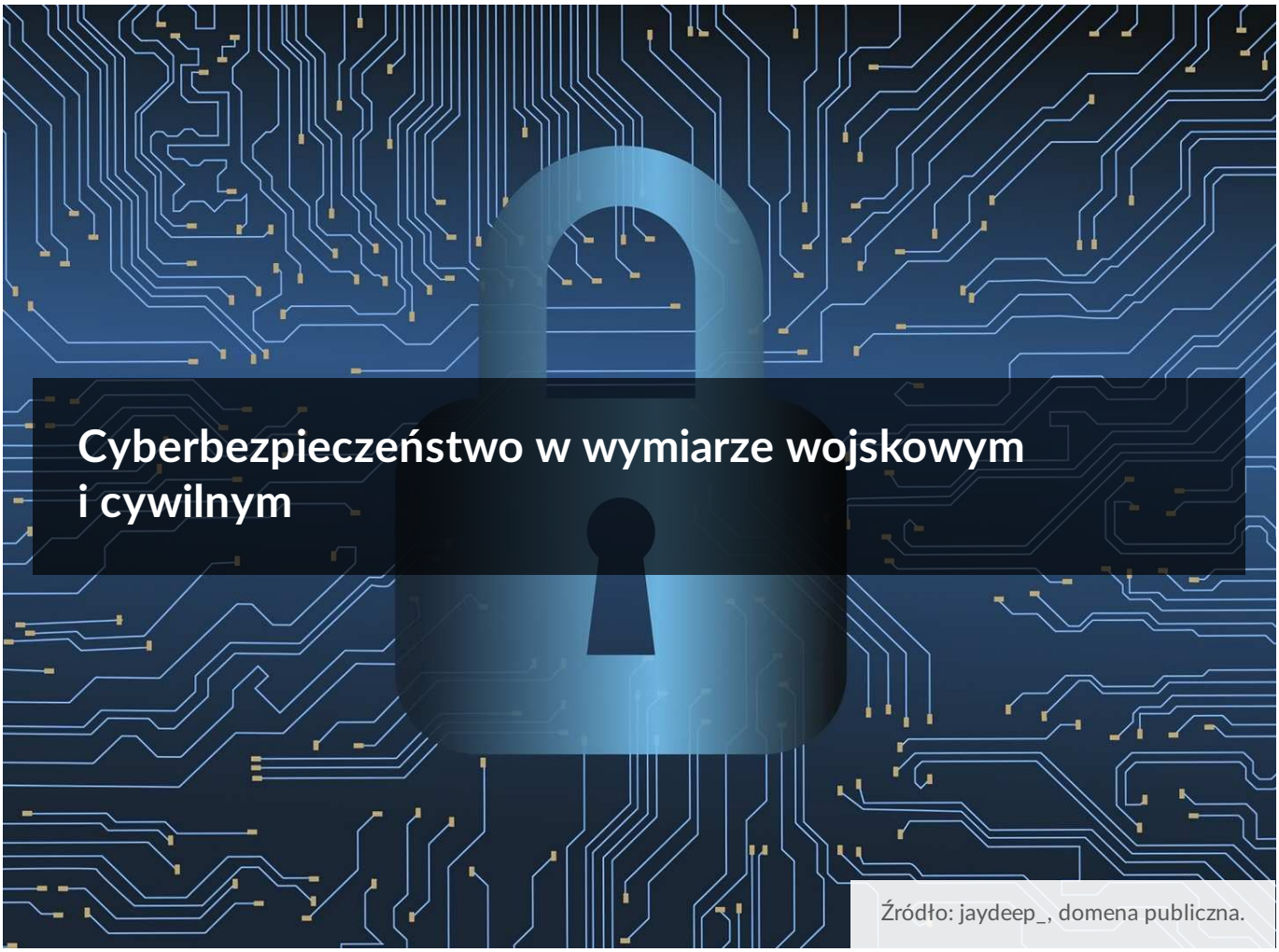
Cyberbezpieczeństwo w wymiarze wojskowym i cywilnym

Bibliografia:

- Źródło: *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dziennik Ustaw 2018, pozycja 1560 z późniejszymi zmianami*, dostępny w internecie: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560/U/D20181560Lj.pdf [dostęp 30.06.2022].
- Źródło: *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024*, dostępny w internecie: https://www.dziennikustaw.gov.pl/M2019000103701.pdf [dostęp 30.06.2022].
- Źródło: *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. art 2 pkt 4*, dostępny w internecie: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/U/D20181560Lj.pdf.



Źródło: jaydeep_, domena publiczna.

Szybko rozwijające się technologie informacyjne i duży stopień uzależnienia od nich obywateli, firm, instytucji oraz organów państwa spowodował, że bezpieczeństwo w cyberprzestrzeni w XXI wieku decyduje o aspektach życia codziennego. Co więcej, stało się ono także nową domeną starć o charakterze wojskowym. Więcej na ten temat dowiesz się z tego materiału.

Cyberataki to bardzo poważne zagrożenie zarówno dla jednostek jak i całych społeczeństw. Spróbuj odnaleźć w wiarygodnych źródłach, kiedy nastąpił pierwszy potwierdzony cyberatak, który doprowadził do paraliżu całego państwa. Sprawdź, co to było za państwo, jakie były przyczyny i przebieg ataku.

Możesz w tym celu skorzystać z innego e-materiału pt. Cyberterroryzm.

> **Nauczysz się**
>
> - identyfikować podstawowe zagrożenia cyberbezpieczeństwa;

- przedstawiać i wyjaśniać wybrane definicje dotyczące cyberbezpieczeństwa;
- określać podział ról w czasie współdziałania podmiotów układu pozamilitarnego i militarnego w kontekście cyberbezpieczeństwa;
- odbierać ze zrozumieniem informacje dotyczące cyberbezpieczeństwa militarnego w systemie cyberbezpieczeństwa państwa i samemu tworzyć wypowiedzi na ten temat.

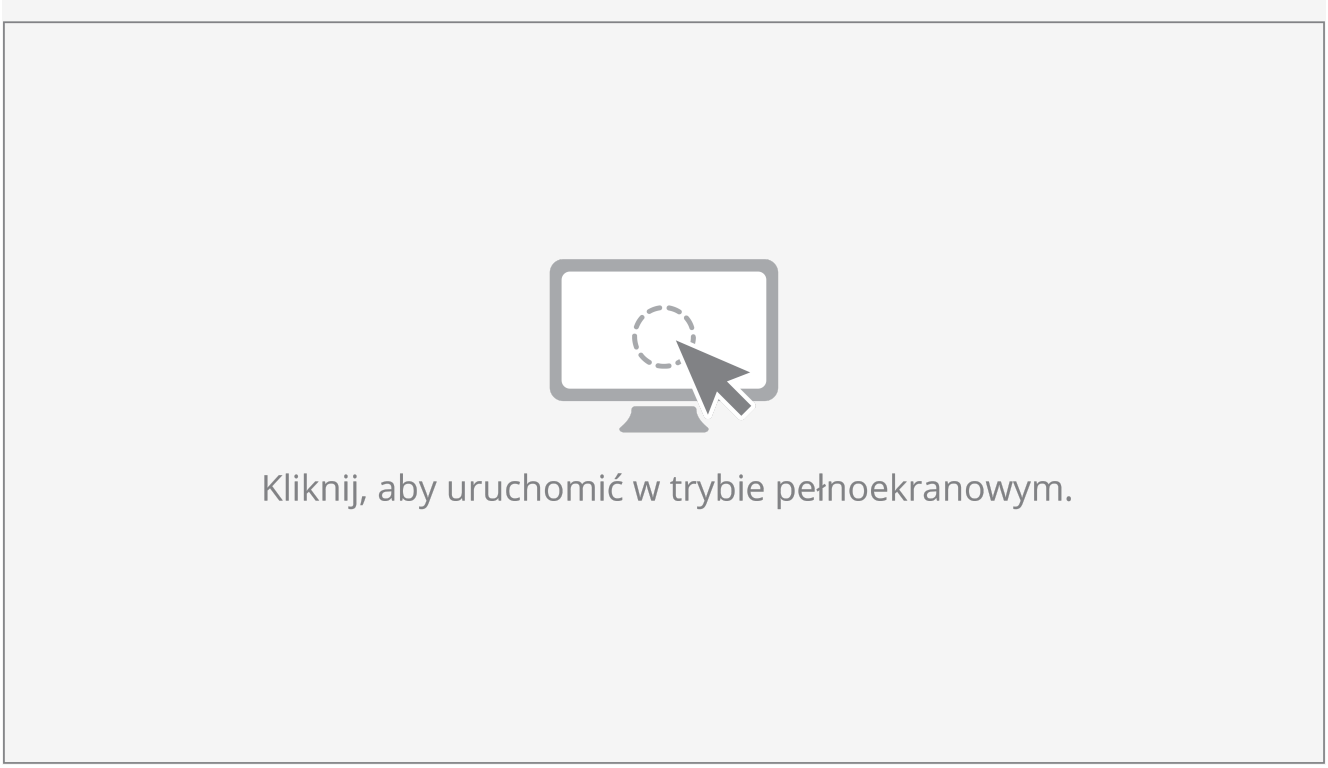
1. Cyberbezpieczeństwo w wymiarze cywilnym

Rozwój społeczny i gospodarczy w coraz większym stopniu zależny jest od szybkiego i nieskrępowanego dostępu do informacji. Od sprawności i stabilności systemów teleinformatycznych zależy funkcjonowanie całego państwa.

Cyberbezpieczeństwo to:

> **Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa**
>
> [...] odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.
>
> Źródło: *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. art 2 pkt 4*, dostępny w internecie: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/U/D20181560Lj.pdf.

W tym podrozdziale skupimy się na jego wymiarze cywilnym i zagrożeniach. Zapoznaj się z poniższą prezentacją multimedialną.



> **Polecenie 1**
> Wyjaśnij, czym jest phishing [wym. fiszin]. Podaj przykłady takiego działania.

> **Polecenie 2**
> Wytłumacz, o jakie aspekty poszerza się zakres potencjalnych cyberzagrożeń dla podmiotów prowadzących działalność gospodarczą w porównaniu z osobami fizycznymi.

> **Polecenie 3**
> Opisz a czym polega działanie określane mianem „deepfake” [dipfejk].

Dokumentem strategicznym określającym ryzyka, szanse i wyzwania w zakresie cyberbezpieczeństwa jest *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej.*

Cel główny określony w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 to:

> ## Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024

> Podniesienie poziomu odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji.
>
> Źródło: *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024*, dostępny w internecie: https://www.dziennikustaw.gov.pl/M2019000103701.pdf [dostęp 30.06.2022].

W dokumencie wymieniono także następujące cele szczegółowe:

- rozwój krajowego systemu cyberbezpieczeństwa;
- podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty;
- zwiększanie potencjału narodowego w zakresie bezpieczeństwa w cyberprzestrzeni;
- budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa;
- zbudowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w zakresie cyberbezpieczeństwa.

Zgodnie ze Strategią ochrona systemów informacyjnych oraz przetwarzanych w nich informacji jest wyzwaniem dla wszystkich podmiotów tworzących krajowy system cyberbezpieczeństwa, a więc:

- podmiotów gospodarczych świadczących usługi przy wykorzystaniu systemów informacyjnych,
- organów władzy publicznej,
- organów odpowiedzialnych za bezpieczeństwo narodowe,
- wyspecjalizowanych podmiotów zajmujących się cyberbezpieczeństwem w sferze operacyjnej.

Jest to tym istotniejsze, iż Polska jest ściśle powiązana z innymi państwami przez współpracę międzynarodową w ramach takich organizacji jak Unia Europejska (EU),

Organizacja Traktatu Północnoatlantyckiego (NATO), Organizacja Narodów Zjednoczonych (ONZ) czy Organizacja Bezpieczeństwa i Współpracy w Europie (OBWE). Współpraca ta odgrywa istotną rolę w reagowaniu na zwiększającą się liczbę incydentów powodowanych nielegalnymi działaniami w cyberprzestrzeni, powodujących rosnące straty materialne i wizerunkowe.

Drugim ważnym dokumentem, w którym uregulowano kwestie cyberbezpieczeństwa jest *Ustawa o krajowym systemie cyberbezpieczeństwa*.

> ## Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa
>
> Krajowy system cyberbezpieczeństwa ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów.
>
> Źródło: *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dziennik Ustaw 2018, pozycja 1560 z późniejszymi zmianami*, dostępny w internecie: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560/U/D20181560Lj.pdf [dostęp 30.06.2022].

Na mocy Ustawy zostały powołane trzy Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego na poziomie krajowym – w skrócie CSIRT. Są to:

- **CSIRT GOV –** prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;
- **CSIRT MON –** prowadzony przez Ministra Obrony Narodowej;
- **CSIRT NASK –** prowadzony przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy.

Internet to jedno z głównych źródeł informacji o różnych wydarzeniach i przestrzeń, w której funkcjonują portale społecznościowe. Jest to także miejsce w którym na szeroką skalę prowadzi się dezinformację i rozpowszechnia fake newsy [wym. fejk niusy]. Celem takiego działania jest np. manipulacja, wprowadzanie w błąd,

wywoływanie paniki, dyskredytowanie ludzi, szokowanie, odwracanie uwagi od innych zdarzeń. Fałszywe wiadomości mogą być niebezpieczne, w szczególności dla młodych odbiorców. Takimi informacjami mogą być m.in. posty w mediach społecznościowych, informacje w serwisach internetowych, tweety [wym. tłity], komentarze pod artykułami, teksty propagandowe, a nawet memy. Szokujący charakter takich przekazów przyciąga uwagę, skłania do kliknięcia, zapoznania się z nimi i podzielenia wiadomością z innymi, co wpływa na szybkie rozprzestrzenianie się szkodliwej treści. Fałszywe posty lub strony coraz częściej stają się też narzędziem do przeprowadzenia ataków phishingowych, kształtowania poglądów i zachowań oraz wywoływaia negatywnych emocji.

2. Militarne zagrożenia cyberbezpieczeństwa

Współczesna sztuka wojenna zakłada wykorzystanie nowoczesnych środków walki, dowodzenia oraz łączności. Celem jest możliwie jak najdokładniejsze zobrazowanie sytuacji na polu walki już od szczebla taktycznego - pojedynczego wozu czy pododdziału, poprzez operacyjny, aż do szczebla strategicznego dowodzenia. Ten rodzaj pola walki określamy mianem sieciocentrycznego.

Stopień, w jakim dana armia jest nimi nasycona, jest proporcjonalny do rozwoju gospodarczego i technicznego danego państwa. Na przykład, co najmniej od lat 80. XX wieku liderem na tym polu były Stany Zjednoczone, w których rozpoczęła się kolejna fala rewolucji przemysłowych związana z produkcją mikroprocesorów, komputerów, rozwojem internetu.

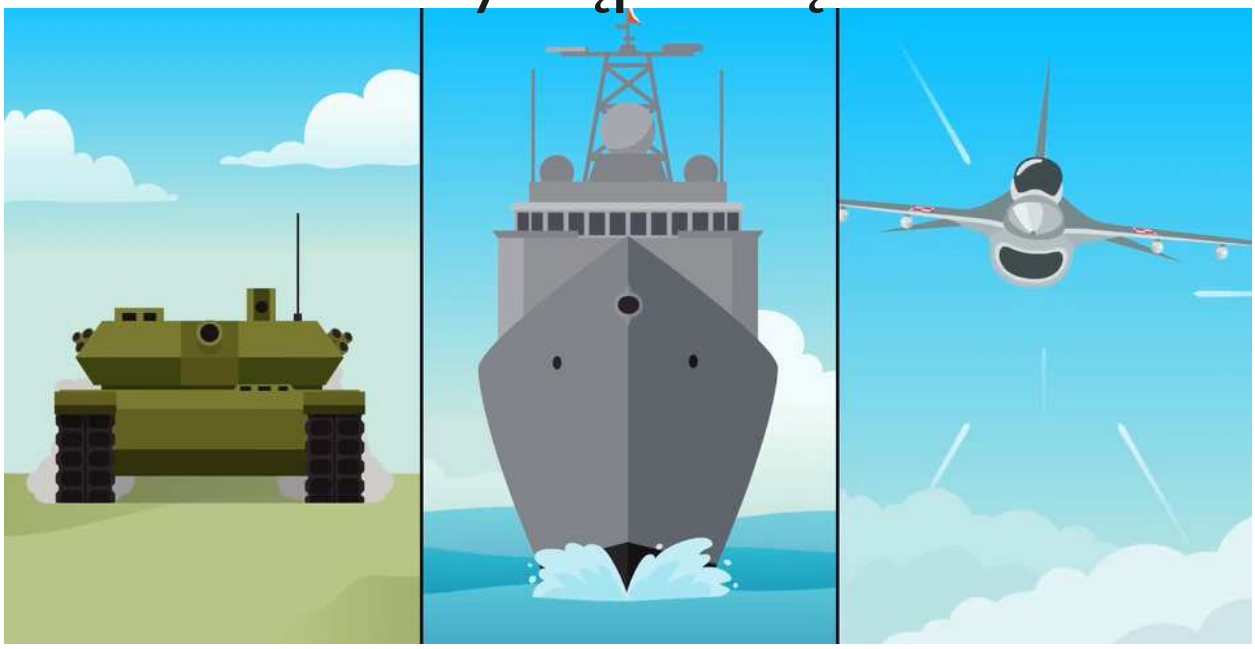
Konflikty, w które były w XXI wieku zaangażowane państwa NATO pokazały, że zwykle w pierwszej kolejności dążono do zlikwidowania takich wrogich obiektów jak systemy rozpoznania, dowodzenia oraz łączności. Uderzenie sił konwencjonalnych, jeżeli następowało, było kolejnym etapem.

Wraz z rozwojem przekazywania informacji drogą cyfrową doszły jednak również zagrożenia prowadzenia przez inne państwa lub podmioty działań mających na celu

neutralizację lub zniszczenie takich zdolności.

Najważniejsze informacje na ten temat znajdziesz w animacji poniżej.

Wystąpił błąd



Film dostępny pod adresem /preview/resource/Rt27Hf7vO7O8Y

Militarne zagrożenia cyberbezpieczeństwa Polski

Animacja opowiada o zagrożeniach dla cyberbezpieczeństwa Polski.

Polecenie 4

Wyjaśnij, jakie były tradycyjne domeny konfliktów zbrojnych, a jakie pojawiły się współcześnie.

Polecenie 5

Opisz, na czym polega wojna hybrydowa.

Polecenie 6

Wyjaśnij, w jaki sposób niektóre elementy konfliktów asymetrycznych stały się częścią walki w cyberprzestrzeni.

Na czele Wojsk Obrony Cyberprzestrzeni stoi Dowódca Komponentu Wojsk Obrony Cyberprzestrzeni.

Zgodnie z *Ustawą o obronie Ojczyzny*[1] podlega on:

- Ministrowi Obrony Narodowej do czasu mianowania Naczelnego Dowódcy Sił Zbrojnych;
- Naczelnemu Dowódcy Sił Zbrojnych z chwilą jego mianowania i przejęcia przez niego dowodzenia Siłami Zbrojnymi.

Wojska Obrony Cyberprzestrzeni gen. bryg. Karol Molenda
Źródło: Leszek Chemperek/CO MON, licencja: CC BY 3.0.

Do kompetencji Dowódcy Wojsk Obrony Cyberprzestrzeni[1] należy:

- realizacja programu rozwoju Sił Zbrojnych;
- programowanie, planowanie, organizowanie, prowadzenie oraz nadzorowanie prowadzenia szkoleń będących we właściwości Dowódcy Komponentu Wojsk Obrony Cyberprzestrzeni na rzecz podległych jednostek wojskowych i związków organizacyjnych, komórek organizacyjnych i jednostek organizacyjnych, a także instytucji, organów i podmiotów, na podstawie zawartych porozumień;

- planowanie oraz organizowanie mobilizacyjnego i operacyjnego rozwinięcia oraz użycia Wojsk Obrony Cyberprzestrzeni;
- budowa, utrzymanie oraz ochrona infrastruktury, a także ochrona informacji w cyberprzestrzeni;
- prowadzenie działań i operacji w cyberprzestrzeni;
- zapewnienie wsparcia operacji militarnych prowadzonych przez Siły Zbrojne oraz operacji w układzie sojuszniczym i koalicyjnym;
- współpraca z innymi organami i podmiotami w sprawach związanych z obronnością państwa;
- zarządzanie i przeprowadzanie kontroli podległych jednostek wojskowych i związków organizacyjnych.

Wykonuje on swoje zadania za pośrednictwem Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni.[1]

Prezydent USA Barack Obama oraz Prezydent Polski Andrzej Duda udzielają wywiadu na szczycie NATO w Warszawie, Polska 8 lipca 2016 roku.
Źródło: Ash Carter, domena publiczna.

Wraz z rozwojem nowoczesnych technologii, cyberbezpieczeństwo staje się coraz istotniejszym tematem na forum NATO. Podczas szczytu w Warszawie w 2016 roku,

Sojusz uznał cyberprzestrzeń za czwartą domenę prowadzenia działań bojowych. Cyberprzestrzeń jest jednym z obszarów prowadzenia walki, dlatego NATO aby reagować na „znaczące wrogie cyberdziałania" zbuduje zdolności do szybkiego reagowania na tego typu zagrożenia. W nowej koncepcji strategicznej NATO wskazano że „pojedyncze lub skumulowane złośliwe działania w cyberprzestrzeni (...) mogą osiągnąć poziom ataku zbrojnego i tym samym skłonić Radę Północnoatlantycką do powołania się na art. 5 Traktatu Północnoatlantyckiego". Artykuł 5 Traktatu NATO stanowi, że: „Strony zgadzają się, że zbrojna napaść na jedną lub kilka z nich w Europie lub Ameryce Północnej będzie uważana za napaść przeciwko nim wszystkim. Obecnie NATO wkłada wiele wysiłku, aby zabezpieczyć swoje systemy i sieci oraz pomóc sojusznikom w zwiększeniu ich zdolności do skutecznej cyberobrony."

3. Podsumowanie

- Cyberbezpieczeństwo to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.
- Podniesienie poziomu odporności na cyberzagrożenia prowadzone jest zarówno wymiarze cywilnym, jak i wojskowym.
- Cyberzagrożenia dotyczą zarówno osób prywatnych, jak i podmiotów gospodarczych oraz instytucji państwowych.
- Cyberprzestrzeń jest jedną z nowych domen konfliktów zbrojnych - obok lądowej, morskiej, powietrznej.
- W 2022 roku powstał w Polsce komponent Wojsk Obrony Cyberprzestrzeni.

4. Słownik

cyberbezpieczeństwo

odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy

infrastruktura krytyczna

należy przez to rozumieć systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej; przykłady to: systemy łączności, teleinformatyczne, finansowe, zaopatrzenia w żywność i wodę, ochrony zdrowia

krajowy system cyberbezpieczeństwa

krajowy system cyberbezpieczeństwa ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów

wojna hybrydowa

wojna tocząca się na wielu płaszczyznach i w różnych domenach; często nie jest formalnie wypowiedziana i nie występuje konfrontacja kinetyczna, czyli fizyczne starcie wrogich wojsk; zamiast tego mogą występować np. prowokacje, zamieszki, akty dywersji

5. Zadania

Ćwiczenie 1

Ćwiczenie 2

Ćwiczenie 3

Ćwiczenie 4

Ćwiczenie 5

Ćwiczenie 6

Ćwiczenie 7

Scharakteryzuj rolę i miejsce cyberbezpieczeństwa militarnego w systemie cyberbezpieczeństwa państwa.

Ćwiczenie 8

Wykaż zagrożenia związane z pozyskaniem przez cyberprzestępców poufnych informacji z baz danych.

6. Notatnik

7. Bibliografia

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, dostępny w internecie: https://www.dziennikustaw.gov.pl/M2019000103701.pdf [dostęp dn. 30.06.2022].

Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny, dostępny w internecie: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20220000655 [dostęp dn. 30.06.2022].

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, dostępny w internecie: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20070890590 [dostęp dn. 30.06.2022].

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, dostępny w internecie: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/U/D20181560Lj.pdf [dostęp dn. 30.06.2022].