KURS SPECJALISTA CYBERBEZPIECZEŃSTWA

Spis treści

1. Wprowadzenie – sieć komputerowa

Aby mówić o bezpieczeństwie w cyberprzestrzeni konieczne jest zapoznanie się z definicją sieci komputerowych:

Sieć komputerowa

- wg. Akademii Sieci Cisco - jest to system wzajemnie ze sobą powiązanych stacji roboczych, urządzeń preferencyjnych i innych
- jest to połączenie przynajmniej 2 komputerów w celu wymiany danych; urządzenia za pomocą mediów transmisyjnych komunikują się ze sobą, w tym celu wykorzystują odpowiednie protokoły komunikacyjne

Współcześnie należałoby rozszerzyć definicję sieci, ponieważ wzrosła liczba urządzeń, które są podłączane do sieci lub korzystają z niej. Oprócz komputerów czy serwerów do sieci komputerowych podłącza się:

- ✓ telefony komórkowe
- ✓ tablety
- ✓ sprzęt AGD – pralki, lodówki, piekarniki, itp.

Sama podstawa działania sieci komputerowej nie uległa zmianie, ponieważ w dalszym ciągu głównym jej zadaniem jest udostępnianie:

Zmieniła się jedynie liczba i zakres urządzeń z niej korzystających.

Słownik pojęć

HOST

- jest urządzeniem końcowym sieci komputerowej, stanowiącym źródło lub cel przesyłania danych w sieci – każde urządzenie, któremu w sieci przypisany został adres IP

SERWER

- główny komputer, na którym zostały zainstalowane specjalistyczne oprogramowania, oferujące usługi innym urządzeniom/komputerom – www, zasoby plikowe, poczta

KLIENT

- każdy komputer, który korzysta z usług udostępnianych przez serwer

KLIENT – SERWER

- relacja/architektura sieci komputerowej, w której znajduje się komputer pełniący funkcję serwera oraz komputer korzystający z usług (klient)

P2P – Peer to Peer

- komputery działające w sieci są na równi – w architekturze sieci komputerowej nie występuje jeden, główny komputer udostępniający usługi – serwer

MEDIUM TRANSMISYJNE

- jest to element sieci komputerowej, dzięki któremu możliwe jest wzajemne komunikowanie się urządzeń – rolę tę może pełnić miedziany kabel, światłowody, WiFi

PROTOKÓŁ KOMUNIKACYJNY

- określony język/sposób komunikacji umożliwiający wymianę danych między urządzeniami w sieci

LAN

- lokalna sieć komputerowa, która może obejmować swoim zasięgiem pewien obszar – pomieszczenie, piętro, budynek, itp.

MAN

- miejska sieć komputerowa

WAN

- rozległa sieć komputerowa, której zadaniem jest umożliwienie komunikacji pomiędzy odległymi sieciami LAN

TOPOLOGIA FIZYCZNA SIECI

- określa, w jaki sposób połączone zostały ze sobą komputery w sieci

TOPOLOGIA LOGICZNA SIECI

- określa, w jaki sposób komunikują się ze sobą komputery w sieci

KARTA SIECIOWA

- adapter, który instaluje się w urządzeniu w celu umożliwienia łączenia się danego urządzenia z siecią komputerową

ROUTER

- jest to urządzenie sieciowe mające na celu łączenie ze sobą różnych sieci aby mogły się ze sobą wzajemnie komunikować; dodatkowo - na podstawie adresu IP
- określa ścieżki przepływu danych pomiędzy sieciami

PRZEŁĄCZNIK

- jest urządzeniem sieciowym, które łączy urządzenia w danej sieci lokalnej, decyduje również o przesyle danych (na podstawie adresu MAC) pomiędzy urządzeniami

ADRES IP

- jest to logiczny adres interfejsu danego urządzenia podłączonego do sieci komputerowej

ADRES MAC

- sprzętowy/fizyczny adres karty sieciowej urządzenia, który jest nadawany przez producenta na etapie produkcji

INTERNET

- siatka, która łączy w sobie sieci rozległe

INTRANET

- jest to rodzaj prywatnej sieci, która wykorzystuje w komunikacji takie standardy, jakie występują w sieci Internet – www, FTP, POP3 czy SMTP – mają do nich dostęp tylko upoważnieni użytkownicy

EXTRANET

- forma rozszerzonej sieci prywatnej, do której zasobów mają dostęp także inni użytkownicy

VPN

- sieć o charakterze prywatnym, do której można się dostać przez sieć Internet – poprzez tzw. tunelowy kanał transmisji danych

DNS

- system zmieniający nazwę mnemoniczną na odpowiadający jej adres IP w sieci

2. Cyberprzestrzeń

Definicja cyberprzestrzeni w różnym ujęciu

Po raz pierwszy z tym terminem można było się spotkać w roku 1984 czytając powieść „Burning Chrome" W. Gibsona.

Autor zdefiniował ją jako:

- **stworzony przez komputer świat wirtualnej, immersyjnej rzeczywistości, zwanej także matrycą**

Rozpowszechnienie pojęcia cyberprzestrzeni wiązało się również z rozwojem i ogólnym dostępem do Internetu, lecz także poprzez różnego rodzaju filmy typu „Matrix".

We współczesnym świecie cyberprzestrzeń rozumie się jako:

- **przestrzeń otwartej komunikacji odbywającej się za pomocą połączonych ze sobą komputerów oraz pamięci informatycznych na całym świecie.**

W ujęciu humanistycznym cyberprzestrzeń uważana jest za synonim Internetu.

P. Levy scharakteryzował cyberprzestrzeń jako:

- **plastyczną**
- **płynną**
- **obliczalną (z dużą dokładnością)**
- **przetwarzalną w rzeczywistym czasie**
- **hipertekstualną**
- **interaktywną**
- **wirtualną**

Jest środowiskiem, które umożliwia współdziałanie wszystkich narzędzi, które tworzą informację, rejestrację, komunikację oraz symulację. Jest ona jednym z głównych kanałów informacji, przekazu i nośników pamięci ludzkiej.

W literaturze czy sztuce cyberprzestrzeń rozumiana jest jako przestrzeń:

- **Internetu**
- **artystycznej działalności w sieci**
- **żywych oraz możliwych dzięki komunikacji online sieci społecznych**

Krytycy nowych mediów mówią o dziele w cyberprzestrzeni – tj. uważają ją za przestrzeń do publikowania, wystawiania dzieł – a także o dziele, które wykorzystuje jej język, jego numeryczny charakter. ***W takim ujęciu można także spotkać się z cyberprzestrzennym sposobem prezentowania dzieła*** – dane, jakie składają się na utwór są prezentowane w wizualnej/przestrzennej formie.

Najbardziej popularna definicja cyberprzestrzeni została stworzona przez Departament Obrony USA, wg. której to jest ona:

- globalną domeną środowiska informacyjnego, która składa się ze współzależnych sieci stworzonych przez infrastrukturę IT oraz zawartych w nich danych – w tym Internet, sieci telekomunikacyjne, systemy komputerowe (wraz z procesorami czy kontrolerami).

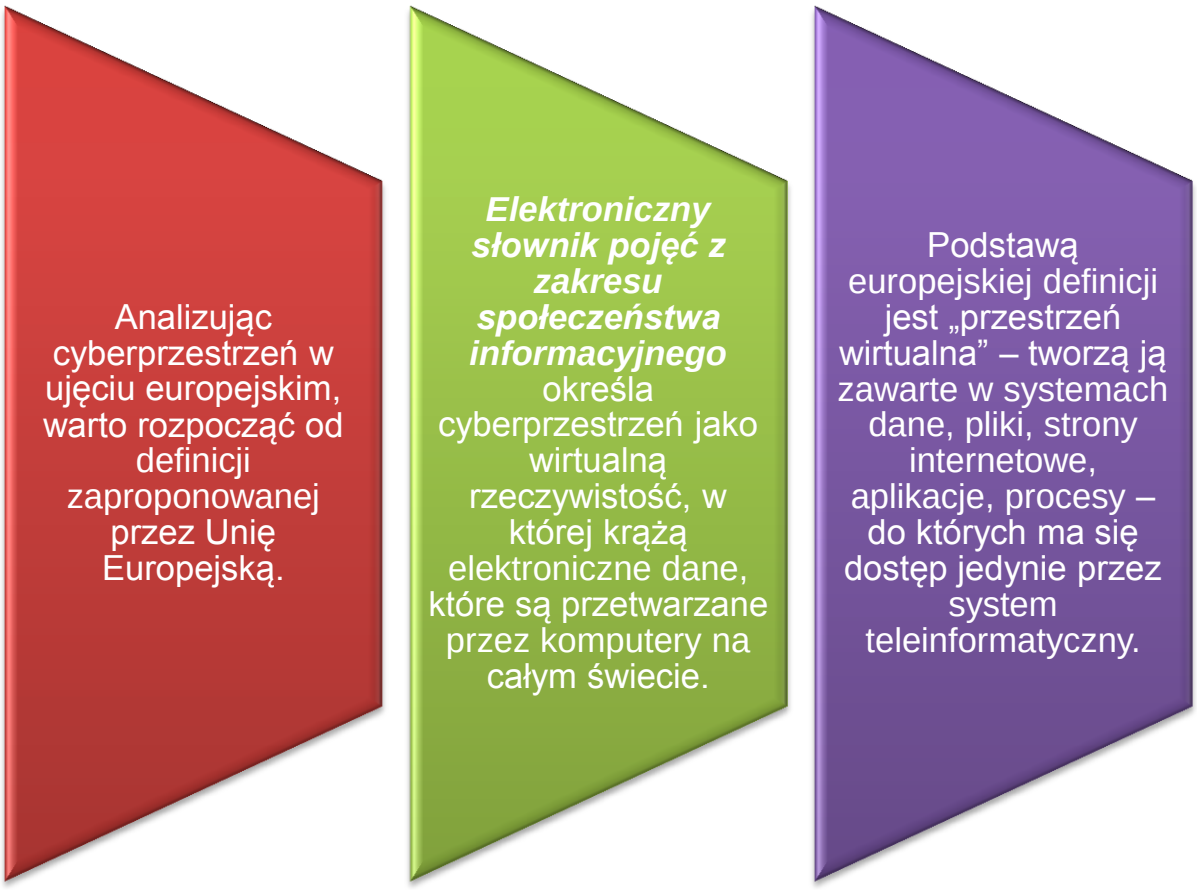
Warto zwrócić uwagę, że tym ujęciu cyberprzestrzeni, brak jest jakichkolwiek odwoływań do jej społecznych aspektów, czy też do ludzi, jako jej użytkowników. Definicja skupia się na technologicznym fundamencie cyberprzestrzeni.

Poniższy cytat pochodzący z „Narodowej Strategii dla Bezpiecznej Cyberprzestrzeni" – oryg. *National Strategy to Secure Cyberspace* mówi, że:

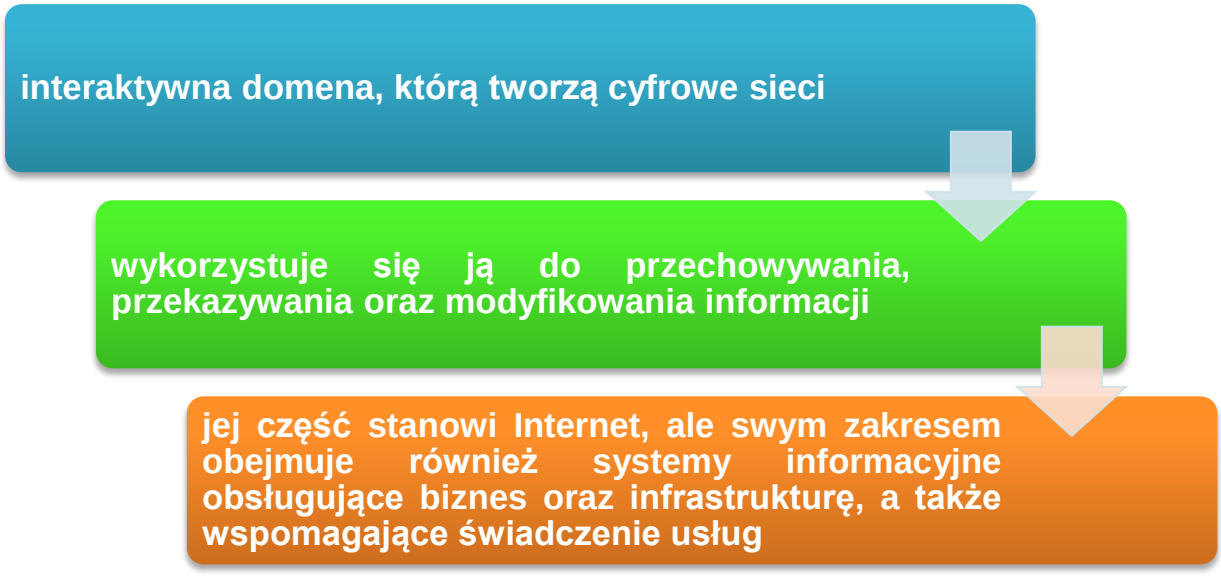
"Nasza Krajowa infrastruktura krytyczna jest budowana przez publiczne, jak i prywatne instytucje funkcjonujące w sektorach rolnym, żywieniowym, zaopatrzenia w wodę, służby zdrowia, usług ratunkowych, rządowym, obronnym, przemysłowym, informacyjnym oraz telekomunikacyjnym, energetycznym, transportowym, bankowym oraz finansowym, chemicznym oraz materiałów niebezpiecznych, a także pocztowym oraz dostawczym. Cyberprzestrzeń stanowi ich układ nerwowy – system kontrolny naszego kraju. Cyberprzestrzeń jest zbudowana z setek tysięcy połączonych komputerów, serwerów, routerów, switchy oraz światłowodów, które umożliwiają pracę naszej infrastrukturze krytycznej. Stąd też zdrowe funkcjonowanie cyberprzestrzeni jest kluczowe dla naszej ekonomii oraz bezpieczeństwa narodowego".

Takie ujęcie cyberprzestrzeni pokazuje jak rozległa jest to infrastruktura, a także z jak wielu utworzona jest elementów, które połączone są z krajową infrastrukturą krytyczną. Ukazuje również aspekt ekonomiczny oraz społeczny. USA pokazują, że cyberprzestrzeń – traktowana jako nowoczesny i zautomatyzowany obszar natychmiastowej wymiany informacji – jest jednym z

najważniejszych ośrodków krajowej działalności gospodarczej. Przykład – brak funkcjonowania w sieci/Internecie świadczy o ograniczonym udziale w nowoczesnej gospodarce.



Wg. „Strategii Cyberbezpieczeństwa Zjednoczonego Królestwa – ochrona oraz promocja Zjednoczonego Królestwa w cyfrowym świecie" cyberprzestrzenią jest:



Współcześnie sieci cyfrowe są wykorzystywane do zaopatrywania domów w wodę, czy energię, wspomagają dostawę żywności bądź odbiór zakupów ze sklepów, są narzędziem biznesowym, a ich zasięg stale się powiększa.

W takim ujęciu cyberprzestrzeń jest połączeniem Internetu z innymi sieciami – niekoniecznie tymi globalnymi. W brytyjskiej definicji mamy do czynienia z nowym pojęciem – tj. interaktywnością.

W odróżnieniu do Wielkiej Brytanii Niemcy – w swojej „Strategii Cyberbezpieczeństwa dla Niemiec" określają cyberprzestrzeń jako:

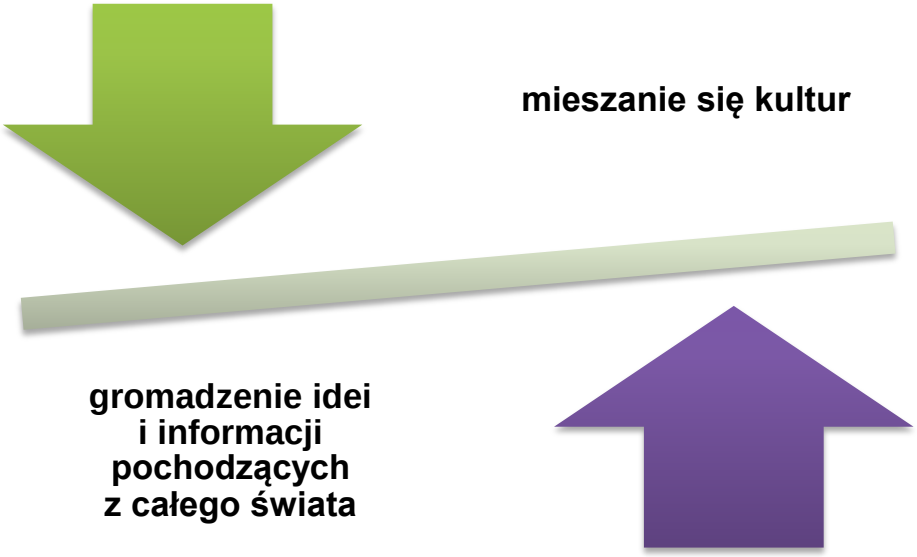
- wirtualną przestrzeń wszelkich systemów technologii informacyjnej, które są powiązane na poziomie danych w globalnej skali
- fundamentem cyberprzestrzeni jest Internet – będący uniwersalną i powszechnie dostępną siecią, która oferuje połączenia oraz transport, a także może być rozszerzana czy też uzupełniana przez kolejne, dowolne ilości dodatkowych sieci danych
- systemy IT, które działają w wyizolowanej, wirtualnej przestrzeni nie są częścią cyberprzestrzeni

„Obrona oraz bezpieczeństwo systemów informacyjnych. Strategia dla Francji" – dokument przygotowany przez francuską Agencję Bezpieczeństwa Sieci oraz informacji – ukazuje cyberprzestrzeń jako:

- ***przestrzeń komunikacyjną, którą utworzono przez globalne połączenia sprzętu mającego za zadanie automatycznie przetwarzać cyfrowe dane.***

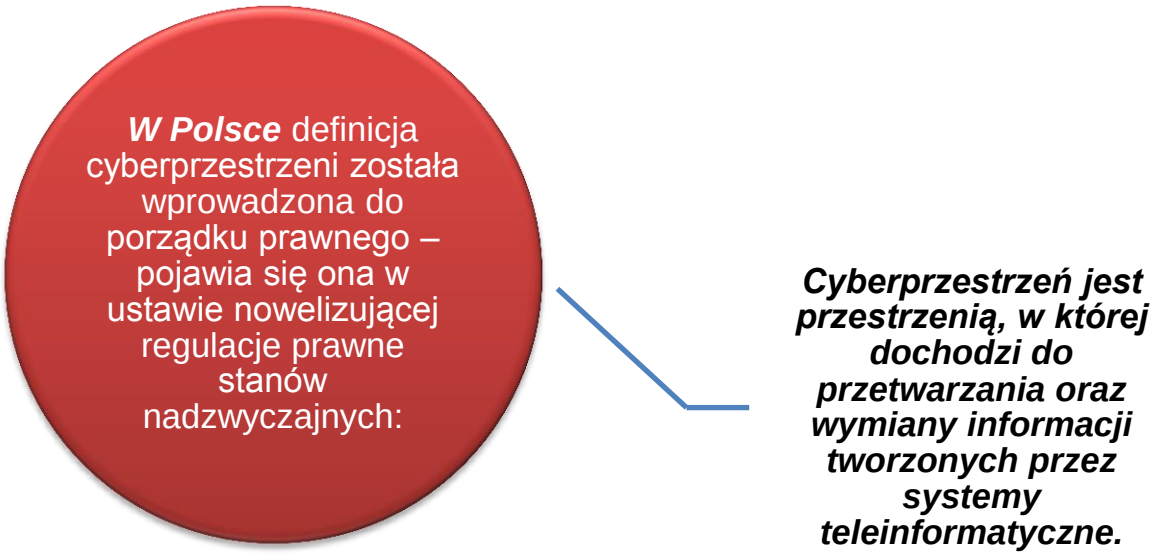
Warto zwrócić uwagę na fakt, że we francuskiej definicji brak jest bezpośredniego nawiązania do użytkowników bądź też zjawisk ekonomicznych i społecznych. Cyberprzestrzeń w całościowym ujęciu jest traktowana jako obszar komunikacji opierającej się na infrastrukturze istniejącej na całym świecie. ***Dodatkowo, w socjologicznym ujęciu, cyberprzestrzeń jest tratowana jako obszar komunikacji o światowym zasięgu i nazywa się ją „Nową Wieżą Babel".***

To właśnie dzięki cyberprzestrzeni możliwe jest:



O tym, jak ogromne jest znaczenie cyberprzestrzeni do tego, by uczestniczyć w nowoczesnej społeczności, świadczy stwierdzenie, że wyłączając się z niej doprowadza się do:

W strategii francuskiej możemy się spotkać z jeszcze jednym ciekawym określeniem cyberprzestrzeni, jest nim ***Nowe Termopile***. W materialnym świecie dochodzi do niewidocznych starć, które zaburzają poprawne funkcjonowanie systemów oraz naruszają dobra prawne użytkowników, ale także mogą zagrozić nawet ich życiu, np. jeśli zaatakowane zostaną systemy odpowiedzialne za bezpieczeństwo publiczne.



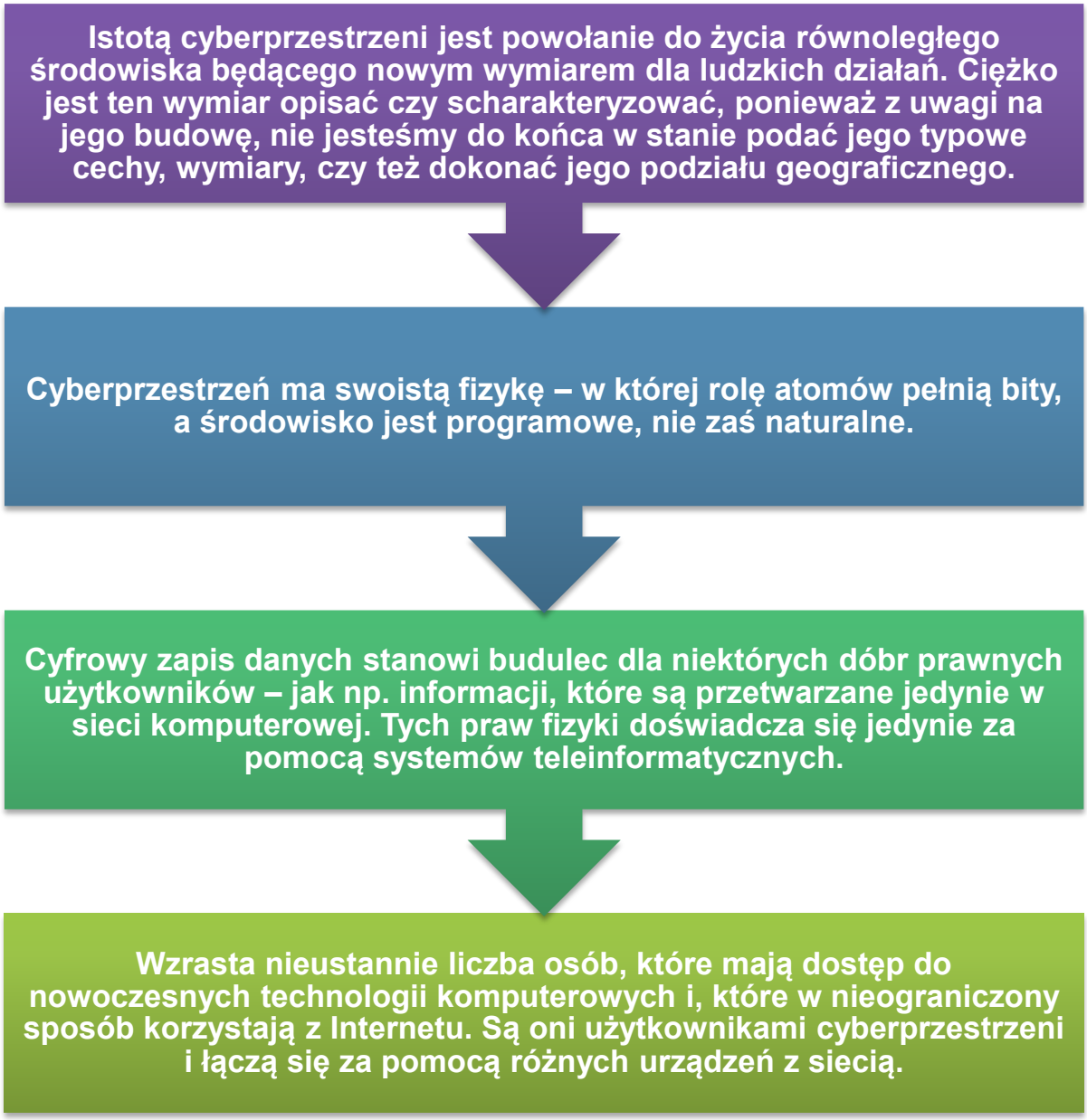
Biorąc pod uwagę najważniejsze cechy definicji warto zwrócić uwagę na fakt, że wprowadza ona ideę jednej cyberprzestrzeni, która wydzielona została z obszaru – cyfrowej domeny przetwarzania oraz wymiany informacji. Przestrzeń ta jest o charakterze ponadnarodowym i tworzą ją systemy teleinformatyczne, połączone za pośrednictwem sieci telekomunikacyjnych, w tym także Internetu, które zbudowane są z elementów infrastrukturalnych znajdujących się na terenie innych krajów. Zatem wszelkie działania w cyberprzestrzeni nie ograniczają się jedynie do wymiany informacji, lecz także na jej:

- ✓ wytwarzaniu,
- ✓ modyfikowaniu,
- ✓ odczytywaniu.

Działania te mogą być podejmowane na gruncie cyfrowej domeny.

Podsumowanie definicji cyberprzestrzeni

Reasumując cyberprzestrzeń nie jest jedynie sumą składników, takich jak systemy, sieci czy oprogramowania i przetwarzania informacji. Nie jest też Internetem – choć to właśnie on stanowi najistotniejszy element cyberprzestrzeni – pojawia się też w każdej omówionej powyżej definicji. Cyberprzestrzeń nie jest też tylko sumą operacji, których dokonuje użytkownik w sieci.



Funkcja definicji cyberprzestrzeni w aspekcie bezpieczeństwa kraju

Biorąc pod uwagę wszelkie definicje cyberprzestrzeni, warto zastanowić się nad jej wpływem na nowoczesne społeczeństwa oraz państwa, a także nad tym w jaki sposób wpływa ona na bezpieczeństwo państw. Cyberprzestrzeń rozumiana jako nowa domena ludzkiej aktywności powinna wiązać się ściśle z należytym poziomem ochrony, którą powinno zapewniać swoim obywatelom każde państwo. ***To, w jaki sposób została zdefiniowana cyberprzestrzeń w kraju wpływa bezpośrednio na sposób określenia obszaru bezpieczeństwa:***

Jeśli wyłączymy z definicji użytkowników, to automatycznie bezpieczeństwo w cyberprzestrzeni będzie skupiało się na zagwarantowaniu ochrony elementom infrastruktury.

Dodając do definicji relacje między użytkownikami a podbudowującym cyberprzestrzeń sprzętem, a także relacje pomiędzy samymi użytkownikami będzie się to wiązało z koniecznością zapewnienia bezpieczeństwa w sposób dynamiczny, bo wiążący się z ludzkimi działaniami.

Biorąc pod uwagę polską definicję cyberprzestrzeni, bezpieczeństwo domeny cyfrowej obejmuje wszelkie powyższe aspekty wraz z działaniami poszczególnych użytkowników. Dzięki temu nie jest to jedynie zestaw zagadnień, które teoretycznie opisują ochronę w tej przestrzeni, lecz bezpieczeństwo dotyczy tego, co dzieje się w cyberprzestrzeni.

Ważną kwestią jest to, że zawarte w definicji relacje między systemami teleinformatycznymi, a co za tym idzie również te zautomatyzowane, wymuszają niejako objęcie bezpieczeństwem obszarów cyberprzestrzeni, w której użytkownicy nie biorą bezpośredniego udziału – przykład: przetwarzanie danych w chmurze. Bezpieczeństwem objęte są także strefy, które nie są dostrzegane przez większość uczestników Internetu – jak np. swoista natura domeny cyfrowej.

3. Definicje bezpieczeństwa w cyberprzestrzeni

Definicji cyberbezpieczeństwa jest wiele, są one uzależnione od tego, do kogo się będzie odnosić – czy do pojedynczych użytkowników Internetu czy też państw, firm, narodów. Jednakże – niezależnie od tego, do jakiej grupy się odnosi, wspólna dla wszystkich definicja cyberbezpieczeństwa oznacza:

zbiór zasobów i podejmowanych działań, które mają na celu umożliwić obywatelom, firmom czy państwom osiąganie celów informatycznych w sposób niezawodny i bezpieczny, przy zachowaniu maksimum prywatności.

Pojęcie bezpieczeństwo w cyberprzestrzeni zostało określone na potrzeby Polityki Ochrony Cyberprzestrzeni RP jako:

- zespół czynności organizacyjnych, prawnych, technicznych, fizycznych oraz edukacyjnych, które mają za zadanie zapewnić spokojne i niezakłócone funkcjonowanie cyberprzestrzeni.

Ujęte w taki sposób bezpieczeństwo odwołuje się do katalogu działań, które są niezbędne do tego, by ochronić wszelkie zasoby domeny cyfrowej i jej użytkowników.

Tak przyjęta definicja cyberbezpieczeństwa wskazuje na podejmowanie działań w sposób nieustanny, które mają na celu zapewnić ochronę nie tylko w aspekcie technicznym, czy fizycznym, ale również edukacyjnym i prawnym.

4. Strategia cyberbezpieczeństwa w Polsce – program na lata 2016-2020

Zakres i cele

Głównym celem strategii cyberbezpieczeństwa jest osiągnięcie odpowiedniego poziomu bezpieczeństwa w państwie, które rozumie się przez zapewnienie zdolności do:

- realizowania funkcji kraju
- zapewnienia osobom indywidualnym oraz podmiotom instytucjonalnym, firmom, niezbędnych dostaw usług i towarów
- niezakłócanego dostępu oraz korzystania z sieci internetowych

Osiągnięcie celu możliwe będzie poprzez utworzenie ram prawno-organizacyjnych, a także systemu skutecznego koordynowania i komunikowania się między jego użytkownikami.

Do szczegółowych celów zalicza się:

- zwiększenie poziomu bezpieczeństwa infrastruktury sieci teleinformatycznej w kraju
- wzrost zdolności zapobiegania i zwalczania zagrożeń w cyberprzestrzeni
- zmniejszanie skutków zdarzeń, które zakłócają bezpieczeństwo w cyberprzestrzeni

Strategia dotyczy następujących grup użytkowników Internetu:

obywateli kraju poprzez:

- zwiększenie bezpieczeństwa w cyberprzestrzeni
- wzrost poziomu zaufania do korzystania z e-usług
- nieustanny i bezpieczny dostęp do e-usług

osób prowadzących firmy poprzez:

- wzrost poziomu zaufania do korzystania z e-usług w prowadzeniu biznesu
- zwiększenie bezpieczeństwa operacji – finansowych oraz technologicznych
- wzrost poziomu zaufania do korzystania z e-usług
- nieustanny i bezpieczny dostęp do e-usług
- rozwój rodzimych technologii w sektorze bezpieczeństwa w cyberprzestrzeni

pracowników administracji publicznej poprzez:

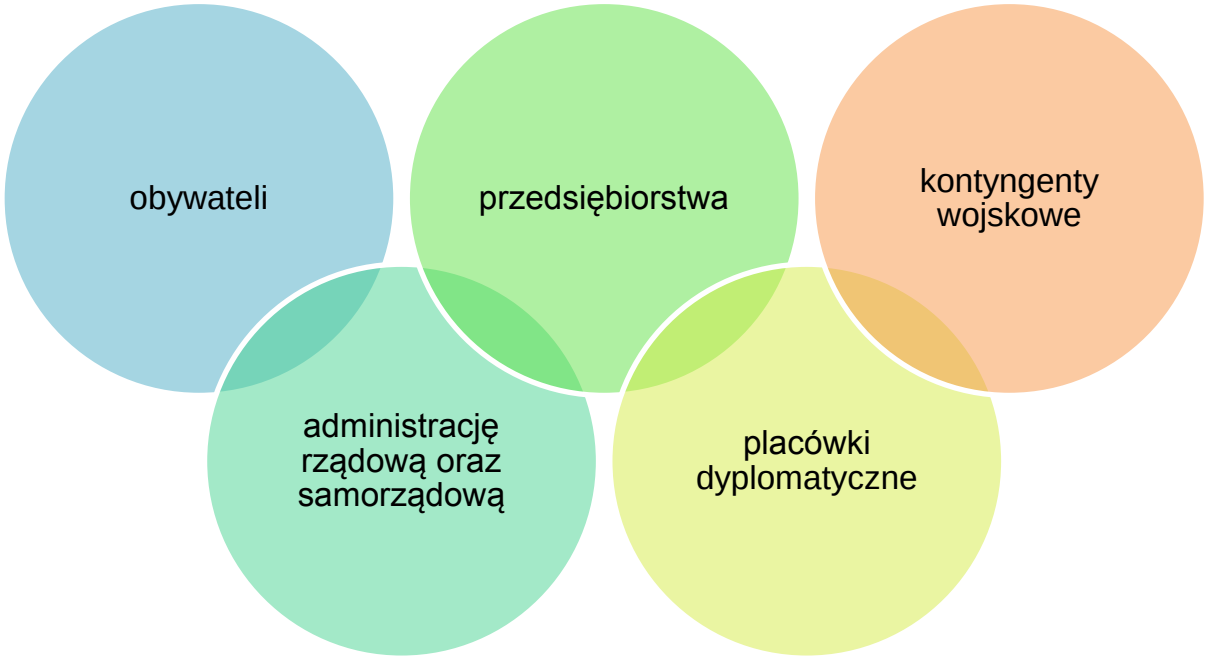
- zapewnienie ciągłej realizacji ważnych funkcji państwa oraz odpowiedniego poziomu bezpieczeństwa w cyfryzacji i informatyzacji procesów administracyjnych i usług
- zapewnienie ciągłego dostępu do e-usług
- zwiększenie odporności na cybernetyczne ataki
- utworzenie działów w administracji publicznej zajmujących się teleinformatyką i cyberbezpieczeństwem

operatorów kluczowych usług poprzez:

- ukierunkowanie na działania państwa, których celem jest wspomaganie ciągłego świadczenia kluczowych usług

Zakres przyjętej strategii

Strategia oddziałuje w sposób pośredni oraz bezpośredni na wszystkich użytkowników w obrębie kraju, a także poza jego granicami, tj. na:



Ochrona niejawnych informacji jest z tego systemu wykluczona, ponieważ ten zakres rządzi się swoimi regulacjami prawnymi i posiada własne mechanizmy ochronne. Jednak trzeba być świadomym, że zagrożenia, które dotyczą systemów jawnych mogą także obejmować niejawne obszary, stąd

podejmowane działania będą mieć bezpośrednie przełożenia na bezpieczeństwo systemów, które przetwarzają klasyfikowane informacje.

Aby osiągnąć założenia przyjęte w strategii konieczne było i jest:

- zorganizowanie krajowego systemu cyberbezpieczeństwa – wraz z uwzględnieniem roli publicznych i prywatnych podmiotów wraz z obywatelami
- koordynowanie działań w kraju z dziedziny cyberbezpieczeństwa na arenie międzynarodowej – uwzględniając poziom polityczny, strategiczny oraz operacyjny
- podjęcie współpracy z ośrodkami akademickimi, organizacjami pozarządowymi, a także sektorem prywatnym mającej na celu zarządzanie wiedzą i innowacjami w dziedzinie cyberbezpieczeństwa

Współczesne podejście do problemu cyberbezpieczeństwa polega na:

- zapewnieniu ochrony w cyberprzestrzeni takich funkcji państwa, jak dostawy energii, usługi bankowe, ochrona zdrowia, transport, itp.

zapewnieniu całodobowej kontroli nad bezpieczeństwem w cyberprzestrzeni ważnych i istotnych danych, serwisów, usług oraz użytkowników

wprowadzeniu systemu ochrony, który jest trzypoziomowy i polega na:

- skoordynowanej ochronie cyberprzestrzeni RP na transgranicznych punktach wymiany Internetu (IXP)
- dostosowaniu sieci do potrzeb bezpieczeństwa w obszarze branżowym, funkcjonalnym bądź terytorialnym
- zapewnieniu bezpieczeństwa danych na poziomie architektury poszczególnych systemów – kopie zapasowe, archiwizacja danych

wprowadzeniu szkoleń dla specjalistów zajmujących się bezpieczeństwem teleinformatycznym, projektowaniem, użytkowaniem i eksploatacją systemów teleinformatycznych

bezpiecznym użytkowaniu indywidualnych środków cyfrowej komunikacji (PC, laptopy, tablety, telefony, itp.), którą wykorzystują obywatele do komunikowania się z państwowymi systemami

wprowadzeniu przepisów i procedur dotyczących reagowania na incydenty i współpracy z zagranicą

zastosowaniu standardów dotyczących technologii w zakresie teleinformatycznego bezpieczeństwa

Cyberprzestrzeń – poszanowanie wolności i praw w cyberprzestrzeni

Działania, które będzie podejmował polski rząd, dotyczące zwiększenia bezpieczeństwa w cyberprzestrzeni muszą odbywać się z poszanowaniem wolności i prawa obywateli. Cyberbezpieczeństwo nie powinno być związane z ograniczaniem praw człowieka.

Wyznacznikiem cyberbezpieczeństwa są nie tylko:

ale również

Wszelkie prawa nie zwalniają jednak osób, które korzystają z dóbr cyberprzestrzeni, z odpowiedzialności. Należy być świadomym zagrożeń, jakie istnieją w sieci, ale też z faktu, że nieodpowiedzialne korzystanie z zasobów Internetu może również być niebezpieczne.

W Polsce rośnie stale liczba urządzeń, które umożliwiają korzystanie z Internetu. Osoby prywatne używają ich do celów:

- ✓ komunikacyjnych,
- ✓ rozrywkowych,
- ✓ pozyskiwania informacji,
- ✓ prowadzenia działalności gospodarczej.

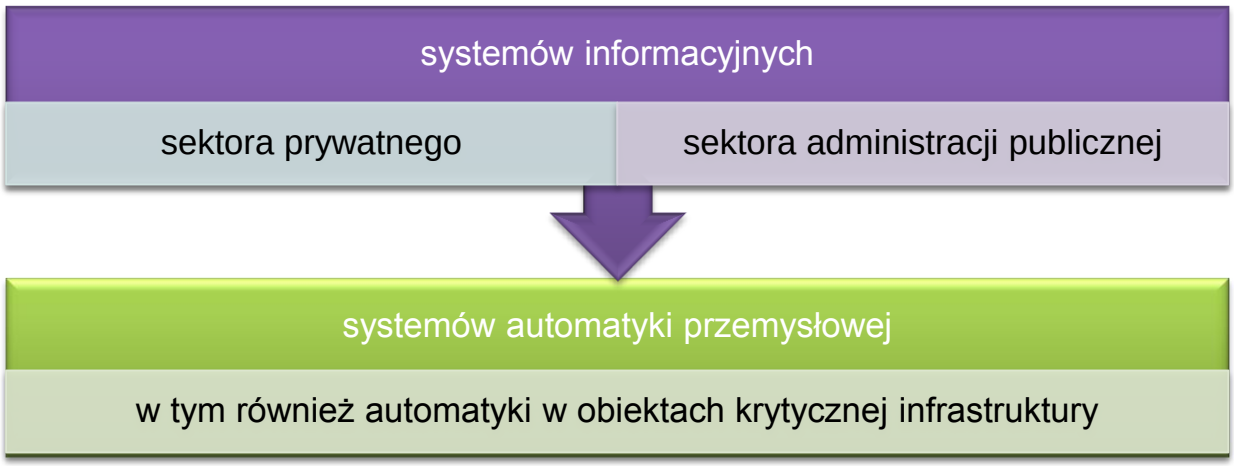
Nieumiejętne korzystanie ze stron internetowych, które często są narażone na ataki złośliwych oprogramowań skutkuje tym, że podczas łączenia się z zaufanymi systemami – szczególnie bankowością elektroniczną czy administracją publiczną – narażonym się jest na poważne zagrożenia.

Każdy obywatel ma tak naprawdę wpływ na bezpieczeństwo pozostałych użytkowników Internetu, stąd tak ***ważne jest by podejmowane działania na rzecz bezpieczeństwa w cyberprzestrzeni:***

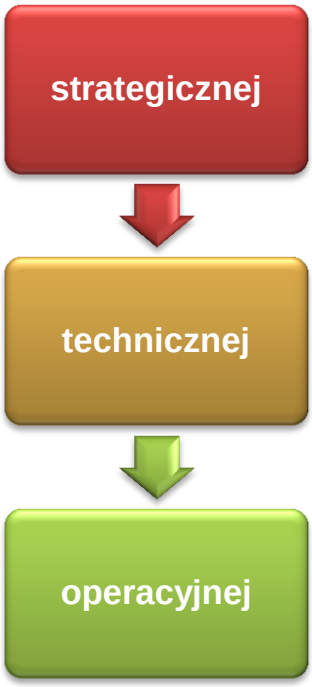
Cyberbezpieczeństwo elementem polityki kraju

Działania mające na celu wprowadzenie strategii oparte są na modelu sieci OSI - *Open Systems Interconnection Reference Model.* Każdy z poziomów modelu obejmuje swoim zakresem działania w obszarze technologicznym i informacyjnym. Wiąże się to z koniecznością ścisłej współpracy służb odpowiadających za infrastrukturę krytyczną oraz e-usług.

Ataki z cyberprzestrzeni mogą dotyczyć:

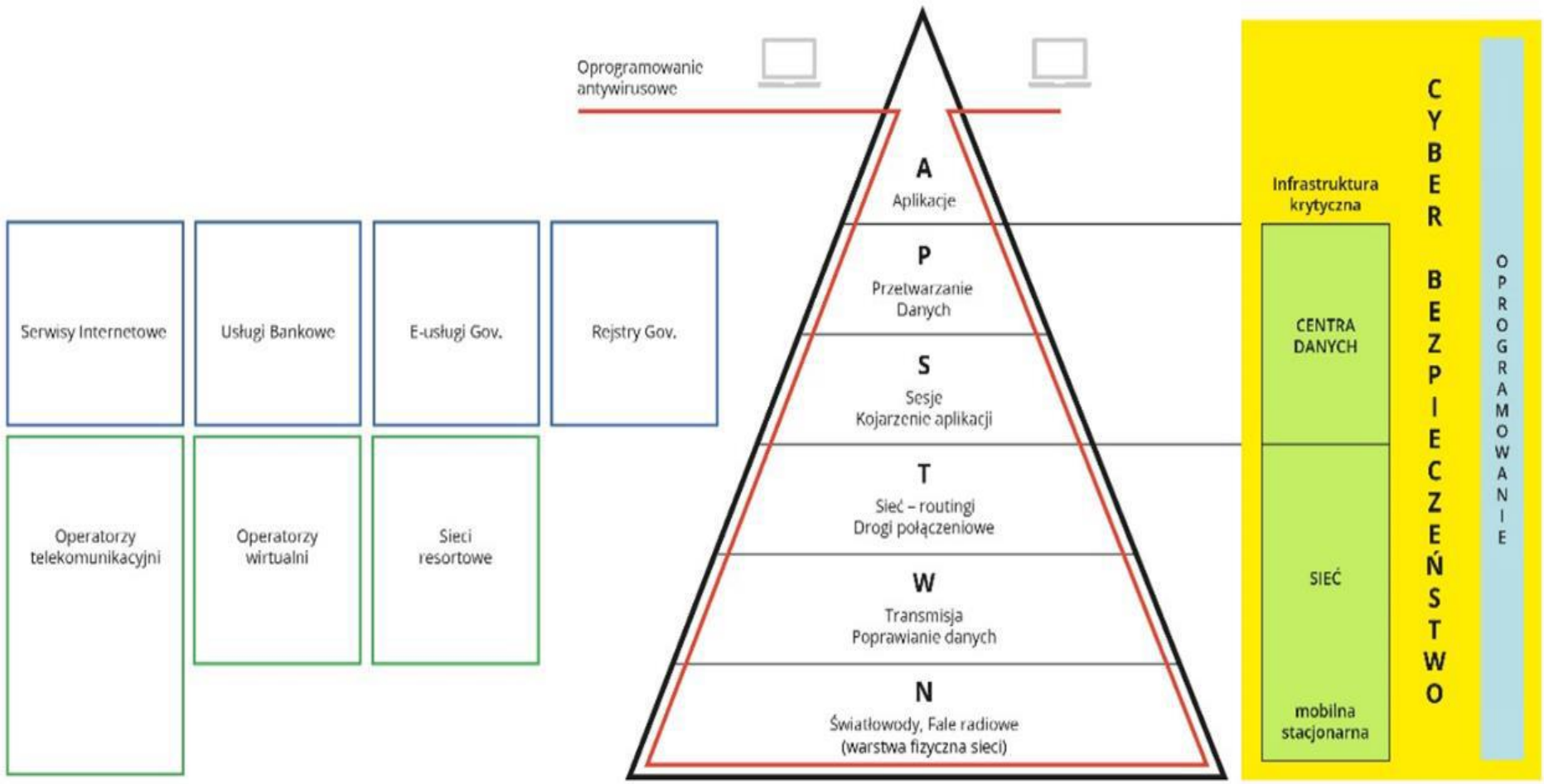


Cały proces zapewnienia bezpieczeństwa w sieci przebiega na 3 różnych płaszczyznach:

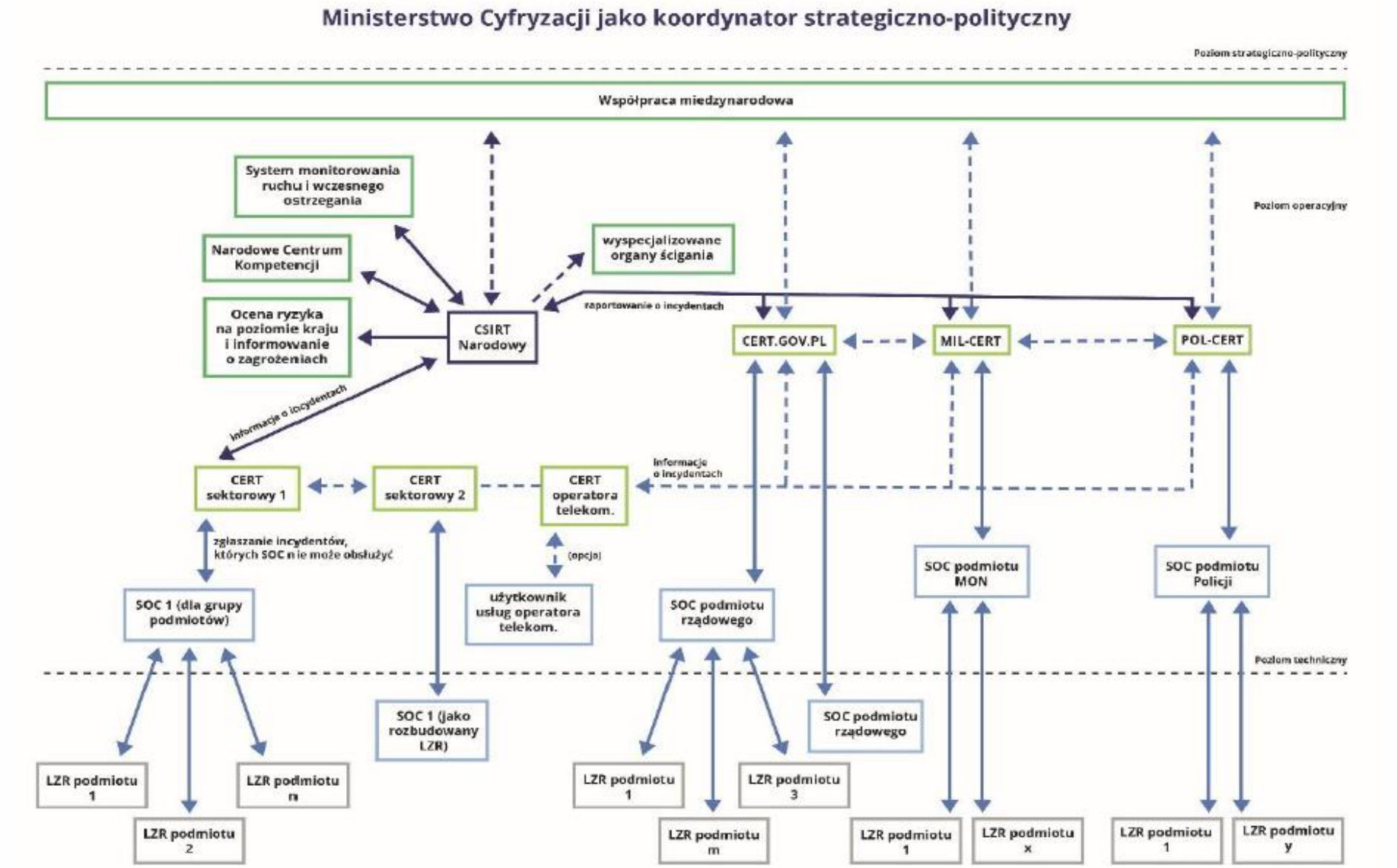


Na każdej płaszczyźnie podejmowane są określone działania w zakresie technologicznym i zarządzania. W obszarze strategicznym przeważać będą wszelkie działania związane z zarządzaniem, w technicznym – w zakresie technologicznym.

Cały proces „*powiązania warstw modelu OSI z obszarami cyberbezpieczeństwa*” obrazuje poniższy schemat:



Źródło: „Strategia cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2016-2020”, Ministerstwo Cyfryzacji



LZR – Lokalne Zespoły Reagowania; SOC – Operacyjne Centrum Bezpieczeństwa; Źródło: „Strategia cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2016-2020”, Ministerstwo Cyfryzacji

Wewnętrzne uwarunkowania

Strategiczny wymiar

Podejmowane działania związane z ochroną w cyberprzestrzeni muszą być ustanowione poprzez przepisy zgodne z konstytucją państwa, a także uwzględniać odpowiedzialność i kompetencje władz organów publicznych. ***Strategiczny wymiar obejmuje poszczególne strefy, do których zalicza się:***

Organ doradczy prezydenta RP – Biuro Bezpieczeństwa Narodowego

- Ma za zadanie opracować Doktrynę Cyberbezpieczeństwa RP, określając tym samym kierunek działań wpisanych w międzynarodową sytuację.

Wiodąca rola w procesie stanowienia prawa w zakresie walki z cyberprzestępczością – Minister Sprawiedliwości

Szef ABW

- Odpowiada za bezpieczeństwo organizacji systemu w przypadku, gdy zagrożone zostają interesy państwa - w tym ataki terrorystyczne.
- Wykonuje bieżące zadania w ścisłej współpracy z pozostałymi podmiotami systemu.

Minister Obrony Narodowej

- Jest odpowiedzialny za organizację obrony kraju.
- Ma za zadanie pozyskiwać – poprzez Siły Zbrojne RP – pełen zakres zdolności do aktywnej obrony i ofensywnych działań w cyberprzestrzeni.
- Podejmuje wszelkie działania na wypadek ewentualnych zagrożeń wojennych, a także w czasie trwania wojny, wykorzystując mechanizmy planowania obronnego.
- Kieruje systemem bezpieczeństwa w sieci w razie wyższych stanów gotowości obronnej kraju.
- Przygotowuje i opracowuje (plan organizacyjny) zasady działania CSIRT Narodowego w czasie trwania wojny lub kryzysu.
- Podczas wykonywania zadań ściśle współpracuje z innymi podmiotami systemu.

Minister Spraw Wewnętrznych i Administracji

- Odpowiada za organizację działań związanych z zapewnieniem ochrony systemów teleinformatycznych resortu spraw wew. i administracji.
- Podczas wykonywania zadań ściśle współpracuje z innymi podmiotami systemu.

Komendant Główny Policji

- Odpowiada za ściganie przestępców w obszarze cyberprzestrzeni.
- Ma za zadnie nadzorować działania związane z zapewnieniem ochrony systemów teleinformatycznych w kraju.

Minister Cyfryzacji

- Nie wchodzi w kompetencje pozostałych użytkowników systemu.
- Działa zgodnie z ustawą o działach administracji rządowej.
- Ma za zadanie podejmować działania organizacyjne i prawne, które będą podnosić bezpieczeństwo w sieci – tj. przygotowuje projekty aktów prawnych, zalecenia, nadzoruje i harmonizuje procedury oraz procesy zarządzania informacją w obszarze cyberbezpieczeństwa.
- Odpowiada za współdziałanie poszczególnych sektorów, takich jak energetyka, finanse, telekomunikacja, rejestry państwowe, itp.
- Tworzy system wczesnego ostrzegania oraz klastry bezpieczeństwa.
- Podczas wykonywania zadań ściśle współpracuje z innymi podmiotami systemu.

Sposób uporządkowania kompetencji między podmiotami odpowiedzialnymi za ochronę cyberprzestrzeni RP określa ustawa o krajowym systemie cyberbezpieczeństwa.

Operacyjny wymiar

Obejmuje swoim zakresem działania, które mają:

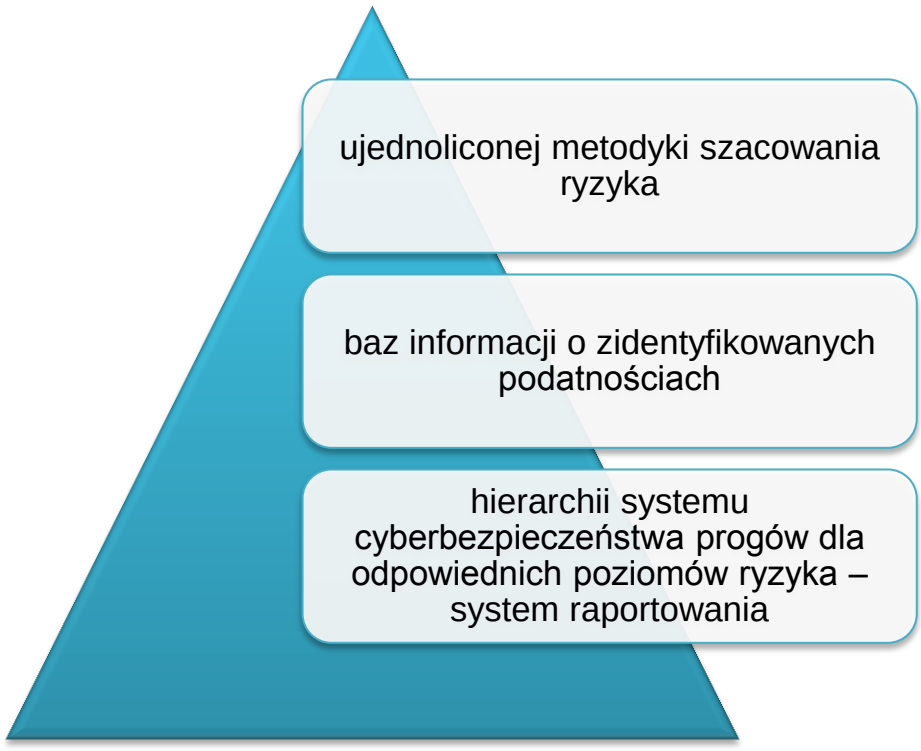
- ✓ zapobiegać i wykrywać, a także przeciwdziałać potencjalnym atakom,

- ✓ reagować na ataki już zaistniałe,
- ✓ informować o ryzyku wystąpienia ataku.

Sprawna wymiana informacji jest niezwykle ważna, by minimalizować potencjalne negatywne skutki dla krajowych systemów teleinformatycznych.

System informacyjno-ostrzegawczy opiera się na ścisłej współpracy wszystkich ogniw, które funkcjonują w łańcuchu monitorowania cyberprzestrzeni. Dzięki niemu zapewniona jest efektywność działania całego systemu.

Efektywny system zarządzania ryzykiem wpływa na sprawność podejmowanych działań w wymiarze operacyjnym. ***Najważniejszą rolę pełni system szacowania rodzajów ryzyka w rzeczywistym czasie***. Aby proces sprawnie funkcjonował konieczne było zapewnienie:



Na szczycie hierarchii podmiotów w krajowym systemie cyberbezpieczeństwa stoi Narodowe Centrum Cyberbezpieczeństwa. Zbiera ono informacje o incydentach naruszania bezpieczeństwa i ocenia je pod kątem ryzyka i konsekwencji, jakie mogą nastąpić w cyberprzestrzeni pod kątem bezpieczeństwa.

Techniczny wymiar

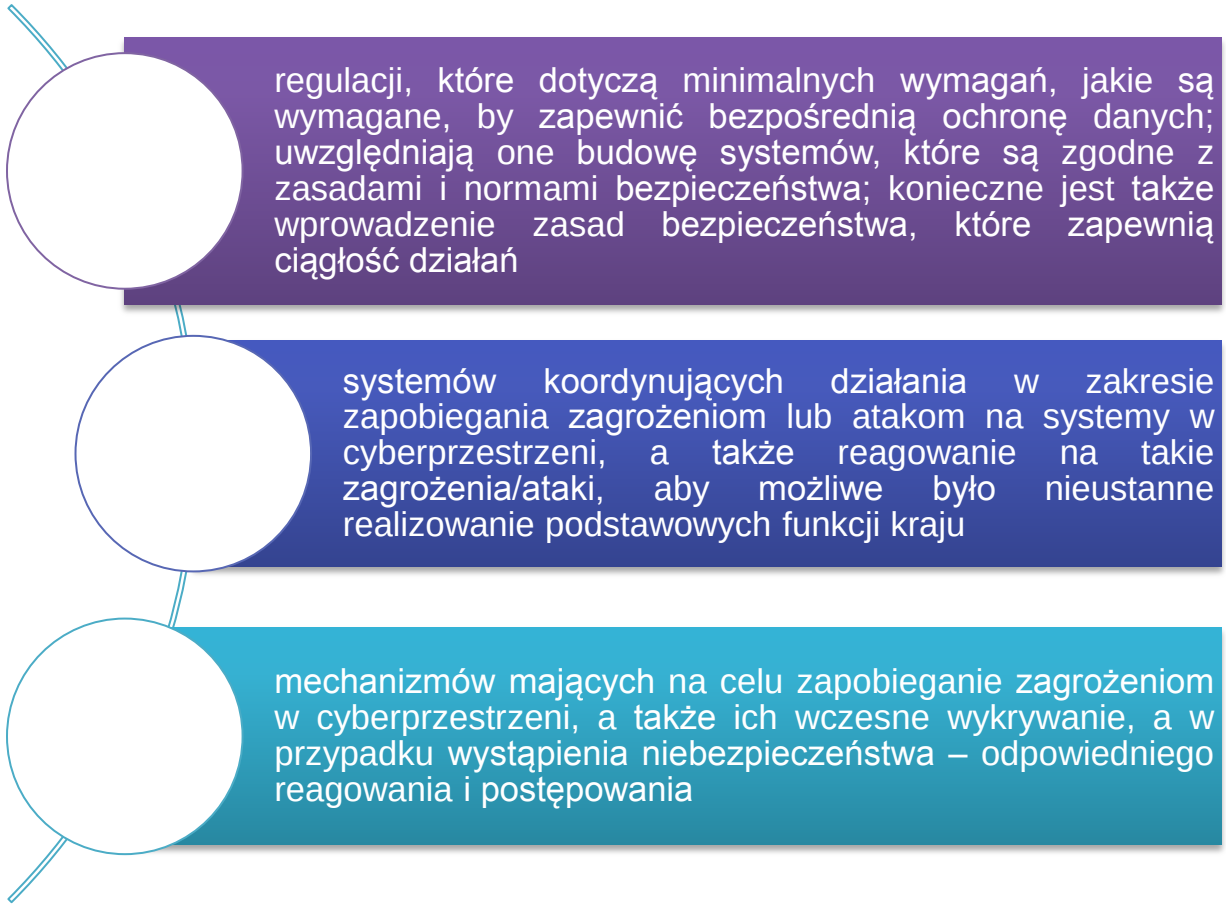
Techniczny wymiar jest domeną aktywności właścicieli sieci wraz z systemami teleinformatycznymi. Oba podmioty muszą wydzielać środki, a także siły, które służą do tego, by:

- aktywnie analizować ryzyko,
- wdrażać zabezpieczenia zgodnie z oceną zidentyfikowanego rodzaju ryzyka,
- monitorować cyberbezpieczeństwo,
- przeciwdziałać atakom.

Krajowy system cyberbezpieczeństwa – organizacja

Wdrażany system krajowego cyberbezpieczeństwa obejmuje całokształt działań podejmowanych do tego, by ustanowić i utrzymywać odpowiedni poziom bezpieczeństwa w sieci. Żaden z elementów systemu nie może zostać pominięty w procedurach reagowania na występujące zagrożenia. Podejmowane przez państwo działania nie ograniczają się jedynie do państwowych czy samorządowych zasobów, lecz także obejmują sektor prywatny i obywateli.

Zarówno użytkownicy indywidualni, jak również przedsiębiorcy, poprzez korzystanie z niezaufanych serwisów, infekują swoje urządzenia oprogramowaniami zawierającymi wirusy. To z kolei może przyczyniać się do zwiększenia liczby zagrożeń w cyberprzestrzeni zarówno wśród użytkowników indywidualnych, jak również w systemach publicznych podmiotów. Dlatego tak ważne było i jest utworzenie:

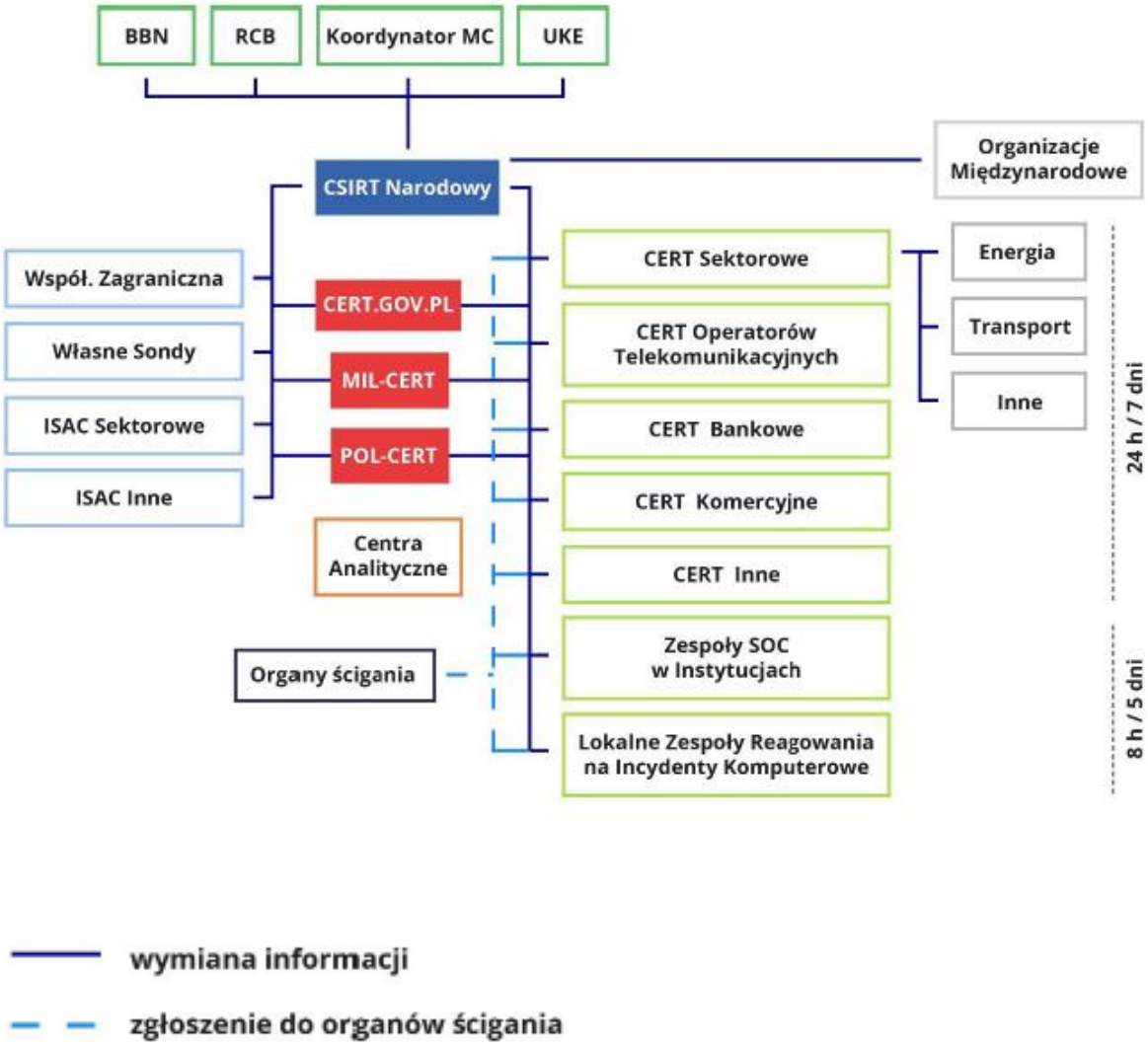


Budowa systemu

Krajowy system cyberbezpieczeństwa ma obejmować:

- ministerstwo właściwe do spraw informatyzacji – minister ma pełnić funkcję koordynatora na poziomie polityczno-strategicznym
- ministrowie zgodnie z określonymi zakresami kompetencji
- NCCyber
- sektorowe CSIRT
- kierownicy urzędów oraz instytucji, którą obejmuje strategia – są odpowiedzialni za wdrażanie cyberbezpieczeństwa w urzędach/instytucjach niższego szczebla

Budowę systemu przestawia się w następujący sposób:



Źródło: „Strategia cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2016-2020", Ministerstwo Cyfryzacji

Funkcje ministra właściwego do spraw informatyzacji

Rola jaką pełni minister polega na koordynowaniu strategii w sferze cyberbezpieczeństwa kraju. Jest tym samym odpowiedzialny za realizację m.in. takich zadań, jak:

- opracowywanie i przygotowywanie projektów aktów prawnych, które są niezbędne do stanowienia wymagań w zakresie bezpieczeństwa w sieci
- koordynowanie tworzenia stanowiska w zakresie międzynarodowych regulacji
- koordynowanie działań, które wiążą się z zapewnieniem bezpieczeństwa w sieci administracji publicznej
- organizowanie współpracy (w zakresie bezpieczeństwa w sieci) z takimi organami władzy, jak Biuro Bezpieczeństwa Narodowego i przedstawicielami placówek samorządu terytorialnego w ramach *Komisji Wspólnej Rządu i Samorządu Terytorialnego*
- organizowanie współpracy z pozarządowymi organizacjami - szczególnie w zakresie edukacji o cyberbezpieczeństwie
- nadzór nad Narodowym Centrum Cyberbezpieczeństwa

Rola NC Cyber

- ***Narodowe Centrum Cyberbezpieczeństwa ma w swoim zakresie obowiązków zorganizowanie oraz zapewnienie bezpiecznych kanałów komunikacyjnych, które mają umożliwiać korzystanie z usług NCCyber.***
- ***Wszelkie zadania operacyjne oraz świadczenie usług przez NC Cyber będzie odbywało się każdego dnia przez 24 h.***

Pozostałe zadania i funkcje NC Cyber to:

To właśnie NC Cyber ma za zadanie monitorować i kontrolować wszelkie incydenty związane z cyberniebezpieczeństwem, do których będzie dochodzić w kraju i przekazywać je we wczesnych ostrzeżeniach, alarmach, ogłoszeniach, a także wydawać niezbędne informacje na temat rodzajów zagrożeń i potencjalnych incydentów za pomocą zbierania danych z transgranicznych punktów wymiany Internetu.

NC Cyber ma oceniać zagrożenia występujące w ruchu międzynarodowych oraz między operatorami.

NC Cyber ma zapewnić wsparcie merytoryczne (opracowywanie standardów z zakresu bezpieczeństwa oraz ich promocja) operatorom usług kluczowych.

Współpraca NC Cyber ma dotyczyć także CERT.GOV.PL w zakresie incydentów dotyczących bezpieczeństwa w systemach teleinformatycznych krytycznej infrastruktury.