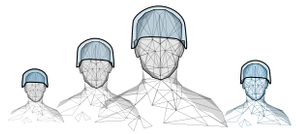

Podsumowanie programu CYBER.MIL.PL
2019-2021
CBC



CYBER.MIL.PL to program realizowany przez Ministerstwo Obrony Narodowej w latach 2019–2021. Jego głównym zadaniem jest zwiększenie bezpieczeństwa w cyberprzestrzeni poprzez szeroko zakrojone działania, które realizowane są w ramach czterech filarów:

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

Działania podejmowane w ramach programu CYBER.MIL.PL są realizowane w ramach intensywnej współpracy pomiędzy Narodowym Centrum Bezpieczeństwa Cyberprzestrzeni, Służbą Kontrwywiadu Wojskowego, Dowództwem Wojsk Obrony Terytorialnej, Wojskowym Instytutem Łączności oraz wojskowymi uczelniami i jednostkami szkoleniowym, czyli wszystkimi podmiotami realizującymi program Ministra Obrony Narodowej.

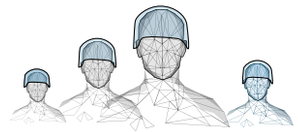
CYBER.MIL.PL

1. KONSOLIDACJA I BUDOWA STRUKTUR CYBERBEZPIECZEŃSTWA

2. EDUKACJA, SZKOLENIA, TRENINGI

3. WSPÓŁPRACA I BUDOWA SILNEJ POZYCJI MIĘDZYNARODOWEJ

4. PODNIESIENIE POZIOMU BEZPIECZEŃSTWA RESORTOWYCH I WOJSKOWYCH SIECI ORAZ SYSTEMÓW



CYBER.MIL.PL w 2019 roku

Pierwszy rok funkcjonowania Programu, to okres planowania i projektowania działań oraz rozpoczęcie tworzenia nowych struktur związanych z cyberbezpieczeństwem.

Przez trzy lata funkcjonowania Programu CYBER.MIL.PL konsekwentnie zwiększane były 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.

Budowa silnych struktur odpowiedzialnych za cyberbezpieczeństwo wiąże się z ciągłym doskonaleniem umiejętności i zdobywaniem nowej wiedzy przez żołnierzy i pracowników resortu obrony narodowej, którzy podnoszą swoje kompetencje biorąc udział w licznych szkoleniach, konferencjach i ćwiczeniach, zarówno krajowych jak i międzynarodowych.

Pierwszy rok funkcjonowania programu Cyber.mil.pl to prace koncepcyjne niezbędne do rozpoczęcia dużych projektów takich jak „CYBER.MIL z klasą”, otwarcie pierwszych studiów MBA

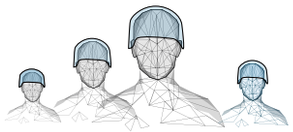
z zakresu cyberbezpieczeństwa i rozpoczęcie prac zmierzających do uruchomienia kolejnych studiów tego typu.

Podpisane zostały pierwsze porozumienia dwustronne, Polska zaangażowała się w jeden z największych projektów, do których należy PESCO CRRTs (Cyber Rapid Response Teams) w ramach stałej współpracy Unii Europejskiej.

1. KONSOLIDACJA I BUDOWA STRUKTUR CYBERBEZPIECZEŃSTWA

Jedną z pierwszych decyzji **Ministra Obrony Narodowej Mariusza Błaszczaka** było powołanie **Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni**, którym został ówczesny wiceminister Obrony Narodowej – **Tomasz Zdzikot, który opracował program CYBER.MIL.PL.**

Początek realizacji programu CYBER.MIL.PL, to powołanie przez Ministra Obrony Narodowej **pułkownika Karola Molendy**



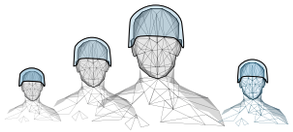
na stanowisko Pełnomocnika Ministra Obrony Narodowej ds. utworzenia Wojsk Obrony Cyberprzestrzeni.

Został on zobowiązany do opracowania koncepcji utworzenia WOC, która to po opracowaniu została zatwierdzona przez Ministra Obrony Narodowej Mariusza Błaszczaka, dzięki czemu proces formowania WOC został rozpoczęty.

Jednocześnie dokonano konsolidacji zasobów i struktur. Utworzono nową specjalistyczną jednostkę odpowiedzialną za bezpieczeństwo wojskowych systemów informatycznych. Na bazie Narodowego Centrum Kryptologi i Inspektoratu Informatyki powstało **Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni z gen. bryg. Karolem Molendą na czele.**

NCBC kontynuuje najlepsze tradycje polskich kryptologów nie tylko poprzez swoją codzienną działalność, kultywuje także pamięć o ich dokonaniach poprzez przyjęcie imienia Jerzego Witolda Różyckiego.

W Wojskach Obrony Terytorialnej został utworzony Zespół Działań Cyberprzestrzennych. Docelowo w późniejszym czasie i jego członkowie będą działać w samodzielnych zespołach przy Brygadach WOT.



2. EDUKACJA, SZKOLENIA, TRENINGI

 # Wojskowe Ogólnokształcące Liceum Informatyczne przy Wojskowej Akademii Technicznej rozpoczęło działanie 1 września 2019 roku. W pierwszym roku uruchomione zostały dwie klasy liczące po 25 uczniów. O jedno miejsce ubiegało się ponad 10 kandydatów!

 # Na Wojskowej Akademii Technicznej zostały w październiku 2019 uruchomione **pierwsze w Polsce studia MBA** z zakresu zarządzania cyberbezpieczeństwem.

 # Październik 2019 roku to również miesiąc uruchomienia Szkoły Podoficerskiej SONDA w Zegrzu i Toruniu. Kształci ona podoficerów w zakresie łączności i informatyki (Zegrze) oraz podoficerów Wojsk Obrony Terytorialnej i specjalności piechota (Toruń).

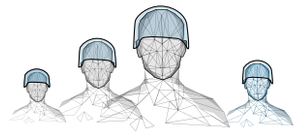
 # Resort obrony narodowej był w 2019 roku partnerem Hack Yeah! – największego stacjonarnego hackathonu w Europie. Polska była też gospodarzem konkursu projektowo-programistycznego NATO TIDE Hackathon organizowanego przez Dowództwo Sił Sojuszniczych NATO ds. Transformacji (ACT). W dwóch z trzech kategorii zwyciężyli przedstawiciele resortu obrony narodowej.

 # Została opracowana koncepcja programu MON „CYBER. MIL z klasą” przewidująca utworzenie w każdym województwie jednej klasy o profilu cyberbezpieczeństwo i nowoczesne technologie informatyczne. Szkoły biorące udział w programie otrzymają wsparcie finansowe z MON na zakup sprzętu, oprogramowania i wynagrodzenie nauczycieli. MON finansuje 80% poniesionych wydatków.
Pilotażowa edycja programu ruszyła w I Liceum Ogólnokształcącym im. Józefa Chełmońskiego w Łowiczu.

 # Po raz pierwszy został ogłoszony konkurs o Nagrodę im. Mariana Rejewskiego za najlepszą pracę inżynierską, licencjacką, magisterską i rozprawę doktorską poświęconą kryptologii, cyberobronie, cyberbezpieczeństwu oraz zwalczaniu cyberprzestępczości. Jego kolejne edycje, skupione wokół cyberbezpieczeństwa i kryptologii, miały miejsce w kolejnych latach.

3. WSPÓŁPRACA I BUDOWA SILNEJ POZYCJI MIĘDZYNARODOWEJ

 # Polski zespół ekspertów zdobył 6. miejsce w ćwiczeniach LOCKED SHIELDS 2019. Prowadzone przez NATO Cooperative Cyber Defence Centre of Excellence, jest to coroczne najwięk-



sze i najbardziej zaawansowane technicznie międzynarodowe przedsięwzięcie z zakresu obrony teleinformatycznej na świecie.

 # W lipcu podpisane zostało Memorandum of Understanding między Rządem RP a NATO. Umowa dotyczy współpracy w obszarze obrony cyberprzestrzeni. Jej celem jest określenie podstaw prawnych i ram współpracy.

 # W listopadzie Polska dołączyła do projektu PESCO CRRTs. Wówczas celem projektu było utworzenie zespołu Szybkiego Reagowania z zakresu cyber.

 # Podpisane polsko-amerykańskie porozumienie o współpracy w cyberprzestrzeni otworzyło drogę do organizacji wspólnych ćwiczeń i szerszej wymiany informacji.

4. PODNOSZENIE POZIOMU BEZPIECZEŃSTWA RESORTOWYCH I WOJSKOWYCH SIECI ORAZ SYSTEMÓW

Czwarty filar programu Cyber.mil.pl to działania, których celem jest podnoszenie poziomu bezpieczeństwa resortowych i wojskowych sieci oraz systemów teleinformatycznych.

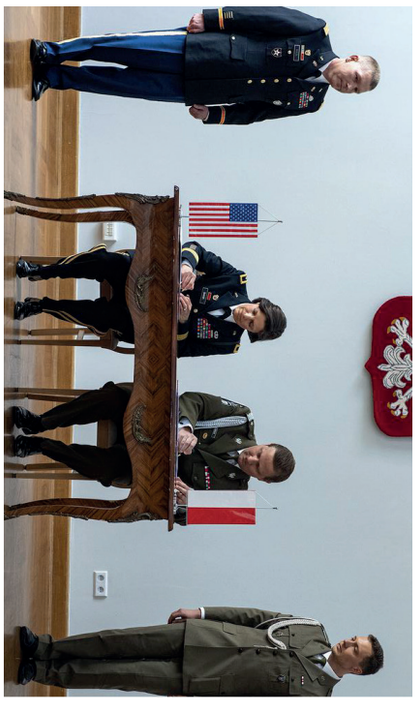
Centrum, odpowiadając za informatyzację Sił Zbrojnych RP, projektuje, implementuje i wdraża szereg rozwiązań technologicznych, które są ukierunkowane na dostarczanie funkcjonalności przy jednoczesnym zachowaniu wysokiego poziomu bezpieczeństwa użytkowania.

 # W listopadzie wprowadzono w resorcie obrony narodowej uregulowania dotyczące organizacji i funkcjonowania systemu cyberbezpieczeństwa. Wiązało się to m.in. z potrzebą dostosowania obowiązujących w resorcie przepisów wykonawczych do ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa. Ustawa nakłada na MON szereg zadań, w tym organizację i utrzymanie Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego – CSIRT MON oraz Narodowego Punktu Kontaktowego do współpracy z Organizacją Traktatu Północnoatlantyckiego.

 # Prowadzone były prace nad uruchomieniem postępowań na pozyskanie urządzeń kryptograficznych zgodnych ze standardami NATO.

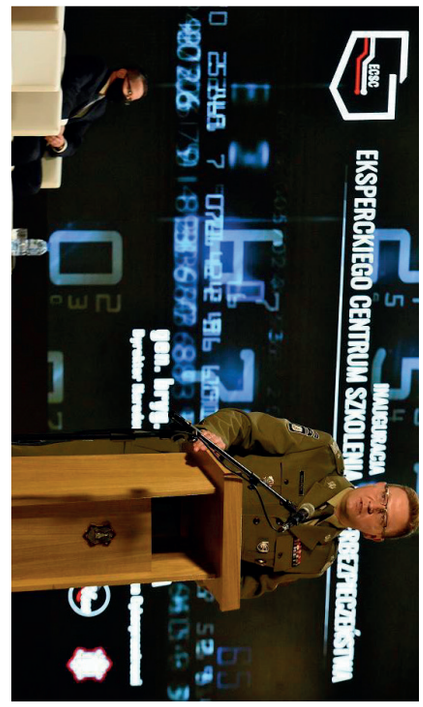
.

WWW.CYBER.MIL.PL



2019-2021

WWW.CYBER.MIL.PL



2019-2021

CYBER.MIL.PL w 2020 roku

Drugi rok funkcjonowania programu CYBER.MIL.PL to kolejne działania mające na celu dalszą konsolidację struktur i pozyskanie ekspertów do służby i pracy w strukturach odpowiedzialnych za zapewnienie cyberbezpieczeństwa.

Kontynuowane były prace koncepcyjne dla największych projektów, pandemia wymusiła nowe działania i postawiła wyzwania związane z zapewnieniem bezpieczeństwa w rzeczywistości, w której znaczna część aktywności przeniosła się do sieci. Rok 2020 przyniósł też kolejne wyróżnienia polskich drużyn w międzynarodowych konkursach i ćwiczeniach.

1. KONSOLIDACJA I BUDOWA STRUKTUR CYBERBEZPIECZEŃSTWA

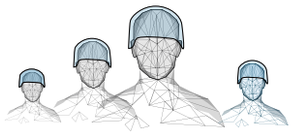
 # W kwietniu 2020 roku w ramach rozbudowy struktur państwowych z zakresu cyberbezpieczeństwa decyzjami Premiera Mateusza Morawieckiego oraz Ministra Obrony Narodowej Mariusz Błaszczaka zostali powołani nowi pełnomocnicy rządu oraz MON z zakresu cyberbezpieczeństwa.

Pełnomocnikiem Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni został Maciej Materka, Szef Służby Kontrwywiadu Wojskowego.

 # Rekrutacja do Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni, które jest odpowiedzialne za formowanie Wojsk Obrony Cyberprzestrzeni, prowadzona jest przy wykorzystaniu nowoczesnych, elektronicznych narzędzi komunikacyjnych takich jak Twitter, Facebook, Messenger, LinkedIn i Skype. Procedury związane z rekrutacją i zatrudnieniem zostały skrócone i uproszczone, by proces pozyskiwania nowych pracowników był szybki i zarazem efektywny

 # NCBC uruchomiło pierwszą w resorcie infolinię rekrutacyjną. Pod numerem 509-677-777 przez pięć dni w tygodniu, w dni robocze w godzinach między 8.00 a 20.00 rekruterzy NCBC odpowiadają na pytania dotyczące możliwości podjęcia pracy i służby w strukturach Centrum.

 # Opracowano rozporządzenie MON w sprawie dodatków do uposażenia zasadniczego żołnierzy zawodowych, które przyznało żołnierzom służącym w NCBC, Centrum Operacji Cybernetycznych (COC) oraz Centrum Projektów Informatycznych (CPI) w obszarze cyberbezpieczeństwa, kryptologii lub projektowania i programowania miesięczny dodatek



w wysokości od 450 do 2100 zł. Po przesłużeniu roku kalendarzowego na danym stanowisku otrzymują oni jednorazowy dodatek w wysokości od 100% do nawet 620% kwoty miesięcznego dodatku stałego otrzymanego w grudniu danego roku.

Powołane zostało **Biuro ds. Programu Zostań Żołnierzem Rzeczypospolitej z gen. bryg. Arturem Dębczakiem** na czele. NCBC wraz z Terenowymi Organami Administracji Wojskowej: Wojewódzkimi Sztabami Wojskowymi i Wojskowymi Komendami Uzupełnień opracowało wspólną strategię działań rekrutacyjnych do struktur cyber.

 # Uruchomiony został Resortowy Portal Rekrutacyjny pod adresem https://zostanzolnierzem.pl/. Głównym zadaniem portalu jest zapewnienie wsparcia informatycznego podczas rekrutacji do służby wojskowej. Każdy, kto chce się zgłosić do Wojska Polskiego może dokonać rejestracji na portalu, a następnie zostanie poinformowany jakie są kolejne etapy rekrutacji.

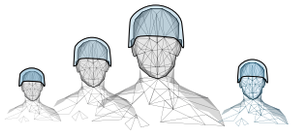
 # Od marca 2020 wpływ na działania podejmowane w obszarze cyberprzestrzeni wywarła pandemia, która zmusiła nas do przeorganizowania naszej pracy i służby oraz wypracowania szeregu nowych rozwiązań. Współpraca NCBC i Rządowego Centrum Bezpieczeństwa polegała na zapewnieniu funkcjonowania oprogramowania **GisCOVID-19**, które pozwala na szybsze i bardziej precyzyjne reagowanie na rozwój sytuacji związanej z COVID-19. Rolą NCBC było udostępnienie RCB infrastruktury teleinformatycznej oraz zapewnienie wsparcia eksperckiego do jej prawidłowego funkcjonowania.

2. EDUKACJA, SZKOLENIA, TRENINGI

 # Programiści z WAT w styczniu 2020 roku, w trakcie regionalnych rozgrywek konkursu Microsoft Imagine Cup 2020 opracowali projekt MONICA – wizualnego asystenta dla osób niewidomych zintegrowanego z inteligentnymi okularami i odpowiadającego na żądania użytkowników za pomocą poleceń głosowych. Jego celem jest ułatwienie codziennego życia osobom niewidomym i niedowidzącym.

Podchorążowie WAT oddelegowani do służby w Dowództwie Wojsk Obrony Terytorialnej opracowali mobilną aplikację ułatwiającą dotarcie z pomocą do osób pozostających w izolacji w związku z rozprzestrzenianiem się koronawirusa.

 # Hackathon „HackYeah 2020" przyniósł zwycięstwo drużynie z Wojskowej Akademii Technicznej. Programiści WAT stworzyli aplikację „Ścieżka weterana", która wskazuje weteranom miejsca, gdzie otrzymają oni zniżki, np. w sklepach lub restauracjach, aby następnie dodać takie miejsce do mapy.



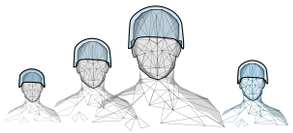
 # NCBC i WAT podjęły w marcu 2020 r. decyzję o zaangażowaniu podchorążych z Wydziału Cybernetyki WAT w bieżące działania Centrum z uwagi na ogłoszony w kraju stan epidemii i związane z tym czasowe zawieszenie zajęć dydaktycznych. Podchorążowie odbywali praktyki online, zostali zaangażowani w prace dotyczące wsparcia teleinformatycznego RON polegające m.in. na przygotowaniu procedur, obsłudze linii wsparcia pracowników RON pracujących zdalnie oraz przygotowywali materiały edukacyjne i szkoleniowe do platformy e-learningowej.

 # Działalność rozpoczęło Eksperckie Centrum Szkolenia Cyberbezpieczeństwa (ECSC). Instytucja podporządkowana MON za pośrednictwem NCBC rozpoczęła funkcjonowanie w listopadzie 2020 roku. ECSC jest odpowiedzialne za przygotowanie i przeprowadzenie skrojonych na miarę potrzeb resortu obrony narodowej szkoleń z zakresu bezpieczeństwa w cyberprzestrzeni. Jest poligonem żołnierzy broniących polską cyberprzestrzeń, na którym mogą trenować i doskonalić swoje umiejętności z wykorzystaniem specjalnego wojskowego cyfrowego poligonu Cyber Range.

Decyzją Ministra Obrony Narodowej z dnia 18 sierpnia 2021 r. patronem Eksperckiego Centrum Szkolenia Cyberbezpieczeństwa został profesor Zdzisław Krygowski, wybitny polski naukowiec. Był on wykładowcą, nauczycielem, promotorem i inspiracją dla wielu młodych matematyków. Zorganizował potajemny kurs kryptografii dla swoich ponad dwudziestu najlepszych studentów i współpracowników. Z tej grupy uzdolnionej młodzieży rekrutowali się znani wszystkim Marian Rejewski, Jerzy W. Różycki i Henryk Zygalski, którzy złamali szyfr Enigmy.

 # Morskie Centrum Cyberbezpieczeństwa zostało otwarte we wrześniu 2020 roku przez Akademię Marynarki Wojennej w Gdyni. To ośrodek analityczno-ekspercki zajmujący się prowadzeniem badań naukowych i eksperckich oraz cyklicznych szkoleń, a także koordynowaniem współpracy oraz wspomaganiem działań w obszarze cyberbezpieczeństwa, w szczególności związanego z obszarem morskim i kosmicznym, na potrzeby resortu obrony narodowej, w tym kadry kierowniczej oraz innych podmiotów działających na rzecz cyberbezpieczeństwa Rzeczypospolitej Polskiej.

 # Akademickie Centrum Polityki Cyberbezpieczeństwa to think tank, który powstał w strukturach Akademii Sztuki Wojennej. Ośrodek koncentruje się na przygotowywaniu opracowań analitycznych raportów i rekomendacji w zakresie cyberbezpieczeństwa, ze szczególnym uwzględnieniem aspektów prawnych, na potrzeby resortu obrony narodowej oraz innych podmiotów działających na rzecz cyberbezpieczeństwa Rzeczypospolitej Polskiej.



Centrum tworzą cztery jednostki organizacyjne: Ośrodek Organizacji i Analiz Prawnych, Ośrodek Strategii Cyberbezpieczeństwa i Edukacji, Ośrodek Implementacji Nowoczesnej Technologii Cyberbezpieczeństwa oraz Laboratorium Bezpieczeństwa Informacji.

 # W kolejną fazę wszedł program Ministra Obrony Narodowej „CYBER.MIL z klasą”. Opracowana została podstawa programowa, wybranych zostało 16 szkół, które zakwalifikowały się do programu – w każdym województwie jest to jedna szkoła średnia. Aby zostać przyjętą do programu, szkoła musiała spełnić szereg kryteriów formalnych, m.in. prowadzić działalność dydaktyczno-wychowawczą w dziedzinie obronności państwa wpisaną w statut szkoły, posiadać klasy realizujące program matematyki i informatyki lub matematyki i fizyki na poziomie rozszerzonym, uzyskać właściwą średnią wyników egzaminu maturalnego z matematyki w ciągu ostatnich trzech lat.

3. WSPÓŁPRACA I BUDOWA SILNEJ POZYCJI MIĘDZYNARODOWEJ

#hackathony #programiści w akcji – zespół jednostki podporządkowanej NCBC – Centrum Projektów Informatycznych wygrał NATO TIDE Hackathon. Odniesiony na początku 2020 roku sukces był trzecim z rzędu na koncie naszych ekspertów w tym prestiżowym i wymagającym konkursie. Podczas tej samej edycji, w innej konkurencji studenci z Wydziału Cybernetyki Wojskowej Akademii Technicznej zajęli trzecie miejsce.

 # W styczniu Tomasz Zdzikot, podsekretarz stanu w Ministerstwie Obrony Narodowej, podpisał porozumienie o współpracy (MoU) w obszarze cyberbezpieczeństwa z resortem obrony Republiki Korei Południowej.

 # W marcu 2020 PESCO formalnie rozpoczęło działalność – podpisane zostało porozumienie o współpracy, tym razem z szefami resortów obrony: Chorwacji, Estonii, Litwy, Holandii i Rumunii, dotyczące przystąpienia do projektu Cyber Rapid Response Teams, czyli międzynarodowych zespołów szybkiego reagowania na incydenty komputerowe. Dokument określa założenia oraz zasady użycia zespołów w sytuacji zagrożeń w cyberprzestrzeni.

 # Porozumienie o współpracy w zakresie obrony cyberprzestrzeni z Izraelem zostało podpisane w grudniu. Jest podstawą do nawiązania współpracy pomiędzy NCBC a Zarządem J6 Cyberobrony, której celem jest wymiana doświadczeń i informacji o zagrożeniach, wspólne szkolenia oraz współpraca w oparciu

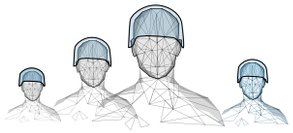
o grupy robocze, szkolenia i edukację oraz rozmowy w obszarze planowania operacji.

4. PODNOSZENIE POZIOMU BEZPIECZEŃSTWA RESORTOWYCH I WOJSKOWYCH SIECI ORAZ SYSTEMÓW

Pandemia i przeniesienie znacznej części realizowanych zadań do cyberprzestrzeni sprawia, że prace związane z nowymi rozwiązaniami podnoszącymi bezpieczeństwo zostały znacznie przyspieszone i zintensyfikowane.

Konsolidując zdolności Wojska Polskiego, zintegrowano możliwość monitorowania systemów teleinformatycznych. W chwili obecnej zdolności w tym obszarze zapewniane są w sposób scentralizowany przez ekspertów NCBC.

Zakończona została modernizacja podkładowej sieci transmisyjnej IP RON przez wymianę newralgicznych urządzeń sieciowych, podnosząc tym samym bezpieczeństwo, efektywność i niezawodność systemów teleinformatycznych. W oparciu o tę modernizację technologiczną resort uzyskał nowe zdolności telekomunikacyjne, kluczowe w okresie pandemii do zapewnienia ciągłości działania jednostek, instytucji i organizacji.

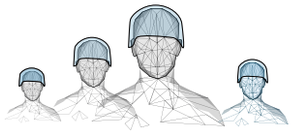


CYBER.MIL.PL w 2021 roku

Trzeci rok funkcjonowania programu to okres wytężonej pracy związanej z ostatnim etapem formowania Wojsk Obrony Cyberprzestrzeni i zapewnienia merytorycznego wsparcia MON dla działań polegających na zapewnieniu bezpieczeństwa w cyberprzestrzeni.

To też rok kolejnych sukcesów Polski na arenie międzynarodowej, ugruntowanie naszej pozycji ekspertów, organizacja jednej z najważniejszych konferencji, jaką był szczyt Warsaw Cyber Summit z warsztatami CSIRT Workshop, czy otwarcie nowych centrów kompetencyjnych.

Podpisane zostały kolejne umowy dwustronne wieńczące wielomiesięczne rozmowy oraz rozpoczęło się jedno z największych wyzwań – koordynacja zespołu PESCO CRRT.
Eksperci resortu obrony narodowej kontynuowali prace nad opracowaniem narzędzi do bezpiecznej komunikacji i nad budową nowych, pod względem konfiguracji i rozwiązań technicznych, ogólnoresortowych sieci IT.



1. KONSOLIDACJA I BUDOWA STRUKTUR CYBERBEZPIECZEŃSTWA

 # Powołano nowego Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni, którym została **Aneta Trojanowska,** Dyrektor Departamentu Cyberbezpieczeństwa w strukturze MON. DC to nowa komórka organizacyjna utworzona zgodnie z Zarządzeniem nr 69/MON Ministra Obrony Narodowej z dnia 20 września 2021 r. Do zadań DC MON należy m.in. projektowanie rozwiązań systemowych w obszarze cyberbezpieczeństwa, w tym udział w wypracowywaniu projektów aktów prawnych na szczeblu rządowym, koordynowanie realizacji zadań związanych z wdrażaniem polityki krajowej i międzynarodowej resortu w obszarze cyberbezpieczeństwa.

Fot. Leszek Chemperek

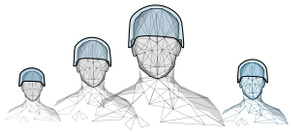
Partnerska kooperacja w obszarze cyberbezpieczeństwa pomiędzy NCBC, a DC MON wynika bezpoeśrednio z obszarów funkcjonowania tych instytucji.

 # Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni – Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni zaczęło formalnie funkcjonować z dniem 1 stycznia 2022 roku. NCBC – DK WOC powstało na bazie NCBC i dwóch Jednostek Bezpośrednio Podporządkowanych Centrum (Centrum Operacji Cybernetycznych i Centrum Projektów Informatycznych). Z ostatnim dniem grudnia 2021 roku swoją działalność zakończyło Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni w kształcie, w jakim instytucja funkcjonowała od 2019 roku.

2. EDUKACJA, SZKOLENIA, TRENINGI

 # Legia Akademicka (program ochotniczego kształcenia studentów uczelni cywilnych) rozpoczęła kształcenie w ramach modułu cyber szkolenia oficerskiego. Uzupełnia ono realizowane w ubiegłych latach szkolenie z zakresu cyber w ramach modułu podoficerskiego.

 # Rok 2021 to podpisanie umów o współpracy z trzema uczelniami wojskowymi i trzema cywilnymi w ramach Programu Cyfrowych Ambasadorów NCBC. Funkcja Ambasadora powierzana jest wyróżniającym się na uczelniach osobowościom, studentom osiągającym doskonałe wyniki w nauczaniu i będącym pasjonatami wiedzy praktycznej. Ich celem jest propagowanie wiedzy związanej z krypto, cyber i IT oraz budowanie w środowisku akademickim świadomości, jakie możliwości rozwoju i pracy daje służba i praca w NCBC.



W pierwszym pełnym roku funkcjonowania programu pełnienie funkcji Cyfrowego Ambasadora NCBC rozpoczęło czternastu studentów z uczelni zarówno wojskowych, jak i cywilnych.

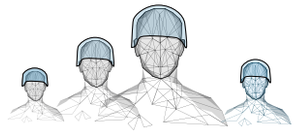
 # Program „CYBER.MIL z klasą" wszedł w kolejną fazę – we wrześniu 2021 roku uczniowie szesnastu szkół rozpoczęli naukę w nowo utworzonych klasach o profilu „Cyberbezpieczeństwo i nowoczesne technologie informatyczne". Program nauczania obejmuje m.in. informatykę na poziomie rozszerzonym oraz przedmioty, takie jak kryptografia, algorytmika, cyberbezpieczeństwo i zarządzanie bezpieczeństwem danych i informacji. Nadzór merytoryczny nad realizacją programu sprawuje Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni przy wsparciu Wojskowej Akademii Technicznej. Eksperci NCBC opracowali projekt ramowego eksperymentalnego planu nauczania oraz programu nauczania przedmiotów specjalistycznych.

 # Na Akademii Marynarki Wojennej zainaugurowano studia Executive MBA z zakresu zarządzania cyberbezpieczeństwem i usługami cyfrowymi.

Podczas dwóch semestrów studiów słuchacze zdobywają wiedzę i umiejętności z zakresu ekonomii i finansów, prawnych aspektów zarządzania usługami kluczowymi, zarządzania cyberbezpieczeństwem, nowoczesnych technologii oraz skutecznych metod zarządzania projektami i usługami.

Główny nacisk jest kładziony na umiejętność identyfikacji potencjalnych ryzyk oraz organizacji pracy tak, by zminimalizować skutki lub prawdopodobieństwo wystąpienia zagrożenia.

 # Zespół Działań Cyberprzestrzennych funkcjonujący w ramach Dowództwa Wojsk Obrony Terytorialnej zorganizował szkolenia dotyczące cyberbezpieczeństwa dla samorządów i gmin objętych stanem wyjątkowym. Były one realizowane w ramach operacji WOT „Silne wsparcie". Zakres szkolenia obejmował zagrożenia w cyberprzestrzeni, z uwzględnieniem mediów społecznościowych i bezpieczeństwa systemów teleinformatycznych. Równolegle zostały przeprowadzone warsztaty dla informatyków z samorządów, obejmujące monitoring i doradztwo w zakresie zabezpieczenia systemów teleinformatycznych.



3. WSPÓŁPRACA I BUDOWA SILNEJ POZYCJI MIĘDZYNARODOWEJ

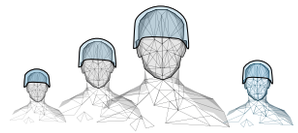
 # Konferencja EU MilCERT Interoperability Conference (MIC21) została w 2021 roku po raz pierwszy wzbogacona o odbywające się na cyberpoligonie ćwiczenie, w którym udział wzięły wojskowe Zespoły Reagowania na Incydenty Komputerowe z osiemnastu krajów europejskich. Polski zespół, w którego skład weszli m.in. eksperci NCBC, zajął drugie miejsce.

 # Locked Shields 2021 było jednym z największych sukcesów polskiej drużyny w ćwiczeniach organizowanych przez Sojusz Północnoatlantycki – zespół dowodzony przez oficera z NCBC zajął 4 miejsce w finalnej klasyfikacji tych największych światowych ćwiczeń z zakresu cyber.

 # Polska przejęła funkcję koordynatora dla unijnego Zespołu Szybkiego Reagowania w Cyberprzestrzeni w projekcie PESCO Cyber Rapid Response Team and Mutual Assistance in Cyberspace. Zadanie to zostało powierzone NCBC na 12 miesięcy (licząc od marca 2021). Jednym z najważniejszych wydarzeń była organizacja ćwiczenia Alarmex, w które zaangażowanych było 11 specjalistów w zakresie cyberbezpieczeństwa z 5 krajów. Zgodnie ze scenariuszem ćwiczeń, strony internetowe Ministerstwa Spraw Zagranicznych Rzeczypospolitej Polskiej, Ambasady Królestwa Niderlandów w Warszawie i Wilnie padły ofiarą ataku cybernetycznego. Atakujący umieścili na nich fałszywe treści mające na celu destabilizację sytuacji politycznej w Europie. W 48 godzin zespół, którego liderem był oficer CSIRT MON, zidentyfikował skompromitowane urządzenia, ustalił funkcjonalności szkodliwego oprogramowania oraz ścieżki jego rozprzestrzeniania się. Ustalił wskaźniki kompromitacji oraz wydał zalecenia pozwalające na przywrócenie możliwości bezpiecznego użytkowania usług IT.

 # Podpisane porozumienia bilateralne z Łotwą i Estonią uregulowały zakres współpracy wojskowych zespołów reagowania na incydenty bezpieczeństwa komputerowego.

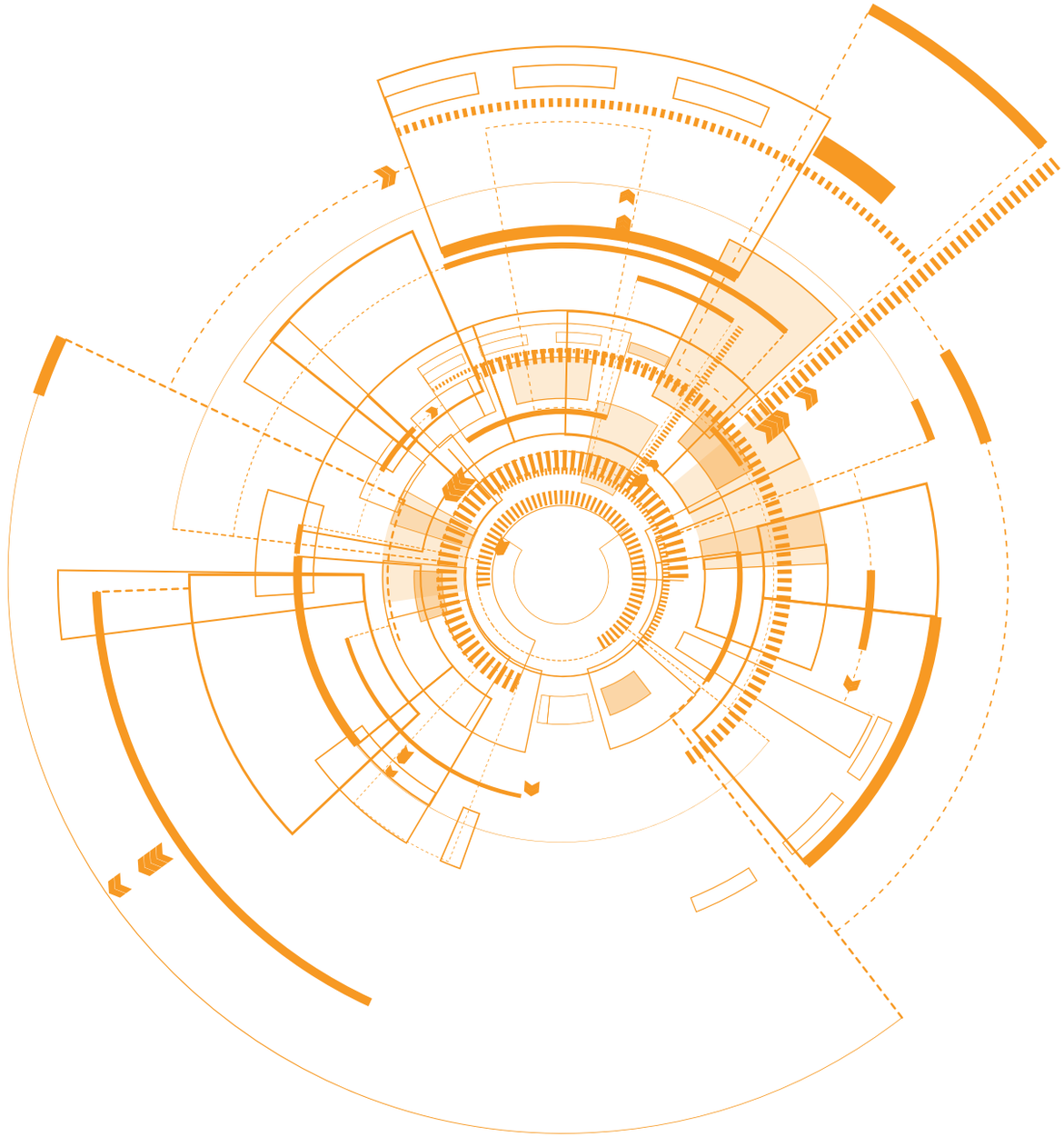
Zgodnie z podpisanymi w ubiegłych latach porozumieniami polscy eksperci do spraw cyberbezpieczeństwa szkolili się na izraelskich cyberpoligonach.



4. PODNOSZENIE POZIOMU BEZPIECZEŃSTWA RESORTOWYCH I WOJSKOWYCH SIECI ORAZ SYSTEMÓW

 # Uzyskano certyfikat ochrony kryptograficznej dla urządzenia IP Krypto 2 (produkcji WIŁ-PIB)

 # Przeprowadzona została migracja Poczty Elektronicznej Zimbra (ron.mil.pl) do systemu Poczty Elektronicznej MS Exchange Milnet-I (mon.gov.pl). Centralizacja usługi poczty wyrównała poziom dostępu do wysokiej jakości środowiska pracy oraz podniosła komfort i bezpieczeństwo korzystania z poczty elektronicznej w resorcie obrony narodowej.



NARODOWE CENTRUM BEZPIECZEŃSTWA CYBERPRZESTRZENI


AI
NARODOWE CENTRUM BEZPIECZEŃSTWA CYBERPRZESTRZENI