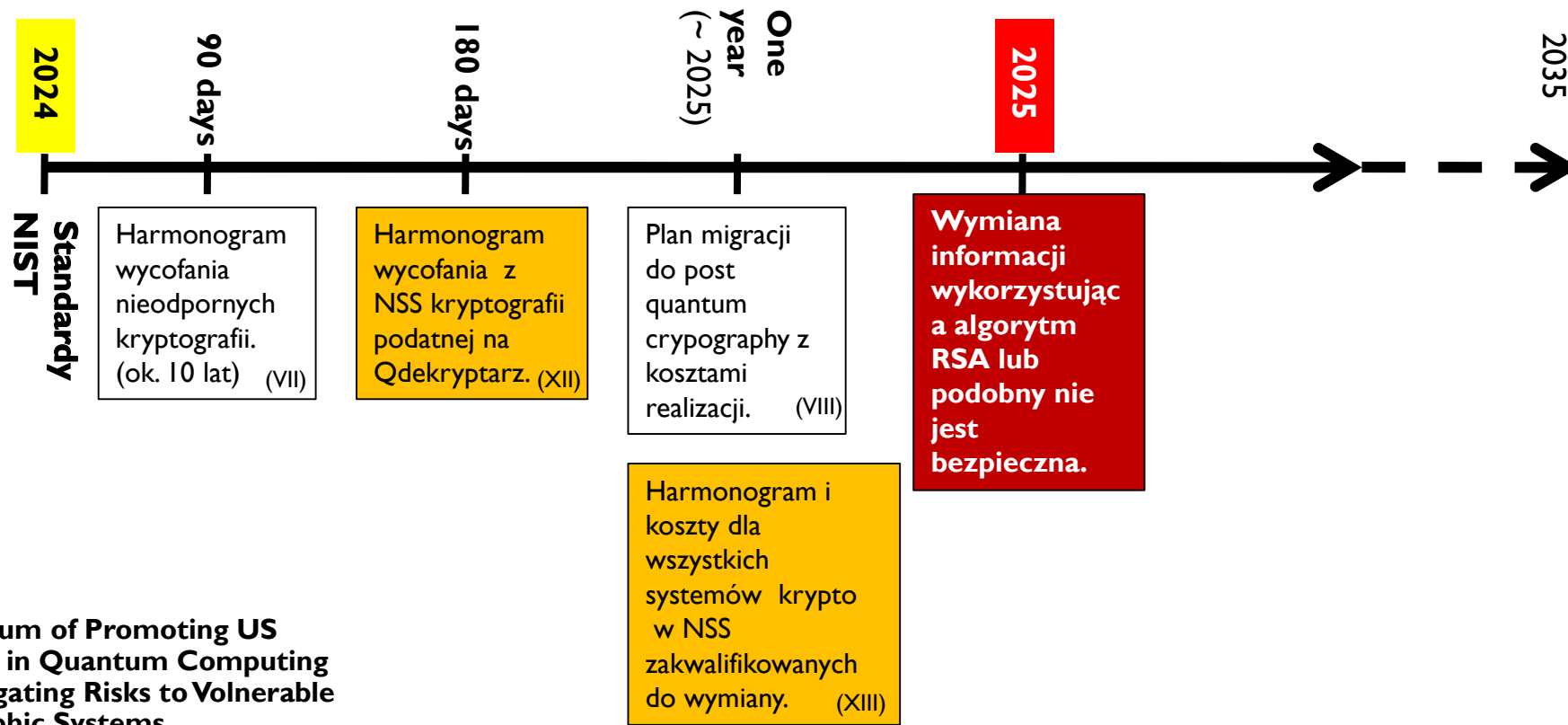
Sekr. Obrony dostarczy ocenę ryzyka dla bazy przemysłowej i łańcuchów dostaw. (XV)

**Standardy NIST dla crypografii odpornej na QC (3.a)**

**Do czasu wydania standardów NIST, Agencje nie będą kupowały komercyjnych rozwiązań krypto, ale mogą je testować. (IX)**

**Memorandum of Promoting US Leadership in Quantum Computing While Mitigating Risks to Volnerable Cryptographic Systems**





**Memorandum of Promoting US Leadership in Quantum Computing While Mitigating Risks to Volnerable Cryptographic Systems**



Dziękuję za uwagę

