URZĄD OCHRONY DANYCH OSOBOWYCH

KPRM
KANCELARIA PREZESA RADY MINISTRÓW

QT szansa czy zagrożenie ?

QT wymaga poważnego traktowania i metodycznego podejścia

Włodzimierz Nowak
Gen.Bryg.(Rez.)

AI LAW TECH

GRAI

URZĄD OCHRONY DANYCH OSOBOWYCH

KPRM
KANCELARIA PREZESA RADY MINISTRÓW

Quantum Technologie

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

AI LAW TECH

GRAI

URZĄD OCHRONY DANYCH OSOBOWYCH

KPRM
KANCELARIA PREZESA RADY MINISTRÓW

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.

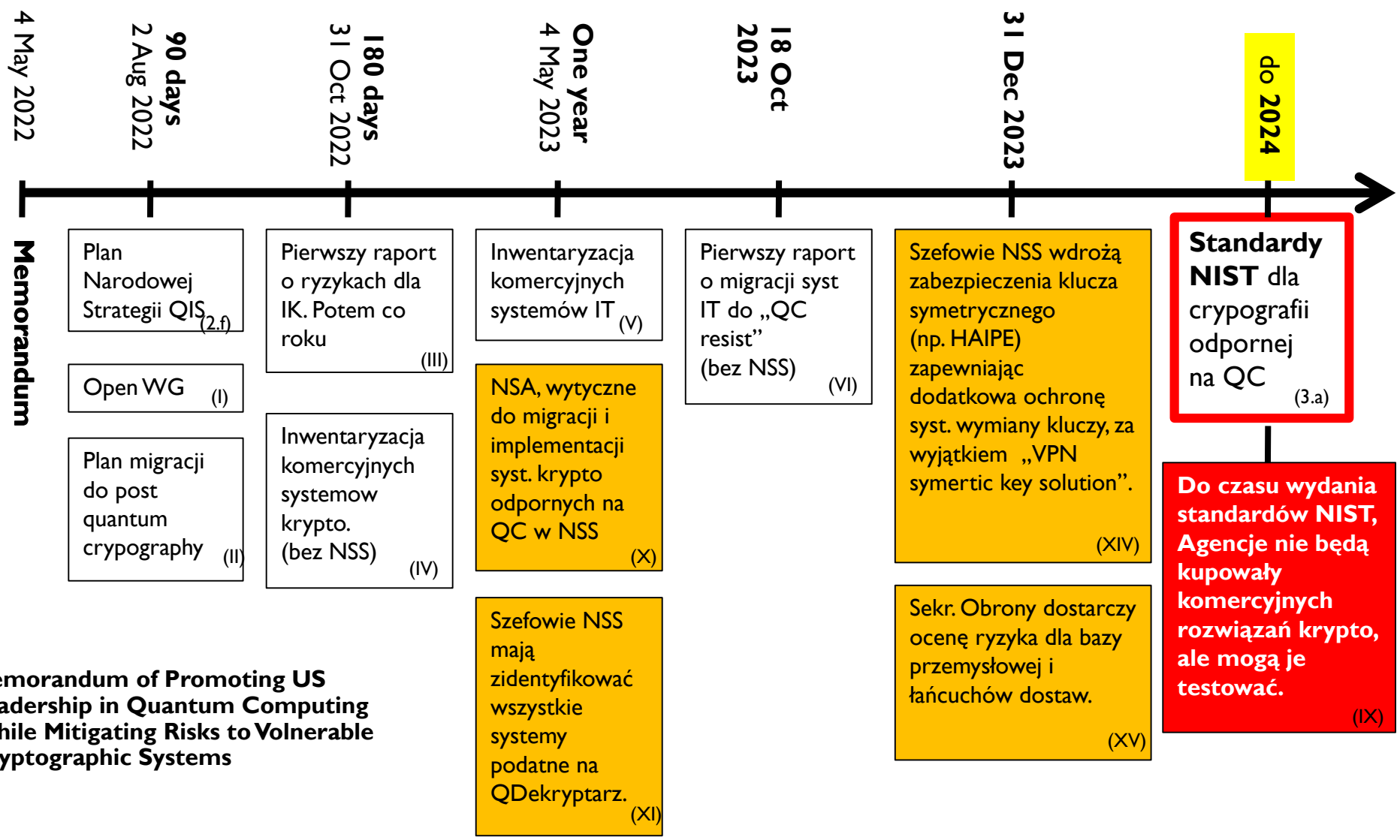
AI LAW TECH

GRAI

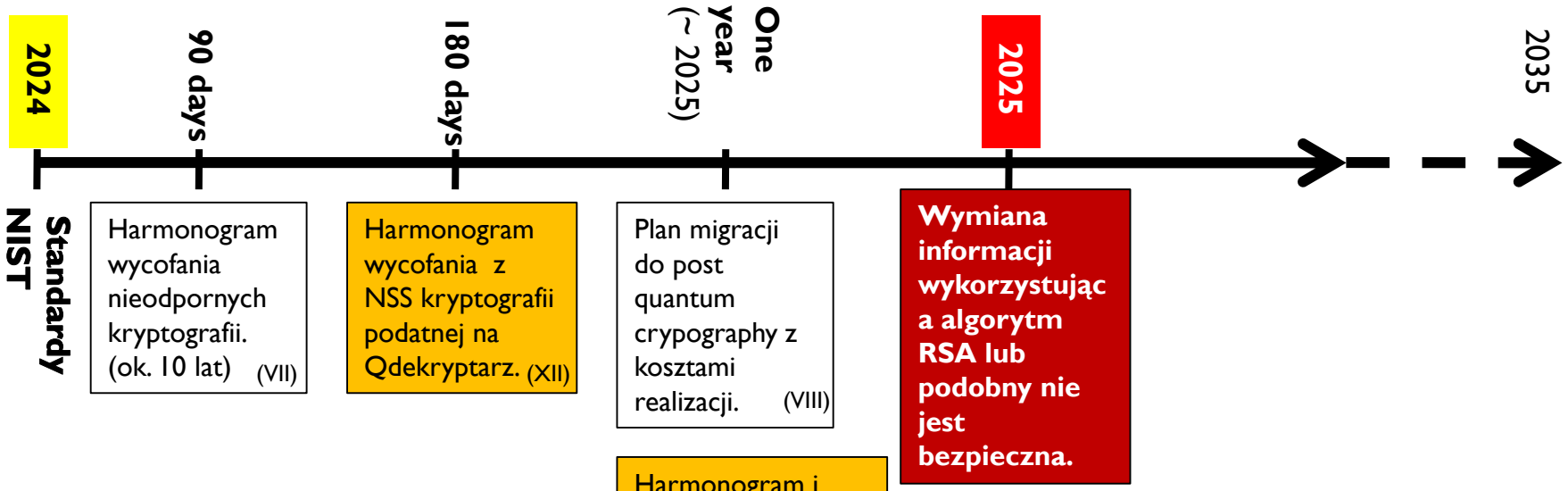
Dlaczego nasze dane są zagrożone ?

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 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

URZĄD OCHRONY DANYCH OSOBOWYCH

KPRM
KANCELARIA PREZESA RADY MINISTRÓW
THE CHANCELLERY OF THE PRIME MINISTER

Dziękuję za uwagę

AI LAW TECH

GRAI