CYBER.MIL.PL

2019

CYBER.MIL.PL

Szanowni Państwo,

cyberprzestrzeń stanowi coraz istotniejszą dziedzinę funkcjonowania współczesnych państw i społeczeństw. Zagwarantowanie bezpieczeństwa sieci teleinformatycznych i zasobów informacyjnych jest jednym z priorytetów naszego rządu. Mamy bowiem pełną świadomość, że obok tradycyjnych domen operacyjnych, cyberprzestrzeń jest miejscem, w którym z taką samą dbałością trzeba pamiętać o bezpieczeństwie państwa i obywateli.

Program CYBER.MIL.PL, który uruchomiliśmy na początku 2019 roku, jest próbą kompleksowej odpowiedzi na aktualne zagrożenia. Budujemy zdolności, które pomogą nam skutecznie radzić sobie w tym środowisku. Z jednej strony integrujemy i wzmacniamy funkcjonujące już instytucje, z drugiej sięgamy po coraz nowsze rozwiązania i potencjał, jakim dysponuje polska nauka i technika. Kierujemy się przy tym zasadą, że inwestycje w wyspecjalizowane kadry są równie ważne, jak inwestycje w nowe technologie. Dzięki temu tworzymy nową jakość, a nasz program stanowi impuls do rozwoju nauki w obszarze cyber.

Rozumiejąc wagę wyzwania, z jakim się mierzymy, budujemy nowoczesne wojska obrony cyberprzestrzeni oraz wspieramy młodzież, która kształci się w specjalnie powołanym liceum informatycznym i na wojskowych uczelniach. Działając tu i teraz, myślimy jednocześnie o przyszłości. Potencjał, który tworzymy, ma nam zapewnić bezpieczeństwo w nadchodzących dekadach. Koordynacja pracy różnych instytucji oraz tworzenie zaplecza personalnego i technicznego to główne filary, na których opiera się budowany w ramach programu CYBER.MIL.PL system bezpieczeństwa w cyberprzestrzeni.

Mariusz Błaszczak, Minister Obrony Narodowej

Szanowni Państwo,

w 2018 roku podjęliśmy w MON zadanie związane z opracowaniem i wdrożeniem kompleksowego programu ukierunkowanego na rozbudowę zdolności Sił Zbrojnych RP i resortu obrony narodowej do działania w cyberprzestrzeni, ustanowionej przez NATO domeną operacyjną działań militarnych. Dziś – niemal rok po uruchomieniu programu CYBER.MIL.PL – możemy potwierdzić, że stał się on efektywną platformą, na której budujemy narodowe zdolności bezpieczeństwa cyberprzestrzeni. Składa się na to szerokie spektrum działań, począwszy od budowania silnych instytucji, przede wszystkim poprzez integrowanie rozproszonego potencjału, przez tworzenie wojsk obrony cyberprzestrzeni i inspirowanie świata nauki do poszukiwania nowatorskich rozwiązań, aż do kształcenia przyszłych kadr.

Rok funkcjonowania programu przyniósł m.in. zatwierdzenie koncepcji funkcjonowania wojsk obrony cyberprzestrzeni, wzrost nakładów finansowych na rozwiązania cyber i krypto, utworzenie elitarnego Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni, sformowanie Zespołu Działań Cyberprzestrzennych w Wojskach Obrony Terytorialnej, znaczne rozszerzenie wojskowej oferty edukacyjnej – od nowej szkoły średniej i podoficerskiej, przez zwiększone limity przyjęć na studia, aż po nowe kierunki, w tym prestiżowe studia MBA oraz wzmocnienie pozycji Polski na arenie międzynarodowej. Przede wszystkim jednak obszar cyberbezpieczeństwa został objęty odpowiednimi działaniami, których głównym celem jest wzrost bezpieczeństwa Polski i Polaków.

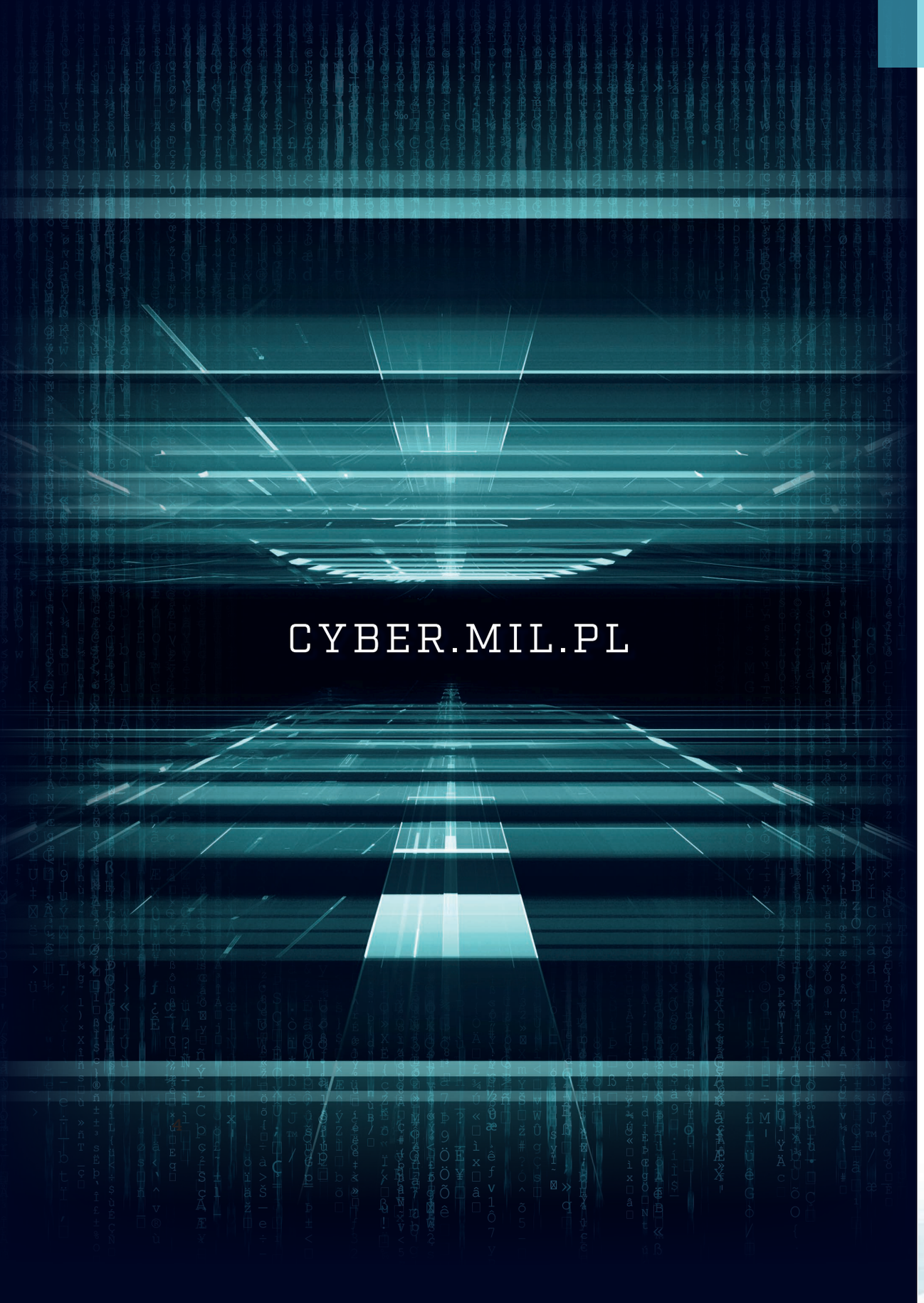
Tylko kompleksowe podejście, projekty realizowane równolegle na wielu polach, mają szansę powodzenia w tak złożonym i dynamicznie zmieniającym się środowisku. Cieszy, że zarówno sam program CYBER.MIL.PL, jak i inne podejmowane inicjatywy spotykają się z tak dużym odzewem i zainteresowaniem. Stanowi to dla nas dodatkowy impuls do działania i systematycznej rozbudowy tego kluczowego dla bezpieczeństwa narodowego naszego kraju programu. Zarówno chwalebne tradycje związane z dokonaniami polskich kryptologów czy spuścizną lwowskiej szkoły matematycznej, jak i obecne sukcesy naszych ekspertów, zaliczanych do światowej elity różnych obszarów informatyki, predestynują Polskę do odgrywania wiodącej roli w sojuszniczych wysiłkach mających na celu bezpieczeństwo cyberprzestrzeni.

Tomasz Zdzikot
Sekretarz Stanu w MON
Pełnomocnik Ministra Obrony Narodowej
do spraw Bezpieczeństwa Cyberprzestrzeni

CYBER.MIL.PL

2019

MINISTERSTWO OBRONY NARODOWEJ



CYBER.MIL.PL to program realizowany przez Ministerstwo Obrony Narodowej, którego głównym zadaniem jest zwiększenie bezpieczeństwa państwa i obywateli w cyberprzestrzeni.

CYBER.MIL.PL Jaki jest nasz cel?

- **konsolidacja i budowa struktur cyberbezpieczeństwa,**
- **edukacja, szkolenia i treningi,**
- **współpraca i budowanie silnej pozycji międzynarodowej,**
- **podniesienie poziomu bezpieczeństwa resortowych i wojskowych sieci oraz systemów.**

W lutym 2019 roku Mariusz Błaszczak, minister obrony narodowej, zainaugurował program CYBER.MIL.PL. To szereg zaplanowanych działań, które pozwolą m.in. na utworzenie nowego rodzaju wojsk – Wojsk Obrony Cyberprzestrzeni, wykształcenie najlepszych specjalistów zajmujących się informatyką i kryptologią, którzy zasilą Siły Zbrojne RP, oraz zwiększenie budżetu na realizację zadań w obszarze kryptologii, cyberbezpieczeństwa oraz rozwoju i utrzymania sieci teleinformatycznych. Przede wszystkim to program, który zwiększy bezpieczeństwo Polski i Polaków w cyberprzestrzeni.

Co udało nam się zrobić?

1. Konsolidacja i budowanie struktur cyberbezpieczeństwa

Stworzyliśmy podstawy prawne, które pozwoliły skutecznie koordynować działania związane z konsolidacją prac w obszarze cyberbezpieczeństwa. Powołaliśmy Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni, którym został wiceminister Tomasz Zdzikot. Powstał również stały Zespół Pełnomocnika MON ds. bezpieczeństwa cyberprzestrzeni.

1 lipca 2019 r. utworzyliśmy specjalistyczną jednostkę - Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni (NCBC). Centrum powstało na bazie Inspektoratu Informatyki i Narodowego Centrum Kryptologii.

NCBC to największe w Polsce centrum kompetencyjne, odpowiadające za kluczowe obszary związane z konsolidacją uprawnień i zasobów resortu obrony narodowej w zakresie kryptologii i cyberbezpieczeństwa oraz funkcjonowania systemów teleinformatycznych.

Minister Obrony Narodowej zatwierdził we wrześniu 2019 r. *Koncepcję organizacji i funkcjonowania wojsk obrony cyberprzestrzeni*, które będą nowym rodzajem wojsk. Do końca 2022 r. powstanie dowództwo wojsk obrony cyberprzestrzeni (WOC), a do końca 2024 r. WOC osiągną gotowość do działania. Koncepcja została opracowana przez gen. bryg. Karola Molendę, dyrektora Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni oraz Pełnomocnika MON ds. utworzenia wojsk obrony cyberprzestrzeni.

W Wojskach Obrony Terytorialnej uruchomiliśmy komponent „cyber". W jego skład wejdzie w I etapie ponad 100-osobowy Zespół Działań Cyberprzestrzennych. Jest to oferta skierowana do osób, które chcą kontynuować karierę zawodową na rynku cywilnym i jednocześnie służyć na rzecz bezpieczeństwa Polaków w cyberprzestrzeni.

Prowadzimy prace legislacyjne w sprawie nadania Wojskowemu Instytutowi Łączności statusu państwowego instytutu badawczego.

Formujemy Inspektorat Łączności, który pozwoli na konsolidację potencjału łączności polowej (mobilnej).

W dokumencie „Priorytetowe kierunki badań na lata 2017-2026" wyróżniliśmy obszar kryptologii i cyberbezpieczeństwa, co pozwoli na finansowanie ze środków MON projektów badawczych na rzecz rozwoju i pozyskania nowych technologii w obszarze cyber.

W ramach Planu Modernizacji Technicznej na lata 2020-2035 przeznaczymy ok. 10 mld złotych na realizację zadań w obszarach kryptologii, cyberbezpieczeństwa oraz rozwoju i utrzymania sieci teleinformatycznych.

2. Edukacja, szkolenie i trening

Konsekwentnie zwiększamy limity przyjęć na uczelniach wojskowych (Wojskowa Akademia Techniczna i Akademia Marynarki Wojennej) na kierunkach związanych z bezpieczeństwem informacyjnym: elektronika i telekomunikacja, informatyka, kryptologia i cyberbezpieczeństwo, systemy informacyjne w bezpieczeństwie. Na samą kryptologię i cyberbezpieczeństwo limit wzrósł aż siedmiokrotnie. W ciągu najbliższych pięciu lat mury uczelni wojskowych opuści łącznie około 2 tys. oficerów w specjalnościach związanych z cyberbezpieczeństwem.

W Akademii Wojsk Lądowych prowadzone są prace nad uruchomieniem siedmiosemestralnych studiów inżynierskich na kierunku informatyka. W inauguracyjnym roku akademickim 2020/21 zaplanowaliśmy przyjęcie 30 osób.

1 września 2019 r., przy Wojskowej Akademii Technicznej, rozpoczęło działalność Wojskowe Ogólnokształcące Liceum Informatyczne (WOLI). Aktualnie w dwóch klasach uczy się po 25 uczniów. O jedno miejsce ubiegało się ponad 10 kandydatów.

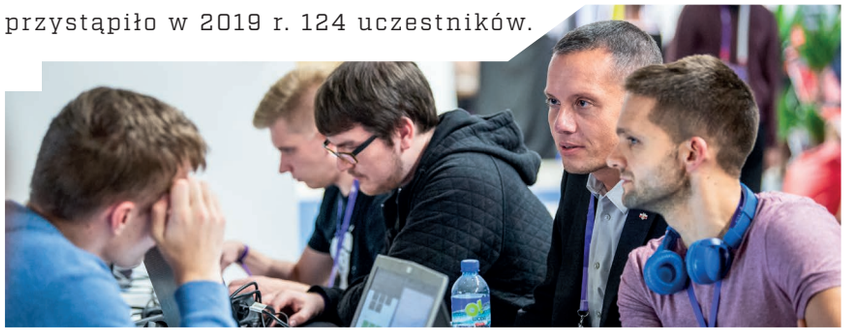
Osoby kończące liceum będą przygotowane do podjęcia studiów na kierunkach takich jak informatyka, kryptologia i cyberbezpieczeństwo. W trakcie nauki uczniowie mają zapewnione bezpłatne: zakwaterowanie, wyżywienie, opiekę medyczną oraz umundurowanie.

W październiku 2019 r. na Wojskowej Akademii Technicznej ruszyły pierwsze w Polsce studia MBA z zakresu zarządzania cyberbezpieczeństwem. Dwusemestralne studia będą prowadzone w języku polskim i angielskim we współpracy z Uniwersytetem w Genui (Włochy).

W semestrze letnim roku akademickiego 2019/20 uruchomimy dwuletnie studia MBA w Akademii Marynarki Wojennej o profilu „zarządzanie bezpieczeństwem" z uwzględnieniem obszaru cyberbezpieczeństwa.

1 października 2019 r. utworzyliśmy Szkołę Podoficerską SONDA w Zegrzu i Toruniu. Wykształci się w niej rocznie 600 kandydatów na podoficerów w zakresie łączności i informatyki (Zegrze) oraz podoficerów Wojsk Obrony Terytorialnej o specjalności piechota (Toruń).

Resort obrony narodowej w latach 2018 i 2019 r. był partnerem Hack Yeah! – największego stacjonarnego hackathonu w Europie. Do zadania MON w kategorii „Cybersecurity" przystąpiło w 2019 r. 124 uczestników.



Ponadto w 2019 r. Polska była gospodarzem konkursu projektowo-programistycznego NATO TIDE Hackathon, organizowanego przez Dowództwo Sił Sojuszniczych NATO ds. Transformacji (ACT). W rywalizacji wzięło udział 13 zespołów reprezentujących instytucje wojskowe, środowiska akademickie oraz firmy komercyjne z 11 państw. W dwóch z trzech kategorii zwyciężyli przedstawiciele resortu obrony narodowej.

W ćwiczeniach LOCKED SHIELDS 2019 zespół z Polski zajął 6. miejsce. Prowadzone przez NATO Cooperative Cyber Defence Centre of Excellence coroczne ćwiczenia były największym i najbardziej zaawansowanym technicznie międzynarodowym przedsięwzięciem z zakresu obrony teleinformatycznej na świecie. W 2019 roku wzięło w nim udział ponad 550 osób z 26 państw sojuszniczych.

CYBER.MIL.PL

W lutym 2019 r. przeprowadziliśmy szkolenie w zakresie cyberbezpieczeństwa dla około 100 przedstawicieli sektora obronnego. Jego celem było wzmocnienie odporności na potencjalne ataki, takie jak np. phishing.

W czerwcu 2019 r. zorganizowaliśmy IV Letnią Szkołę Cyberbezpieczeństwa. Przedsięwzięcie realizowane przez MON ma na celu podniesienie świadomości nowych zagrożeń oraz promowanie debaty w obszarze cyberbezpieczeństwa.

We wrześniu 2019 przeprowadziliśmy specjalistyczne szkolenie dla personelu placówek medycznych, które uznano za operatorów usług kluczowych.

Opracowaliśmy koncepcję programu „**CYBER.MIL z klasą**". Dzięki niemu w każdym województwie zostanie utworzona jedna klasa o profilu cyberbezpieczeństwo i nowoczesne technologie informatyczne. Już od 1 września 2019 r. ruszyła pilotażowa edycja w I Liceum Ogólnokształcącym im. Józefa Chełmońskiego w Łowiczu.

W Centrum Badań nad Bezpieczeństwem w Akademii Sztuki Wojennej tworzymy ośrodek badawczy - Centrum Studiów nad Cyberbezpieczeństwem.

Już wkrótce na portalu internetowym Biblioteki Głównej Akademii Sztuki Wojennej wystartuje cyfrowa biblioteka cyberbezpieczeństwa.

Akademia Sztuki Wojennej rozpoczęła wydawanie nowego czasopisma naukowego, tematycznie związanego z cyberbezpieczeństwem.

Rozszerzyliśmy program ochotniczego szkolenia wojskowego dla studentów „**Legia Akademicka**" o zajęcia dotyczące cyberbezpieczeństwa. Program skierowany jest do cywilnych studentów i umożliwia zdobycie statusu podoficera lub oficera rezerwy.

CYBER.MIL.PL

3. Współpraca i budowa silnej pozycji międzynarodowej Polski

W listopadzie 2018 r. Polska dołączyła do projektu PESCO CRRTs. Celem projektu jest utworzenie Zespołów Szybkiego Reagowania z zakresu Cyber (Cyber Rapid Response Teams) w ramach stałej współpracy strukturalnej na poziomie Unii Europejskiej.

4 lipca 2019 r. Tomasz Zdzikot, sekretarz stanu w MON, podpisał Memorandum of Understanding (MoU) między Rządem RP a NATO, dotyczące współpracy w obszarze obrony cyberprzestrzeni. Celem umowy jest określenie podstaw prawnych i ram współpracy w obszarze cyberobrony między Polską i Sojuszem Północnoatlantyckim.

26 czerwca 2019 r. podpisane zostało polsko-amerykańskie porozumienie o współpracy w cyberprzestrzeni. Umowa pozwoli m.in. na organizację wspólnych ćwiczeń oraz szerszą wymianę doświadczeń.

Przedstawiciele resortu obrony narodowej biorą aktywny udział w najważniejszych konferencjach, targach i innych międzynarodowych eventach dotyczących cyberbezpieczeństwa.

Polskie doświadczenia związane ze zwiększaniem bezpieczeństwa w cyberprzestrzeni prezentowano podczas międzynarodowych forów i konferencji:

CYBERSEC – 8-9 X 2018, Kraków;
Atlantic Council's Poland Cyber Security Conference – 16-17 I 2019, Warszawa;
CYBERSEC Leaders' Foresight – 20 II 2019, Bruksela;
CYBERSEC Leaders' Foresight – 19 III 2019, Waszyngton;
Seoul Defence Dialogue – 4-7 IX 2019, Seul;
The Best Way to Predict the Future is to Create it – 26-27 IX 2019, Waszyngton;
NIAS'19 – 15-17 X 2019, Mons;
CYBERSEC – 29-30 X 2019, Katowice;
CYBER COMMANDERS FORUM – 24-25 IX 2019, Garmisch-Partenkirchen.

Polska będzie pełniła funkcję gospodarza międzynarodowego Cyber Commanders Forum w 2021 r. To prestiżowe wydarzenie skupia dowódców odpowiedzialnych za bezpieczeństwo w obszarze cyberprzestrzeni w siłach zbrojnych wielu krajów.

28 października 2019 r. Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni wspólnie z NATO Communications & Information Agency (NCIA) po raz drugi zorganizowało konferencję Polish Defence IT Industry Day.

4. Podnoszenie poziomu bezpieczeństwa resortowych i wojskowych sieci oraz systemów

W listopadzie 2019 r. wprowadzono w resorcie obrony narodowej uregulowania dotyczące organizacji i funkcjonowania systemu cyberbezpieczeństwa. Wiązało się to m.in. z potrzebą dostosowania przepisów obowiązujących w resorcie do postanowień ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Ustawa nakłada na MON szereg zadań, w tym organizację i utrzymanie zespołu reagowania na incydenty bezpieczeństwa teleinformatycznego – CSIRT MON oraz Narodowego Punktu Kontaktowego do współpracy z Organizacją Traktatu Północnoatlantyckiego.

W ramach stałego podnoszenia poziomu bezpieczeństwa resortowych i wojskowych systemów teleinformatycznych prowadzimy prace nad:

- opracowaniem narzędzi do bezpiecznej komunikacji w resorcie obrony narodowej;
- opracowaniem oraz wprowadzeniem do użytku e-szyfratorów pracujących w standardzie NINE;
- budową nowych pod względem konfiguracji i rozwiązań technicznych ogólnoresortowych sieci IT;
- rozbudową resortowych laboratoriów do badania nośników danych, oprogramowania złośliwego malware'u oraz ruchu sieciowego;
- opracowaniem nowego systemu monitoringu zagrożeń oraz wykrywania incydentów w resortowych systemach IT.

CYBER.MIL.PL

MINISTERSTWO OBRONY NARODOWEJ

2019

WWW.CYBER.MIL.PL

MINISTERSTWO OBRONY NARODOWEJ