podsumowanie 2020

CYBER.MIL.PL

Szanowni Państwo,

We współczesnym świecie cyberprzestrzeń jest jednym z najważniejszych obszarów funkcjonowania państwa i zarazem obszarem, który wymaga od nas ogromnej atencji. Obrona cyberprzestrzeni należy także do podstawowych zadań kolektywnej obrony NATO.

By zapewnić skuteczną ochronę naszych obywateli w środowisku cyfrowym niezbędne są zdecydowane działania podnoszące poziom bezpieczeństwa w cyberprzestrzeni. Takie właśnie działania kolejny już rok podejmuje Ministerstwo Obrony Narodowej realizując program CYBER.MIL.PL.

Mariusz Błaszczak,
Minister Obrony Narodowej

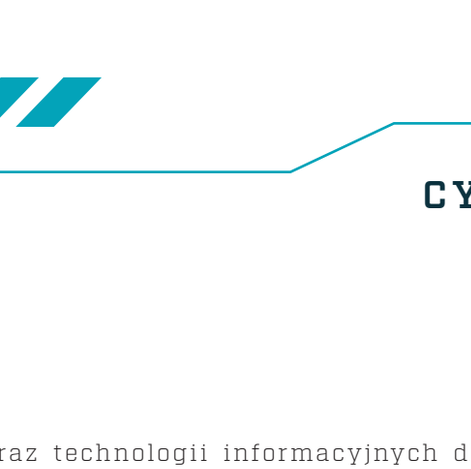
CYBER.MIL.PL

W ramach programu CYBER.MIL.PL powstają Wojska Obrony Cyberprzestrzeni oraz rozwijane są zdolności resortu obrony narodowej w zakresie cyberbezpieczeństwa. W tym niezwykle trudnym czasie walki z pandemią koronawirusa szczególną dumą napawa mnie fakt bardzo szybkiej i trafnej reakcji Wojska Polskiego na aktualne potrzeby. To w szeregach Sił Zbrojnych powstały narzędzia zwiększające bezpieczeństwo epidemiologiczne użytkowników, takie jak: aplikacja H.E.L.P., czy też internetowa platforma wsparcia samorządów, organów sanitarnych i podmiotów leczniczych https://pomocwot.ron.mil.pl.

Program CYBER.MIL.PL to przede wszystkim ludzie – najwyższej klasy eksperci. Ich wyszkolenie i przygotowanie jest dla mnie priorytetem. W tym celu, w ramach programu CYBER.MIL.PL w 2020 r. zrealizowano i rozwijano wiele nowych inicjatyw, w tym nowoczesne narzędzia rekrutacyjne, program dla szkół średnich „CYBER.MIL z klasą", a w szczególności otwarcie Eksperckiego Centrum Szkolenia Cyberbezpieczeństwa, podległej mi instytucji odpowiedzialnej za specjalistyczne szkolenia z zakresu cyberbezpieczeństwa,

kryptologii oraz technologii informacyjnych dla ekspertów z resortu obrony narodowej na potrzeby tworzonych Wojsk Obrony Cyberprzestrzeni.

Program CYBER.MIL.PL to przełomowa zmiana zdolności Sił Zbrojnych RP. Każdy dzień realizacji tego programu zwiększa bezpieczeństwo Polski w cyberprzestrzeni. Wszystkie nasze działania zmierzają do tego, by już w 2024 roku Wojska Obrony Cyberprzestrzeni osiągnęły gotowość do działań operacyjnych.



Cyberprzestrzeń jest jednym z najdynamiczniej rozwijających się obszarów, który stawia przed nami największe wyzwania. Nie tylko operacyjnie, ale też pod kątem przygotowania infrastruktury pozwalającej zapewnić maksymalny poziom bezpieczeństwa.

Rok 2020 postawił przed nami ambitne zadania, których nie byliśmy w stanie przewidzieć. W tym zmieniającym się środowisku bieżąca realizacja zadań stanowiła wyzwanie, któremu udało się nam sprostać.

Kontynuujemy wzmacnianie i podnoszenie bezpieczeństwa resortowych sieci teleinformatycznych, by dostosować je do coraz to nowych pojawiających się zagrożeń.

Nasze działania kierujemy na to, by infrastruktura teleinformatyczna resortu obrony narodowej była coraz bardziej wydajna i coraz bezpieczniejsza. Naszą siłą są ludzie, którzy pracują nad coraz nowocześniejszymi rozwiązaniami zapewniającymi maksymalny poziom bezpieczeństwa.

gen. bryg. MACIEJ MATERKA
Pełnomocnik Ministra Obrony Narodowej
ds. bezpieczeństwa cyberprzestrzeni

CYBER.MIL.PL

2020

gen. bryg. Karol Molenda,
Dyrektor Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni,
Pełnomocnik MON do spraw utworzenia Wojsk Obrony Cyberprzestrzeni

Cyberprzestrzeń to obszar, w którym każdego dnia przychodzi nam mierzyć się z nowymi wyzwaniami. Zadaniem Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni jako jednego z filarów programu CYBER.MIL.PL jest codzienna praca nad podnoszeniem poziomu bezpieczeństwa Polski i Polaków w wirtualnym świecie.

Mimo tego, że pandemia kazała nam już po pierwszym kwartale ubiegłego roku zweryfikować nasze plany, najważniejszym zadaniem do realizacji niezmiennie pozostała budowa Wojsk Obrony Cyberprzestrzeni. Już do końca 2024 roku ten nowy rodzaj wojsk, których bronią i tarczą będzie wiedza i nowoczesna technologia, ma osiągnąć pełną zdolność operacyjną. Cała społeczność NCBC oraz jednostek podporządkowanych robi wszystko, aby to przedsięwzięcie zakończyło się oczekiwanym sukcesem.

Dlatego też rok 2020 upłynął nam pod znakiem doskonalenia umiejętności z zakresu cyberbezpieczeństwa, kryptologii i IT, a także znacznej rozbudowy zespołów działających w Centrum. Z myślą o przyszłych kadrach, NCBC podjęło zakrojoną na szeroką skalę współpracę z wojskowymi i cywilnymi uczelniami wyższymi poprzez uruchomienie Programu Cyfrowych

Ambsadorów NCBC. W ten sposób docieramy do uczelnianych prymusów i entuzjastów, aby zarysować im wizję służby i pracy w naszej - jedynej w swoim rodzaju - eksperckiej cyber-jednostce MON.

Mając na uwadze potrzeby całego Wojska Polskiego skupiliśmy wysiłki na rozbudowie infrastruktury, co zaowocowało otwarciem nowoczesnych budynków Centrum Obliczeniowo-Projektowego i Projektowo - Konstrukcyjnego.

W ostatecznym kształcie działa w NCBC zespół CSIRT MON, który w trybie ciągłym reaguje na występujące incydenty komputerowe i zapewnia bezpieczeństwo resortu w cyberprzestrzeni.

Realizowany przez nas program CYBER.MIL.PL to także budowanie silnej pozycji na arenie międzynarodowej, dlatego już dziś możemy z dumą powiedzieć, że jesteśmy „Silni w Sojuszach".

Rok 2021 to kolejne wyzwania, które systematycznie przybliżą nas do powstania Wojsk Obrony Cyberprzestrzeni, przede wszystkim również intensywna rekrutacja żołnierzy i pracowników oraz doskonalenie umiejętności i kompetencji tych, którzy już na co dzień bronią naszej cyberprzestrzeni.

Bezpieczeństwo czwartej domeny operacyjnej, jaką jest cyberprzestrzeń, to nasz cel i zadanie, które codziennie realizujemy siłą naszych ekspertów oraz przy nieustannie rozbudowywanym wsparciu Partnerów i Sojuszników.

1. KONSOLIDACJA I BUDOWA STRUKTUR CYBERBEZPIECZEŃSTWA

2. EDUKACJA, SZKOLENIE, TRENINGI

3. WSPÓŁPRACA I BUDOWA SILNEJ POZYCJI MIĘDZYNARODOWEJ

4. PODNOSZENIE POZIOMU BEZPIECZEŃSTWA RESORTOWYCH I WOJSKOWYCH SIECI ORAZ SYSTEMÓW

Jaki jest nasz cel?

CYBER.MIL.PL jest programem realizowanym przez Ministerstwo Obrony Narodowej, którego głównym zadaniem jest zwiększenie bezpieczeństwa w cyberprzestrzeni. Działania mające to na celu realizowane są w ramach czterech filarów:

- **Konsolidacja i budowa struktur cyberbezpieczeństwa,**
- **Edukacja, szkolenia i treningi,**
- **Współpraca i budowa silnej pozycji międzynarodowej,**
- **Podnoszenie poziomu bezpieczeństwa resortowych i wojskowych sieci oraz systemów.**

Podejmowane w ramach CYBER.MIL.PL działania w kierunku konsolidacji posiadanych zasobów, intensyfikacji badań naukowych i rekrutacji są realizowane w ramach intensywnej współpracy Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni ze Służbą Kontrwywiadu Wojskowego, Dowództwem Wojsk Obrony Terytorialnej, Wojskowym Instytu-

tem Łączności oraz wojskowymi uczelniami i jednostkami szkoleniowym, czyli wszystkimi podmiotami realizującymi program Ministra Obrony Narodowej.

Rok 2020 był drugim rokiem realizacji programu, którego nadrzędnym celem jest zapewnienie bezpieczeństwa Polsce i Polakom w cyberprzestrzeni.

Co udało nam się zrealizować w 2020 r.?

1.

Konsolidacja i budowa struktur cyberbezpieczeństwa

W ramach działań mających na celu konsolidację i budowę struktur związanych z cyberbezpieczeństwem prowadzony jest szereg działań zmierzających do pozyskania i utrzymania w resorcie obrony narodowej najlepszych ekspertów, zarówno żołnierzy jak i pracowników cywilnych.

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.

Praca i służba wojskowa w obszarze cyber, krypto i IT jest doświadczeniem dostępnym dla najlepszych ekspertów w swoich dziedzinach. NCBC daje swoim pracownikom nie tylko możliwość zmierzenia się z unikalnymi wyzwaniami, ale też możliwość kooperacji z najlepszymi specjalistami w kraju, na najnowocześniejszym sprzęcie.

Ważnym aspektem jest również możliwość pracy na rzecz bezpieczeństwa kraju oraz rozwoju osobistego poprzez udział w kursach i szkoleniach, w tym tych niedostępnych na komercyjnym rynku.

#Atrakcyjne wynagrodzenie

W lutym 2020 roku zmienione zostało rozporządzenie MON w sprawie dodatków do uposażenia zasadniczego żołnierzy zawodowych. Nowe regulacje przyznały 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 dodatkowo jednorazowy dodatek w wysokości od 100% do nawet 620% kwoty miesięcznego dodatku stałego otrzymanego w grudniu danego roku.

stały miesięczny dodatek	jednorazowy dodatek roczny za grudzień
od 450 do 2100 zł	od 100% do nawet 620%

Zespołowa rekrutacja

By pozyskać najlepszych specjalistów na rynku, jednostki w resorcie obrony narodowej prowadzą szeroko zakrojone działania rekrutacyjne. Wspólne działania ma ułatwić powołane w styczniu 2020 roku 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.

Pierwsza infolinia rekrutacyjna w resorcie

By ułatwić chętnym do podjęcia pracy w Narodowym Centrum Bezpieczeństwa Cyberprzestrzeni dostęp do informacji na temat zasad i sposobów rekrutacji, NCBC uruchomiło pierwszą w resorcie infolinię rekrutacyjną. Pod numerem 509-677-777, 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.

Rekrutacja online

Rekrutując najlepszych specjalistów na rynku sięgamy po niestandardowe, nowoczesne rozwiązania. We wrześniu 2020 roku NCBC uruchomiło Resortowy Portal Rekrutacyjny pod adresem https://zostanzolnierzem.pl/. Głównym zadaniem

portalu jest zapewnienie wsparcia informatycznego podczas rekrutacji do służby wojskowej. Kto chce się zgłosić do Wojska Polskiego może dokonać rejestracji na portalu, a następnie zostanie poinformowany o kolejnych etapy rekrutacji.

Portal został zbudowany przez specjalistów z Centrum Projektów Informatycznych, pod kierunkiem NCBC we współpracy z CO MON, Biurem ds. Programu Zostań Żołnierzem Rzeczypospolitej, Zarządem Organizacji i Uzupełnień – P1 SG WP oraz Departamentem Kadr.

Jesteśmy na targach i konferencjach

Kolejnym sposobem na dotarcie do potencjalnych nowych pracowników jest prezentowanie się wszystkich członków zespołu CYBER.MIL.PL podczas najważniejszych targów i konferencji z obszarów cyber, krypto i IT.

By dotrzeć do studentów jako przyszłych pracowników, NCBC nawiązało współpracę z miesięcznikiem Głos Akademicki wydawanym przez Wojskową Akademią Techniczną. Publikowane są w nim aktualne informacje z obszaru cyber, krypto i IT.

W obliczu pandemii

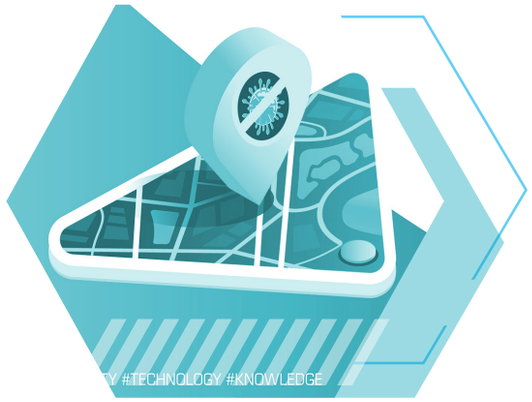
Od marca 2020 wpływ na działania podejmowane w obszarze cyberprzestrzeni wywarła pandemia, która zmusiła nas do przeorganizowania naszej pracy i służby oraz wypracowania szeregu nowych rozwiązań.

Jeszcze w pierwszym kwartale 2020 roku, NCBC i Rządowe Centrum Bezpieczeństwa podpisały porozumienie, w którym zobowiązały się do wspólnego działania w zakresie zwalczania COVID-19 oraz wywołanych pandemią sytuacji kryzysowych. Współpraca obu instytucji polega na zapewnieniu funkcjonowania oprogramowania GisCOVID-19, które pozwala na szybsze i bardziej precyzyjne reagowanie na rozwój sytuacji związanej z COVID-19. Rolą NCBC jest udostępnienie RCB infrastruktury teleinformatycznej oraz zapewnienie wsparcia eksperckiego do jej prawidłowego funkcjonowania.

Ponadto, w ramach walki z Covid – 19 eksperci z NCBC i WAT stworzyli aplikację pod nazwą Health Environment for Living in Pandemia (H.E.L.P.), której celem jest wyszukiwanie osób z koronawirusem znajdujących się w pobliżu i ostrzeganie użytkowników telefonów komórkowych przed niebezpieczeństwem. Aplikacja powstała w ramach #BuildforCOVID19 Global online Hackathon - międzynarodowego przedsięwzięcia zorganizowanego na platformie DEVPOST i wspieranego przez World Health Organization i naukowców z Chan Zuckerberg Biohub.

Pandemia sprawiła, że cześć pracowników resortu obrony narodowej zostało skierowanych do pracy zdalnej. Już w marcu 2020 r. zostało opracowane cyfrowe środowisko pracy dla użytkowników ze struktur resortu obrony narodowej umożliwiające zdalny dostęp do wybranych aplikacji. Rozwiązanie to jest szczególnie istotne w sytuacji światowej walki z pandemią koronawirusa, zapewniając maksimum bezpieczeństwa kadrze i pracownikom RON.

Do walk ze skutkami pandemii już w pierwszym kwartale 2020 roku zostali skierowani podchorążowie z Wojskowej Akademii Technicznej. Zadania dla Wojsk Obrony Terytorial-



nej zaczęli realizować 18 marca, zaraz po decyzji Ministra Obrony Narodowej, na podstawie której komendanci akademii wojskowych przekazali do dyspozycji Dowódcy WOT niezbędne siły i środki. Zakres działań podchorążych WAT obejmował m.in. wsparcie techniczne w zakresie uruchamiania usług zdalnych. Oprócz prac związanych z opracowaniem aplikacji, studenci Wydziału Cybernetyki zaangażowani byli również w zabezpieczenie techniczne całodobowej infolinii wparcia psychologicznego uruchomionej przez Dowództwo WOT przy pomocy NCBC.

#Cyberbezpieczeństwo pod specjalną opieką

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

Pełnomocnikiem Ministra Obrony Narodowej ds. bezpieczeństwa cyberprzestrzeni został gen. bryg.Maciej Materka, Szef Służby Kontrwywiadu Wojskowego.

Pełnomocnikiem rządu ds. cyberbezpieczeństwa został minister cyfryzacji Marek Zagórski, który koordynuje działania i realizuje politykę rządu w zakresie zapewnienia cyberbezpieczeństwa w Rzeczypospolitej Polskiej.

2.

Edukacja, szkolenie i treningi

Budowa silnych struktur odpowiedzialnych za bezpieczeństwo Polski i Polaków w cyberprzestrzeni wiąże się z ciągłym doskonaleniem umiejętności i zdobywaniem nowej wiedzy przez żołnierzy i pracowników resortu obrony narodowej. W minionym roku przedstawiciele NCBC oraz jednostek podporządkowanych (m.in. CPI) brali udział w szeregu szkoleń i konkursów oraz uruchomiliśmy szereg inicjatyw narodowych i międzynarodowych zmierzających do szkolenia potencjalnych przyszłych pracowników resortu obrony narodowej.

#Hackathony - programiści w akcji

Jednym z najlepszych sposobów na sprawdzenie swoich umiejętności jest trening współpracy zespołowej poprzez udział w konkursach programowania. Przedstawiciele MON i instytucji tworzących program CYBER.MIL.PL uczestniczą we wszystkich największych tego typu imprezach i zajmują w nich premiowane miejsca, pracując nad rozwiązaniami podnoszącymi komfort i bezpieczeństwo użytkowników sieci.

Zespół jednostki podporządkowanej NCBC - Centrum Projektów Informatycznych wygrał w 2020 roku NATO TIDE Hackathon. Odniesiony sukces na początku 2020 roku 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. Rywalizacja odbywała się w trzech kategoriach:

- przewidywania kryzysów,
- dynamicznego oznaczania strumieni audio i video,
- ekstrakcji ustrukturyzowanych danych z dokumentów.

Zespół z CPI zwyciężył w kategorii dynamicznego oznaczania strumieni audio i video oraz okazał się najlepszy w całym konkursie.

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.

W listopadzie 2020 zespół studentów WAT zwyciężył w kategorii #Software w hackathonie Best Hacking League organizowanym przez Politechnikę Warszawską. Podczas konkursu zaprezentowali aplikację, która ma przyczynić się do zwalczania i porządkowania nielegalnych wysypisk śmieci.

Drużyna z Wojskowej Akademii Technicznej zwyciężyła również w europejskim hackathonie HackYeah 2020 prezentując aplikację „Ścieżka Weterana", która wskazuje weteranom miejsca, gdzie otrzymają zniżki, np. w sklepach lub restauracjach, aby następnie dodać takie miejsce do mapy. Każdy weteran używając tej aplikacji będzie wiedział, gdzie może otrzymać upust lub skorzystać z innych usług zarezerwowanych dla bohaterów wojennych.

#Cyberterytorialsi w akcji

Miniony rok upłynął pod hasłem doskonalenia umiejętności i sprawdzania się również żołnierzom Wojsk Obrony Terytorialnej. Żołnierze z Zespołu Działań Cyberprzestrzennych WOT brali udział w licznych hackathonach oraz profesjonalnych szkoleniach, zajmując miejsca na podium.

W edycji HackYeah 2020 żołnierze WOT opracowali trzy projekty do trzech zadań - w zadaniu Ministerstwa Rolnictwa i Rozwoju Wsi stworzyli aplikację do prostego i użytecznego zgłaszania obecności dzików, gdyż występująca u nich często choroba ASF (afrykański pomór świń) stanowi zagrożenie dla wielu gospodarstw rolnych w kraju.

W zadaniu przedstawionym przez Bank Gospodarstwa Krajowego opracowali aplikację ChatterBox, która umożliwia swobodny dostęp zarówno do informacji w firmowym intranecie (wewnętrzne zasoby firmy), jak i publicznie dostępnych informacji o BGK.

Trzecim zadaniem było przygotowanie aplikacji mobilnej lub internetowej pomagającej rozwiązać problem zmniejszenia ilości odpadów, a tym samym zapobiegania degradacji środowiska.

Praktyki online

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 zdalnie w trakcie trwania roku akademickiego. Studenci zostali zaangażowani w prace dotyczące wsparcia teleinformatycznego RON polegające m.in.: na przygotowaniu procedur, obsłudze linii wsparcia pracowników RON pracujących zdalnie oraz przygotowywania materiałów edukacyjnych i szkoleniowych do platformy e-learningowej.

#Szkolenia skrojone na miarę

By sprostać wyzwaniu jakim jest konieczność ciągłego doskonalenia umiejętności i zdobywania nowych kompetencji, w listopadzie 2020 roku zostało otwarte Eksperckie Centrum Szkolenia Cyberbezpieczeństwa. To instytucja podporządkowana MON za pośrednictwem NCBC, która ma być odpowiedzialna za przygotowanie i przeprowadzenie skrojonych na miarę potrzeb Resortu Obrony Narodowej szkoleń z zakresu bezpieczeństwa cyberprzestrzeni. ECSC ma być też wyjątkowym obiektem szkoleniowym dla żołnierzy broniących polską cyberprzestrzeń, na którym będą mogli trenować i doskonalić swoje umiejętności w oparciu o dedykowany wojskowy cyfrowy poligon Cyber Range.

Głównym zadaniem ECSC jest prowadzenie szkoleń i ćwiczeń oraz poszerzanie kompetencji SZ RP w zakresie

działań w cyberprzestrzeni. Eksperckie Centrum, podnosząc kwalifikacje żołnierzy i pracowników, będzie pełnić też rolę jednostki do prowadzenia działań w cyberprzestrzeni, a także pełnić rolę jednostki konsolidującej potencjał ekspercki oraz wspierającej Ministerstwo Obrony Narodowej w rozwijaniu współpracy krajowej i międzynarodowej.

Najważniejsze zadania ECSC to:

- kształcenie i szkolenie kadr do działań w cyberprzestrzeni,
- organizacja i prowadzenie ćwiczeń, treningów, gier wojennych z wykorzystaniem zintegrowanego środowiska szkoleniowego (wirtualny poligon - tzw. Cyber Range),
- współpraca z podmiotami krajowymi i zagranicznymi,
- konsolidacja potencjału eksperckiego resortu obrony narodowej - kształtowanie priorytetowych kierunków doskonalenia kadr w sferze cyberbezpieczeństwa, kryptologii oraz IT.

ECSC ma na celu także wyszkolenie kadr pod budowane Wojska Obrony Cyberprzestrzeni, a także przygotowanie i utrzymanie środowiska dla potrzeb prowadzenia procesu certyfikacji personelu i jednostek w ramach tworzenia WOC.

ECSC stanie się w ten sposób jednym z kluczowych ogniw w systemie cyberbezpieczeństwa państwa poprzez szkolenie najwyższej klasy ekspertów, pełniących wiodące role w strukturach odpowiedzialnych za obronę cyberprzestrzeni na wszystkich poziomach dowodzenia SZ RP.

Kilka pierwszych miesięcy działania ECSC przyniosło parę istotnych sukcesów takich jak podpisanie porozumień dotyczących współpracy i szkoleń z Państwową Wyższą Szkołą Zawodową w Wałczu (gdzie jednostka ma oddział zamiejscowy), Akademią Microsoft i Akademią CISCO. Dodatkowo w 2020 r. ECSC uruchomiło 7 nowoczesnych sal szkoleniowych i – mimo funkcjonowania w realiach wynikających z pandemii – przeszkoliło blisko 200 osób: żołnierzy i pracowników cywilnych RON z rónych rodzajów sił zbrojnych (Siły Powietrzne, Marynarka Wojenna, Wojska Lądowe). Szkolenia obejmujące m.in. technologię Palo Alto, przygotowywały uczestników do planowania i wdrażania elementów bezpieczeństwa w systemach teleinformatycznych, przedstawiały też podstawy routingu i przełączania w sieciach komputerowych, Cyber Threat Intelligence (CTI), wielopoziomową analizę zagrożeń, techniczną, behawioralną i kontekstową - zawierającą także analizę typu INFOOPS.

Morskie Centrum Cyberbezpieczeństwa

Akademia Marynarki Wojennej utworzyła we wrześniu 2020 r. Morskie Centrum Cyberbezpieczeństwa (MCC), którego zadaniem będzie prowadzenie badań naukowych i eksperckich, cyklicznych szkoleń. Ponadto Centrum będzie koordynować współpracę oraz wspomagać działania 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.

MCC jest ośrodkiem analityczno-eksperckim prowadzącym badania naukowe, analizy i szkolenia na rzecz Sił Zbrojnych RP, służb, administracji publicznej, przemysłu oraz społeczeństwa. Centrum jest również platformą wymiany wiedzy, doświadczeń oraz dobrych praktyk z zakresu cyberbezpieczeństwa

w wymiarze krajowym oraz międzynarodowym.
Misja MCC wpisuje się w strategię rozwoju Akademii Marynarki Wojennej w obszarach kształcenia i doskonalenia zawodowego, działalności naukowej i badawczej, organizacji i zarządzania oraz inwestycji.

#16 szkół w CYBER.MIL z klasą

Rok 2020 to rok, w którym uruchomiony został program Ministra Obrony Narodowej „CYBER.MIL z klasą". Polega on na utworzeniu i prowadzeniu w szkołach ponadpodstawowych klas o profilu „Cyberbezpieczeństwo i nowoczesne technologie informatyczne". Do udziału w projekcie zakwalifikowanych

zostało 16 szkół w całej Polsce, po jednej w każdym województwie. Program zakłada rozszerzone kształcenie uczniów w zakresie informatyki z uwzględnieniem zagadnień dotyczących cyberbezpieczeństwa, szczególnie w obszarze bezpieczeństwa państwa. Prowadzony będzie przez pierwsze trzy lata nauki, w każdej klasie liczba uczniów nie może być mniejsza niż 10 i nie większa niż 15. Szkoły, które zakwalifikowały się do programu, otrzymają wsparcie finansowe z MON na zakup sprzętu, oprogramowania i wynagrodzenie nauczycieli. MON sfinansuje 80 proc. poniesionych wydatków, resztę stanowić będzie wkład własny beneficjenta.

Głównym celem programu jest wykształcenie potencjalnych kandydatów do korpusów osobowych kadry zawodowej i naukowej RON, w tym szczególnie do tworzonych Wojsk Obrony Cyberprzestrzeni.

#cyberbezpieczny think tank

W strukturach Akademii Sztuki Wojennej 1 czerwca 2020 roku powstał nowy think tank - Akademickie Centrum Polityki Cyberbezpieczeństwa. Zadania realizowane przez ten ośrodek koncentrują się w szczególności 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. ACPC wydaje także czasopismo naukowe, tematycznie związane z cyberprzestrzenią i bezpieczeństwem - półrocznik „Cybersecurity and Law".

#Stawiamy na Cyfrowych Ambasadorów NCBC

W listopadzie 2020 roku uruchomiony został Program Cyfrowych Ambasadorów NCBC. Pierwszą uczelnią, która do niego przystąpiła jest Wojskowa Akademia Techniczna. Rozpoczęte zostały również rozmowy z innymi uczelniami, m.in. UKSW w Warszawie, WSEI w Lublinie i inne, które finalizowane będą w roku 2021 i w kolejnych latach. Program ma na celu budowanie wizerunku NCBC jako atrakcyjnego pracodawcy zarówno dla żołnierzy jak i pracowników RON, m.in.

poprzez swoją działalność na uczelniach, udział w wybranych targach pracy i konferencjach. Od swoich Ambasadorów NCBC oczekuje m.in. zaangażowania w działalność uczelnianych kół naukowych, możliwości udziału w konkursach typu hackhathon pod marką NCBC czy warsztatach oraz działaniach rekrutacyjnych. Rola ambasadora to też szereg benefitów takich jak możliwość udziału w szkoleniach z zakresu cyber, krypto i IT czy też reprezentowania NCBC podczas konferencji i szkoleń. Cyfrowi Ambasadorzy NCBC mają również możliwość odwiedzenia siedziby Centrum oraz zapoznania się z codzienną działalnością instytucji. Funkcjonujące od lat w Polsce i na świecie programy ambasadorskie są uznawane za jedną z najskuteczniejszych metod dotarcia i pozyskania zainteresowania działalnością instytucji przez środowiska akademickie, a także niosą ze sobą liczne korzyści pod względem wizerunkowym oraz rekrutacyjnym.

#Legia Akademicka rośnie w siłę

Komponent cyber realizowany w ramach Legii Akademickiej jest elitarnym szkoleniem specjalistycznym, kierowanym do studentów LA, którzy z sukcesem przeszli dodatkową kwalifikację. We wrześniu 2020 roku, wzorem lat ubiegłych, pod okiem wojskowych specjalistów z Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni w szkoleniu LA z zakresu cyberbezpieczeństwa wzięło udział siedemdziesięciu sześciu najlepszych studentów z całego kraju. To ponad dwukrotnie więcej niż w poprzedniej edycji.

3.

Współpraca i budowa silnej pozycji międzynarodowej Polski

Jednym z filarów, na których opiera się program CYBER.MIL.PL jest rozwijanie współpracy i budowa silnej pozycji Polski w obszarze cyberbezpieczeństwa na arenie międzynarodowej. Taki cel ma zawieranie porozumień w zakresie wymiany doświadczeń oraz współpracy w szeroko rozumianym obszarze cyberbezpieczeństwa oraz udział w międzynarodowych ćwiczeniach z zakresu cyber.

#Partnerzy międzynarodowi

W styczniu 2020 roku Dyrektor Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni podpisał porozumienie o współpracy (Memorandum of Understanding - MoU) w obszarze cyberbezpieczeństwa z resortem obrony Republiki Korei Południowej.

W marcu 2020 zawarto kolejne 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. Program został zainicjowany w 2018 r. w ramach Stałej Współpracy Strukturalnej UE (PESCO). Dokument określa założenia oraz zasady użycia zespołów w sytuacji zagrożeń w cyberprzestrzeni.

Kolejne porozumienie o współpracy w zakresie obrony cyberprzestrzeni podpisane zostało w grudniu 2020 roku ze stroną izraelską. Jego celem jest nawiązanie współpracy pomiędzy NCBC a Zarządem J6 Cyberobrony, czyli wymiana doświadczeń i informacji o zagrożeniach, a także wspólne szkolenie w obszarze cyber. Porozumienie daje możliwość współpracy w oparciu o grupy robocze, szkolenia i edukację oraz rozmowy w obszarze planowania operacji.

CYBER.MIL.PL

Polskie siły dbające o cyberbezpieczeństwo aktywnie uczestniczą w licznych wydarzeniach i ćwiczeniach międzynarodowych. Przykładem takiej aktywności jest udział w kolejnej edycji ćwiczenia NATO Cyber Coalition 2020. Celem ćwiczen było szkolenie żołnierzy w zakresie ich zdolności do obrony sieci NATO i sieci narodowych, testy procesów podejmowania decyzji, procedur technicznych i operacyjnych, a także zdolności NATO w zakresie cyberbezpieczeństwa.

4.

Podnoszenie poziomu bezpieczeństwa resortowych i wojskowych sieci oraz systemów

Czwarty filar programu CYBER.MIL.PL to działania, których celem jest podniesienie 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.

Merkury, czyli bezpieczna komunikacja

Bezpieczna, wieloplatformowa komunikacja staje się kluczowym wymaganiem wielu organizacji, zwłaszcza w zakresie transmisji, ale również i retencji danych (informacji o tym, kto, z kim i kiedy łączył się za pomocą środków komunikacji elektronicznej). Odpowiedzią na tę potrzebę w Resorcie Obrony Narodowej jest zaimplementowany przez NCBC komunikator Merkury, zapewniający bezpieczną komunikację tekstowo-głosową i możliwość bezpiecznego dzielenia się plikami multimedialnymi.

Kluczowym aspektem konstrukcji tego typu rozwiązań jest dostarczenie jak najbardziej funkcjonalnego produktu przy zachowaniu maksymalnego poziomu bezpieczeństwa - od zabezpieczenia wymienianych informacji, po efektywne zarządzanie kontaktami kadry i kluczowego personelu resortu. Wysoki poziom bezpieczeństwa dostarczanej usługi obejmuje zabezpieczenia kryptograficzne, ale przede wszystkim zabezpieczenia wszystkich części składowych systemu takich jak infrastruktura, środowiska serwerowe czy mobilne łącza komunikacyjne.

Priorytetem projektantów było połączenie zrozumiałego oraz intuicyjnego sposobu użytkowania oraz nowoczesnego wyglądu aplikacji oraz zabezpieczenie jej przed niepowołanym dostępem i możliwością przechwycenia treści wrażliwych.

Merkury oferuje również bezpieczny sposób integracji infrastruktury powiadomień platform mobilnych iOS oraz Android, wykorzystując responsywność komunikatów przy jednoczesnym ukryciu notyfikowanych treści.

Nowe rozwiązania

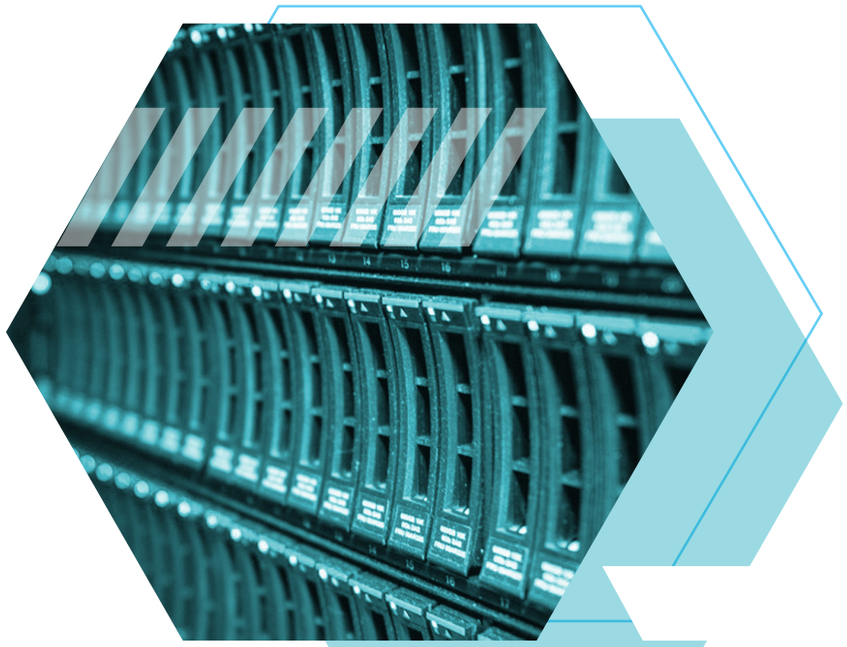
W ramach podnoszenia poziomu bezpieczeństwa systemów teleinformatycznych w ubiegłym roku opracowane zostało studium wykonalności oraz wstępne założenia taktyczno – techniczne dla systemu ochrony kryptograficznej nowej generacji w technologiach NINE i SCIP. Wnioski w sprawie pozyskania ww. sprzętu wojskowego zostały zatwierdzone w marcu br. i obecnie rozpoczęta została procedura ich zakupu.

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.

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

Infrastruktura teleinformatyczna stanowi swoisty krwiobieg systemów informacyjnych, oferujący medium wykorzystywane do transmisji i przetwarzania danych. W przypadku kluczowych systemów teleinformatycznych Resortu Obrony Narodowej, infrastruktura musi nosić szereg cech zapewniających bezpieczną i wydajną warstwę systemu.

W ubiegłym roku NCBC zakończyło również modernizację podkładowej sieci transmisyjnej IP RON poprzez 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

NARODOWE CENTRUM BEZPIECZEŃSTWA CYBERPRZESTRZENI

NARODOWE CENTRUM BEZPIECZEŃSTWA CYBERPRZESTRZENI