Plany Ministerstwa Cyfryzacji w zakresie prewencji i zwalczania przestępczości

gen. bryg. Włodzimierz Nowak

Pełnomocnik Ministra Cyfryzacji ds. Cyberbezpieczeństwa

Ministerstwo Cyfryzacji

Agenda

1. Plany Ministerstwa Cyfryzacji w zakresie cyberbezpieczeństwa
2. Działania w zakresie architektury systemu bezpieczeństwa
3. Organizacja systemu bezpieczeństwa
4. Szkolenia

Ministerstwo
Cyfryzacji

Plany Ministerstwa Cyfryzacji w zakresie cyberbezpieczeństwa

- Strategia Cyberbezpieczeństwa RP
- Ustawa o krajowym systemie cyberbezpieczeństwa

Ministerstwo Cyfryzacji

Plany w zakresie cyberbezpieczeństwa

Strategia

- Uwarunkowania: otoczenie międzynarodowe i krajowa;
- Główne założenia strategii;
- Zakres i cele, mierniki osiągnięcia celów;
  - Zakres Strategii i Cel główny
  - Cele szczegółowe
    - zapewnienie nieprzerwanej realizacji krytycznych funkcji Państwa
    - zapewnienie nieprzerwanego świadczenia usług kluczowych
    - zapewnienie osobistego bezpieczeństwa obywateli w cyberprzestrzeni
- Struktury organizacyjne niezbędne do osiągnięcia celu Strategii

Plany w zakresie cyberbezpieczeństwa

Strategia

- **Ludzie – Technologie – Procesy i Procedury**
  - Ludzie (kierownictwo, personel IT, użytkownicy instytucjonalni, obywatele)
  - Technologie (bezpieczeństwo „zaszyte” w architekturze, minimalne wymagania techniczne (normy i standardy techniczne, uznane praktyki))
  - Procesy i Procedury (zarządzanie bezpieczeństwem w oparciu o uznane normy krajowe i międzynarodowe, krajowy system monitorowania ryzyka, wzajemne powiadamianie i ostrzeganie, eskalacja reagowania);
- **Prace badawcze i rozwojowe** – *wsparcie ze strony środowisk naukowo - akademickich;*
- **Współpraca międzynarodowa;**
- **Finansowanie** (budżet państwa, budżety jednostek samorządu terytorialnego, partnerstwo publiczno – prywatne);
- **Przygotowanie do nowych wyzwań-** IPv6, Smart City, Industry 6.0.

Plany w zakresie cyberbezpieczeństwa

Ustawa o krajowym systemie cyberbezpieczeństwa

- Implementacja dyrektywy NIS
- Ustawa ma objąć swoim działaniem administrację rządową, samorządową oraz państwową
- Ustawa ma objąć swoim działaniem teleinformatyczną infrastrukturę krytyczną

Działania w zakresie architektury systemu bezpieczeństwa

System wczesnego ostrzegania

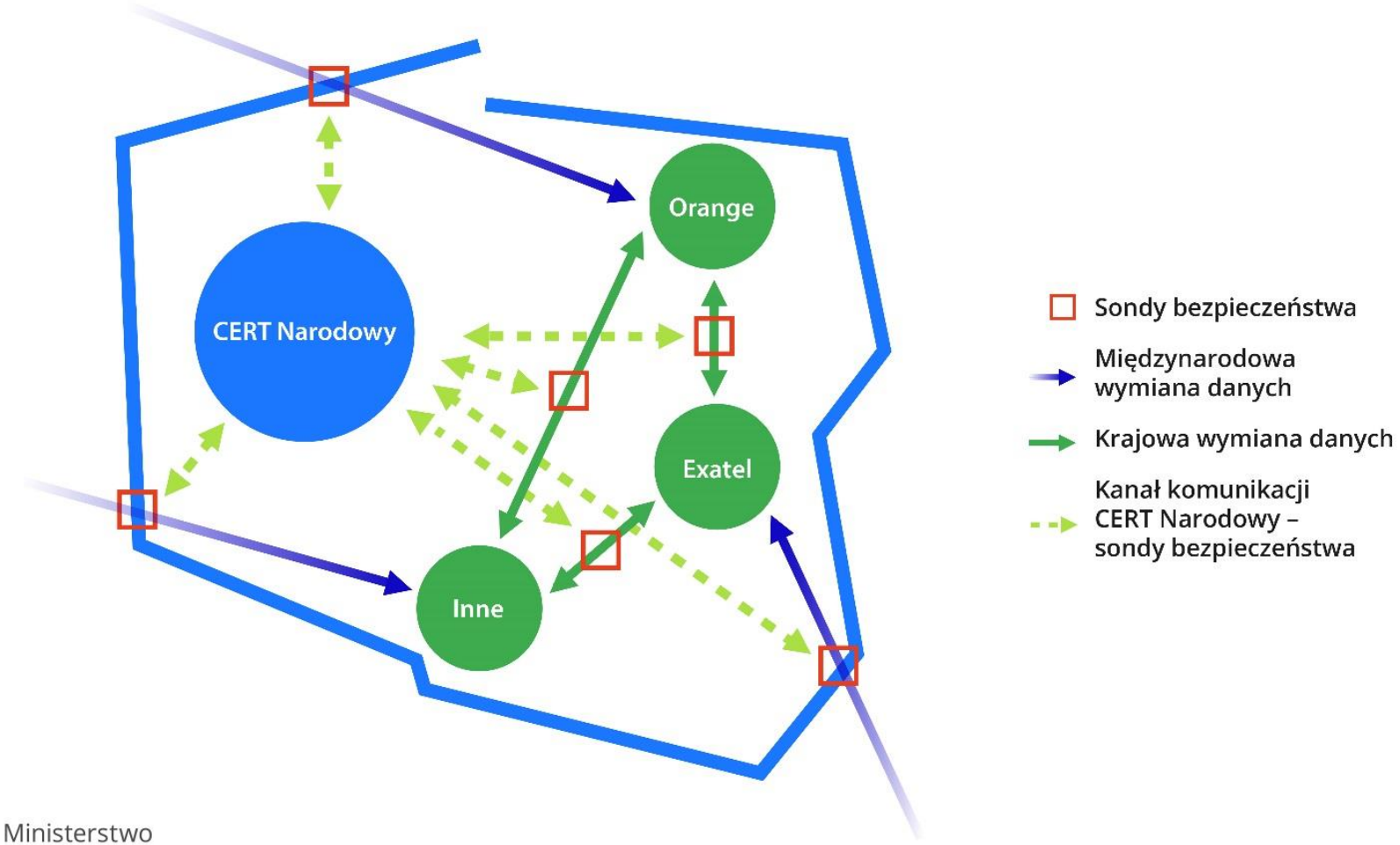
Klastry bezpieczeństwa i bezpośrednia ochrona danych

Bezpieczeństwo danych

Ministerstwo Cyfryzacji

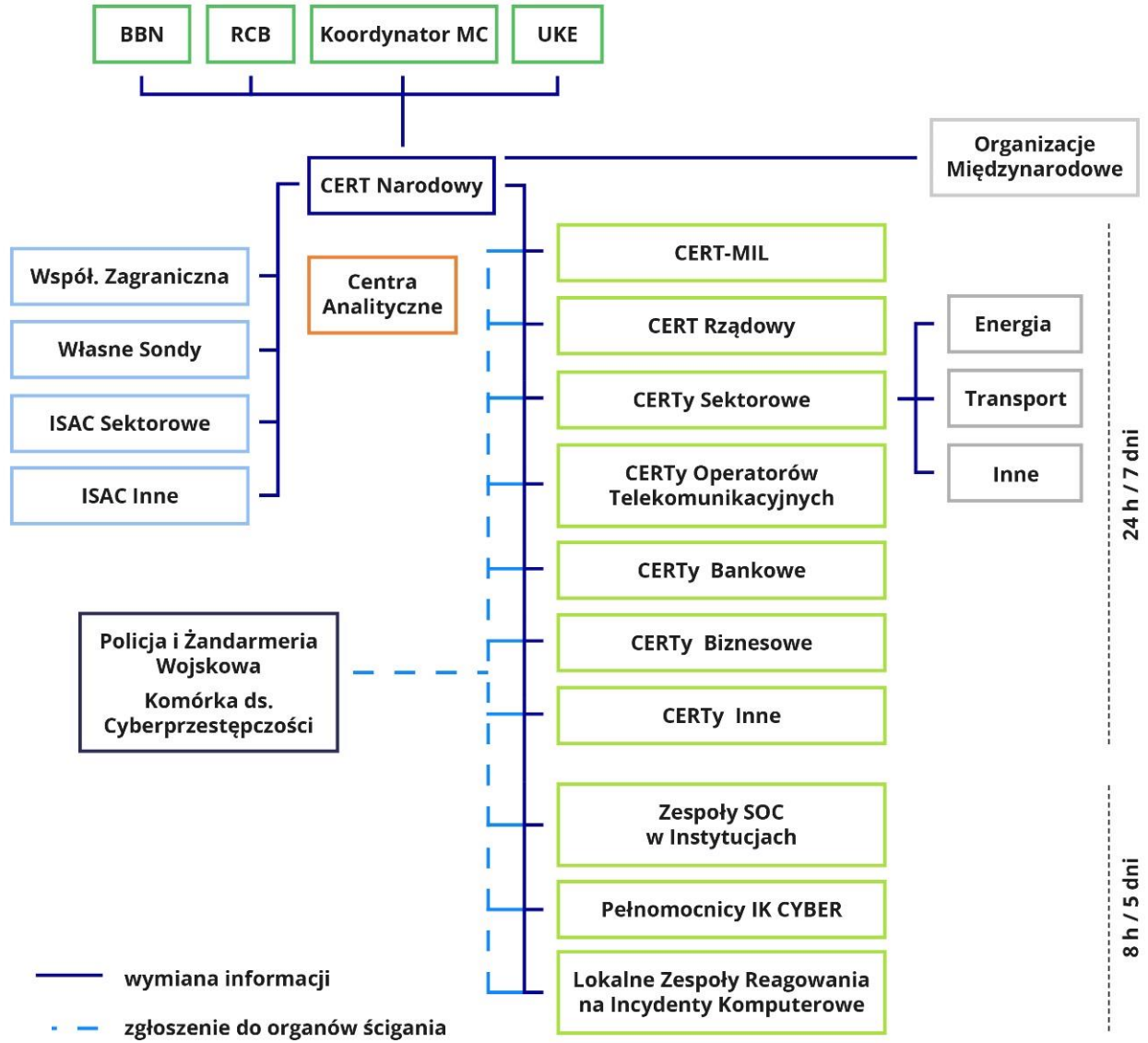
Działania w zakresie architektury systemu bezpieczeństwa

System wczesnego ostrzegania



Ministerstwo Cyfryzacji

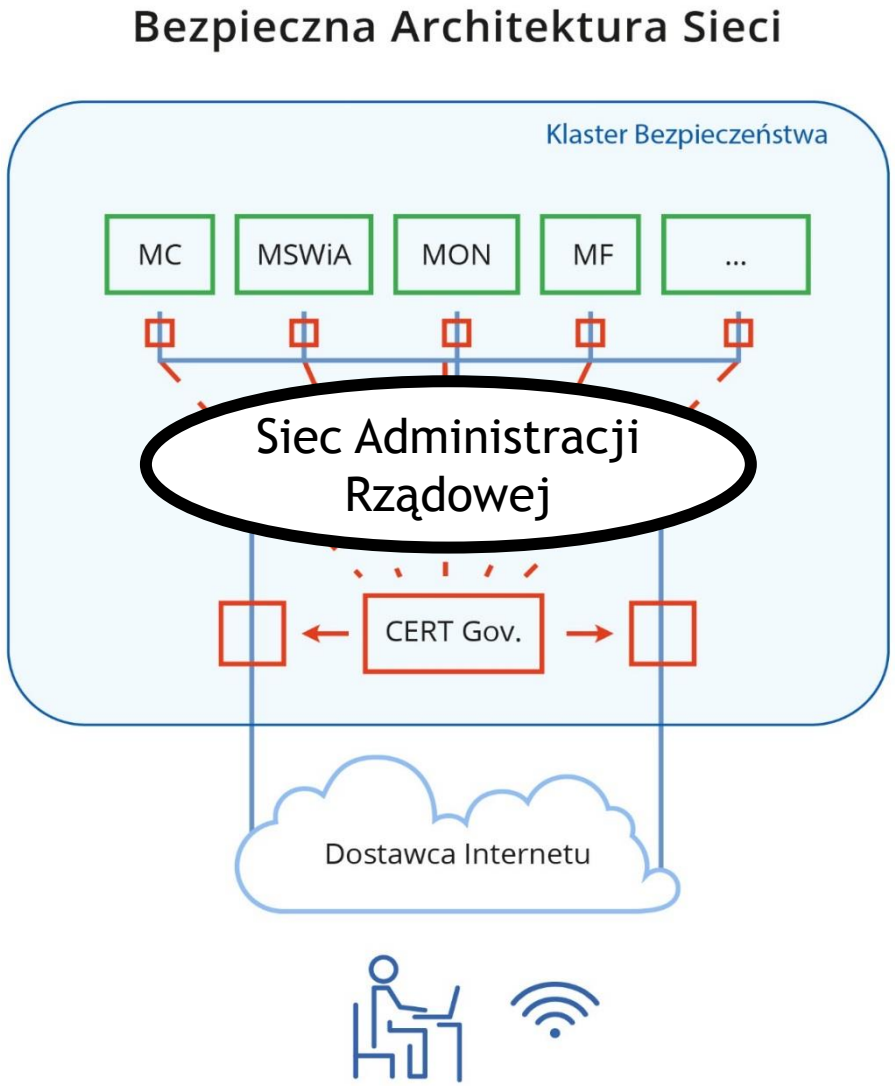
Działania w zakresie architektury systemu bezpieczeństwa



Ministerstwo Cyfryzacji

Działania w zakresie architektury systemu bezpieczeństwa

Klastry bezpieczeństwa i bezpośrednia ochrona danych



Ministerstwo Cyfryzacji

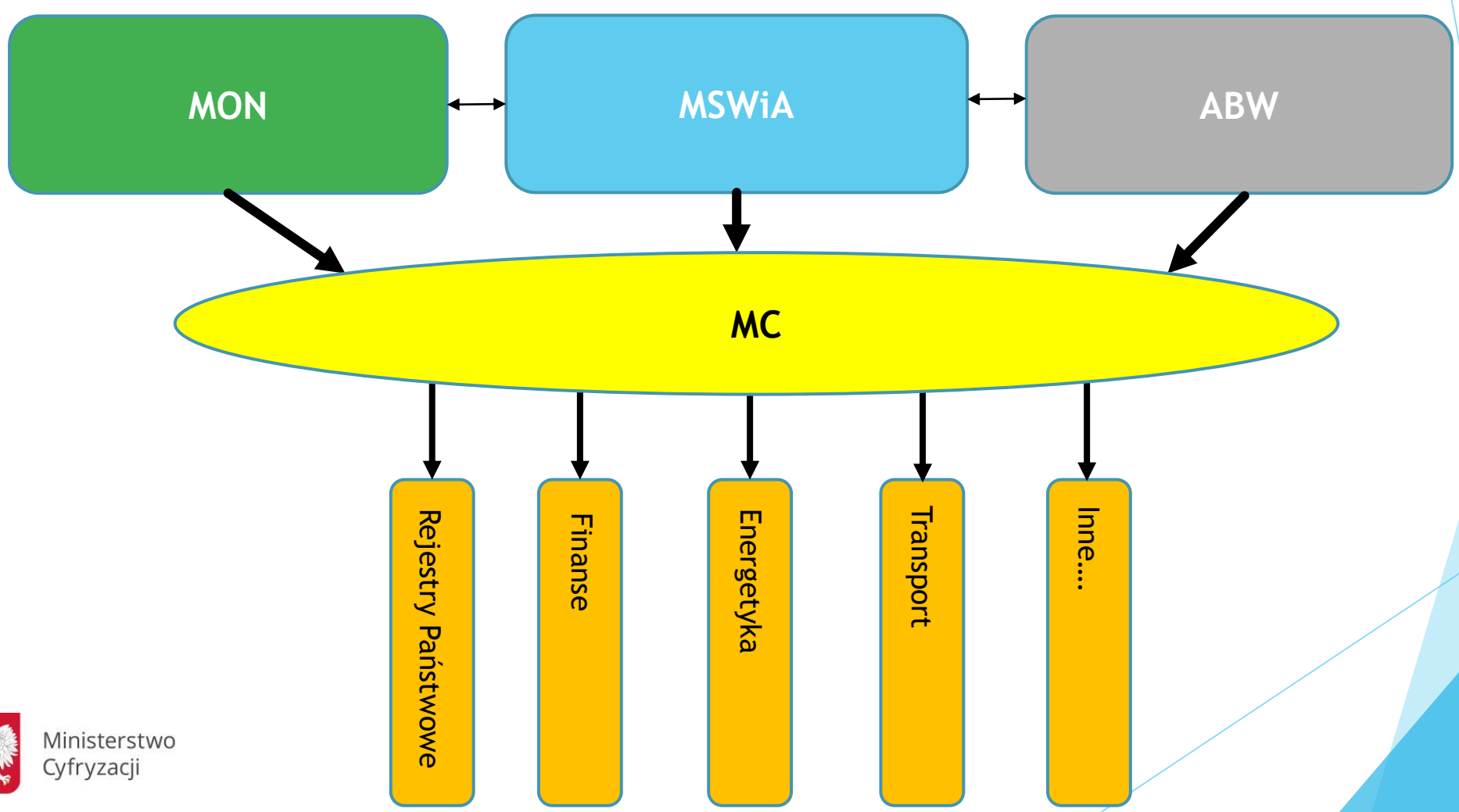
Organizacja systemu bezpieczeństwa

Zdolność do przeciwdziałania i zwalczania zagrożeń w cyberprzestrzeni

Ministerstwo Cyfryzacji

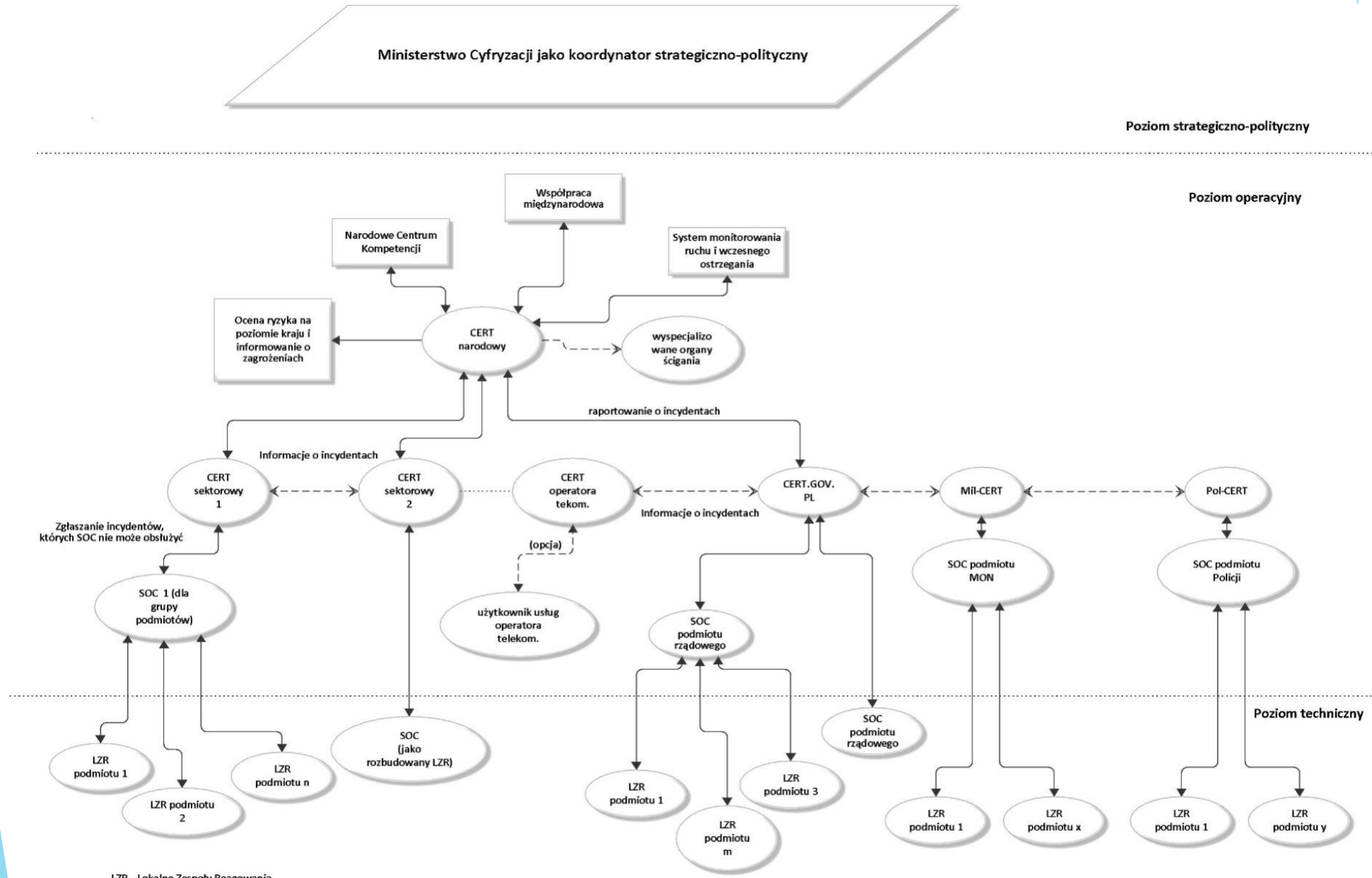
Organizacja systemu cyberbezpieczeństwa

Podział kompetencji i współpraca służb



Ministerstwo Cyfryzacji

Organizacja systemu bezpieczeństwa



LZR-- Lokalne Zespoły Reagowania
SOC - Operacyjne Centrum Bezpieczeństwa

Szkolenia

Szkolenia

- Cel uruchomienia programu szkoleń
- Przewidywane korzyści
- Poziomy szkolenia
- Jednostki przewidywane do objęcia programem
- Forma i zakres
- Czasokres realizacji

Szkolenia

- Prokuratorzy
- Sędziowie
- Policjanci
- Projektanci systemów informatycznych – uczelnia
- Administratorzy systemów – uczelnia
- Administratorzy treści – kursy
- Użytkownicy – dostawcy serwisów informacyjnych
- e-learning

Dziękuję za uwagę

cyber@mc.gov.pl