CYBER.MIL.PL

I. kwartał
2020

Szanowni Państwo,

ostatnie lata przyniosły Polsce i światu szereg nowych wyzwań w obszarze cyberbezpieczeństwa.Dziś, aby zapewnić skuteczną ochronę państwa i jego obywateli w silnie zdigitalizowanym środowisku niezbędne są zdecydowane działania. Takie działania podejmuje Ministerstwo Obrony Narodowej w ramach programu cyber.mil.pl. Nasz pomysł na to jak zwiększyć bezpieczeństwo Polski w cyberprzestrzeni to inwestycja w edukację oraz stałe wzmacnianie i unowocześnianie własnych zasobów wsparte konsolidacją narodowego potencjału. Całość zaś dopełnia szeroka współpraca międzynarodowa.

Mariusz Błaszczak,
Minister Obrony Narodowej

CYBER.MIL.PL

Program cyber.mil.pl to przede wszystkim ludzie – doskonale wyszkoleni specjaliści. Dumą napawa mnie fakt, że gdy dziś w Polsce lub na świecie dzieje się coś związanego z bezpieczeństwem w cyberprzestrzeni Wojsko Polskie jest tam obecne. Rozwiązania przygotowywane przez polskich wojskowych cyberspecjalistów nie tylko wygrywają międzynarodowe konkursy, ale służą przede wszystkim zapewnieniu bezpieczeństwa Polsce, tak jak specjalistyczne oprogramowanie wykorzystywane podczas epidemii koronawirusa.

Dlatego tak ważne są środki finansowe na realizację zadań związanych z cyberbezpieczeństwem. W latach 2020-2035 na realizację zadań w obszarze kryptologii, cyberbezpieczeństwa oraz rozwoju i utrzymania sieci teleinformatycznych planujemy przeznaczyć środki w wysokości ok. 10 mld PLN w ramach Planu Modernizacji Technicznej.
Mam też świadomość dużej rywalizacji na rynku pracy o ekspertów w tym obszarze. Zależy mi na tym, żeby wojsko obok nowoczesnego sprzętu i stałego rozwoju możliwości edukacyjnych, oferowało również atrakcyjne wynagrodzenia dla ekspertów. Dlatego zdecydowałem, że żołnierze zajmujący się tematyką „cyber", „krypto" oraz IT otrzymają stały

– comiesięczny dodatek służbowy oraz specjalną roczną premię.

Od czasu zainicjowania programu cyber.mil przeszliśmy długą drogę, już teraz wyraźnie widać, że założenia jakie przyjęliśmy były słuszne. Jestem pewien, że to o czym możecie Państwo przeczytać w tej publikacji jest znakomitym fundamentem do dalszej budowy naszej wspólnej cyberodporności.

Pierwszy kwartał 2020 r. to kolejne działania zrealizowane przez MON w ramach wprowadzania programu CYBER.MIL.PL, który został uruchomiony w 2019 r. dla podniesienia bezpieczeństwa Polski i Polaków w cyberprzestrzeni.

We wszystkich czterech głównych obszarach, na jakie został podzielony program, możemy mówić o znaczącym postępie. To dobry prognostyk na przyszłość.

Nawet bardzo pobieżny przegląd dotyczący tylko wybranych, sfinalizowanych w pierwszym kwartale roku projektów z obszaru cyberbezpieczeństwa wskazuje, że kompleksowe zmiany postępują w dobrym kierunku, w sposób zsynchronizowany i skoordynowany, a przede wszystkim - zgodnie z wypracowanym planem realizowanym przez RON z determinacją i konsekwencją.

Dziś, niemal rok po uruchomieniu programu **CYBER.MIL.PL,** możemy z satysfakcją potwierdzić, że stał się on efektywną platformą, na której budujemy narodowe zdolności bezpieczeństwa w cyberprzestrzeni.

Tomasz Zdzikot, Sekretarz Stanu w MON, Pełnomocnik Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprestrzeni (od 15.01.2018 r. do 3.04.2020 r.)

CYBER.MIL.PL

2020

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

Cyberprzestrzeń stanowi codzienne wyzwanie w pracy i na służbie każdego z nas. To jedyna domena operacyjna stworzona przez człowieka, nad którą każdego dnia staramy się panować, oczywiście stanowi to nielada wyzwanie, gdyż obszar ten nie tylko nie ma jednoznacznej definicji, ale także granic. Co wiecej rozwój technologiczny z założenia wyklucza ich określenie.

Z tego powodu aktywności żołnierzy podejmowane w trybie 24/7/365 w cyberprzestrzeni wykluczają działanie w pojedynkę. To kolektywna praca organizacji, instytucji krajowych, NATO czy UE, a przede wszystkim to zadanie nas wszystkich – ludzi, którzy w nich pracują, czy służą.

W I. kwartale 2020 r. jako NCBC zrealizowaliśmy wszystkie wyznaczone sobie cele w tym zakresie, w szczególności sykcesywnie rozwijamy CSIRT-MON oraz Wojska Obrony Cyberprzestrzeni.

W ramach programu Cyber.mil.pl zawieramy sojusze i rozwijamy współpracę z ekspertami z szeroko pojętego obszaru IT, krypto i cyber podczas ćwiczeń, konferencji, czy wizyt partnerskich.

1. KONSOLIDACJA I BUDOWA STRUKTUR CYBERBEZPIECZEŃSTWA

2. WSPÓŁPRACA I BUDOWA SILNEJ POZYCJI MIĘDZYNARODOWEJ

3. EDUKACJA, SZKOLENIE, TRENINGI

4. PODNIESIENIE POZIOMU BEZPIECZEŃSTWA RESORTOWYCH I WOJSKOWYCH SIECI ORAZ SYSTEMÓW

Jaki jest nasz cel?

CYBER.MIL.PL to program realizowany przez Ministerstwo Obrony Narodowej, którego głównym zadaniem jest zwiększenie bezpieczeństwa państwa i obywateli w cyberprzestrzeni. Program opiera się na czterech kluczowych filarach.

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

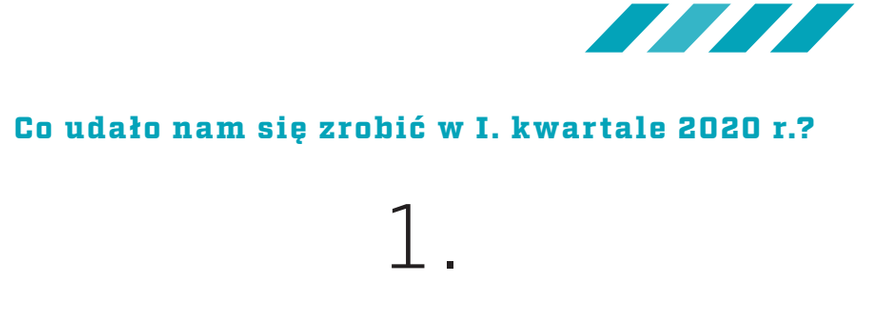
W ubiegłym roku Mariusz Błaszczak, minister obrony narodowej, zainaugurował program CYBER.MIL.PL. To szereg zaplanowanych działań, które pozwolą m.in. na utworzenie nowego rodzaju wojsk – Wojsk Obrony Cyberprzestrzeni, pozyskanie i wykształcenie najlepszych specjalistów zajmujących się informatyką i kryptologią, którzy zasilą resort obrony narodowej, oraz zapewnienie odpowiedniego poziomu wydatków 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 w I. kwartale 2020 r.?

1.

Konsolidacja i budowanie struktur cyberbezpieczeństwa

W ramach pierwszego filaru programu **CYBER.MIL.PL,** związanego z konsolidacją i budowaniem silnych struktur związanych z cyberbepieczeństwem w resorcie obrony narodowej, duży nacisk został położony na pozyskanie i utrzymanie najlepszych ekspertów. Resort Obrony Narodowej (RON) nieszablonowo podchodzi do rekrutacji kandydatów i kieruje się zasadą maksymalnego ułatwienia oraz skracania procedur. Kontakty z kandydatami odbywają się z wykorzystaniem współczesnych i atrakcyjnych narzędzi: m.in. skype, messenger, strony www, facebook, twitter, LinkedIn, instagram. Chcemy, aby praca i służba wojskowa w obszarze cyber, krypto i IT była pod każdym względem atrakcyjna. Obok unikalnych wyzwań, z którymi na co dzień – w trybie 24/7/365 - mogą zmierzyć się cyber-specjaliści, praca w resorcie obrony narodowej to też możliwość współpracy z najlepszymi ekspertami, satysfakcja z możliwości stania na straży bezpieczeństwa kraju, ale też możliwość rozwoju osobistego poprzez: specjalistyczne kursy, szkolenia, studia (w tym podyplomowe i doktoranckie) oraz atrakcyjne wynagrodzenie.



Dodatki do uposażenia żołnierzy

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

W lutym 2020 r. weszła w życie zmiana rozporządzenia MON w sprawie dodatków do uposażenia zasadniczego żołnierzy zawodowych. W jej wyniku żołnierze zajmują-

cy stanowiska w Narodowym Centrum Bezpieczeństwa Cyberprzestrzeni, Centrum Operacji Cybernetycznych oraz Centrum Projektów Informatycznych w obszarze cyberbezpieczeństwa, kryptologii lub projektowania i programowania, otrzymują miesięczny dodatek w wysokości od **450** do **2100** zł. W przypadku, gdy przesłużą rok kalendarzowy na danym stanowisku otrzymają także jednorazowy dodatek w wysokości od **100%** do nawet **620%** kwoty miesięcznego dodatku otrzymanego w grudniu danego roku.

Ramię w ramię z TOAW

Rekrutacja ekspertów do struktur cyber jest grą zespołową i jednym z najważniejszych zdań na 2020 r. wszystkich jednostek w resorcie obrony narodowej. Istotną inicjatywą w tym obszarze było powołanie w styczniu 2020 r. nowego Biura ds. Programu Zostań Żołnierzem Rzeczypospolitej, którego dyrektorem został gen. bryg. Artur Dębczak.

W celu opracowania wspólnej strategii działań w obszarze rekrutacji do struktur cyber, w lutym 2020 r. w NCBC zorganizowano spotkanie instytucji odpowiedzialnych za rekrutację żołnierzy do struktur z TOAW – Terenowymi Organami Administracji Wojskowej: szefami Wojewódzkich Sztabów Wojskowych i komendantami Wojskowych Komend Uzupełnień.

Resortowa infolinia rekrutacyjna

W marcu 2020 r. NCBC uruchomiło pierwszą w resorcie obrony narodowej infolinię rekrutacyjną, gdzie pod numerem **509-677-777**, w dni robocze od godz. 8.00 do 20.00, wszyscy cywilni i wojskowi kandydaci znajdą informacje o możliwości podjęcia pracy lub służby w naszych strukturach.

Budowa ducha zespołu

Zależy nam na budowaniu poczucia tożsamości z Wojskiem Polskim w oparciu o tradycję i tzw. „team spirit", czyli ducha zespołu. To dlatego, utworzone w 2019 r. NCBC otrzymało patrona i od lutego 2020 r. nosi imię wybitnego polskiego kryptologa, który przyczynił się do „złamania" kodu niemieckiej maszyny szyfrującej ENIGMA - Jerzego Witolda Różyckiego. Dodatkowo - w marcu 2020 r. – NCBC otrzymało odznakę pamiątkową, oznaki rozpoznawcze na mundur wyjściowy i polowy oraz proporczyk na beret.

Razem w walce z COVID-19

W marcu 2020 r. NCBC i Rządowe Centrum Bezpieczeństwa (RCB) podpisały porozumienie istotne dla podniesienia bezpieczeństwa Polski i Polaków, w którym zobowiązały się do wspólnego działania w zakresie zwalczania COVID-19 oraz wywołanych tą chorobą sytuacji kryzysowych. Wspólne działania obydwu instytucji polegają na zapewnieniu funkcjonowania oprogramowania GisCOVID-19, które pozwala na szybsze i precyzyjniejsze reagowanie na rozwój sytuacji związanej z COVID-19. W tym celu NCBC udostępniło RCB infrastrukturę teleinformatyczną oraz wsparcie eksperckie do prawidłowego jej funkcjonowania.

Także 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 Wojska Polskiego.

Żołnierze Zespołu Działań Cyberprzestrzennych Dowództwa Wojsk Obrony Terytorialnej wspólnie z podchorążymi Wojskowej Akademii Technicznej oraz ekspertami z NCBC uruchomili platformę wsparcia samorządów, organów sanitarnych i podmiotów leczniczych pod adresem: **https://pomocwot.ron.mil.pl**

Aplikacja pod nazwą: **pomocWOT** łączy koordynatorów ds. wsparcia w brygadach WOT z pracownikami instytucji odpowiedzialnych za realizację zadań związanych z niesieniem pomocy. Dodatkowo, pracownik ośrodka pomocy społecznej lub Caritas ma możliwość śledzenia postępu realizacji zgłoszenia. Wcześniej informacje były przekazywane przez telefon, co zacznie wydłużało proces.

Eksperci-informatycy z NCBC i Wojskowej Akademii Technicznej stworzyli w marcu br. 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 powstrzymanie przed jego dalszym rozprzestrzenianiem się poprzez ostrzeganie użytkowników telefonów komórkowych przed grożącym im niebezpieczeństwem. Aplikacja została zrealizowana w ramach **#Buildfor-COVID19 Global online Hackathon** - międzynarodowego przedsięwzięcia zorganizowanego na platformie DEVPOST i wspieranego przez World Health Organization i naukowców z Chan Zuckerberg Biohub. Łącznie do rywalizacji przystąpiło 18000 ludzi i zgłoszono 1500 projektów z całego świata.

2.

Edukacja, szkolenie i trening

Międzynarodowe hackathony

Drugi filar programu, czyli edukacja, szkolenie i trening, to także kolejny sukces. Potwierdza go **zwycięstwo naszych wojskowych ekspertów w NATO TIDE Hackathon.** W lutym br. w Monachium najlepszy okazał się zespół jednostki podporządkowanej NCBC - Centrum Projektów Informatycznych. Wartym podkreślenia jest fakt, że to trzeci z rzędu triumf drużyn

z MON w tym wymagającym konkursie. W 2018 r. w Czarnogórze i w 2019 r. w Warszawie reprezentanci z resortu obrony narodowej także stawali na najwyższym podium zawodów organizowanych przez Sojusznicze Dowództwo ds. Transformacji (NATO Allied Command Transformation).

Szkoła Podoficerska SONDA

Jako dopełnienie całej struktury szkoleniowej Wojsk Obrony Terytorialnej (pomiędzy funkcjonujące już szkolenia szeregowych oraz kandydatów na oficerów w ramach kursu Agrykola) w 2020 r. ruszała utworzona 1 października 2019 r. Szkoła Podoficerska SONDA w Zegrzu i Toruniu. Szkoła wykształci ok. 600 kandydatów na podoficerów rocznie w zakresie łączności i informatyki (Zegrze) oraz podoficerów WOT o specjalności piechota (Toruń). Projekt łączy: dziedzictwo Szkoły Niższych Dowódców AK, model kształcenia podoficerskiego z USA i polskie doświadczenia. Uwzględnia obecne potrzeby Wojska Polskiego.

Cyber szkolenia

W lutym 2020 r. na terenie Akademii Sztuki Wojennej, NCBC przeprowadziło szkolenie eksperckie w zakresie bezpiecznego korzystania ze środków komunikacji elektronicznej, w tym z przeciwdziałania atakom w cyberprzestrzeni, dla rzeczników i oficerów prasowych wszystkich dowództw i instytucji podległych MON i Sztabowi Generalnemu Wojska Polskiego (do szczebla brygady włącznie), a także osób odpowiedzialnych za komunikację strategiczną i starszych podoficerów dowództw.

Także w lutym, po raz pierwszy zorganizowaliśmy **Zimową Szkołę Cyberbezpieczeństwa**, której celem jest podniesienie świadomości na temat nowych zagrożeń związanych z rozwojem technologicznym oraz promowanie debaty w obszarze cyberbezpieczeństwa. Przedsięwzięcie jest adresowane do kadr Wojska Polskiego i RON. Zimowa szkoła stanowi rozszerzenie formuły szkoleniowo-edukacyjnej zainicjowanej przez Letnią Szkołę Cyberbezpieczeństwa, która okazała się sukcesem i którą w tym roku MON planuje przeprowadzić już po raz piąty.

Szersza oferta edukacyjna

Stale zwiększamy limity miejsc na uczelniach wojskowych (Wojskowa Akademia Techniczna, Akademia Marynarki Wojennej) na kierunkach związanych z bezpieczeństwem informacyjnym: elektronika i telekomunikacja,

informatyka, kryptologia i cyberbezpieczeństwo, systemy informacyjne w bezpieczeństwie.

W roku akademickim 2020/21 Akademia Sztuki Wojennej (ASzWoj), otwiera nabór **na kierunku Bezpieczeństwo Informacyjne na studiach licencjackich i magisterskich**, które pozwolą studentom zdobyć wiedzę i umiejętności niezbędne na stanowiskach: inspektora ochrony danych osobowych, projektanta systemów bezpieczeństwa informacyjnego, menadżera i eksperta w sektorze publicznym i prywatnym.

Jednocześnie Wydział Wojskowy ASzWoj prowadzi studia podyplomowe Ochrona i Bezpieczeństwo Cyberprzestrzeni, a Wydział Bezpieczeństwa Narodowego studia podyplomowe Bezpieczeństwo Cyberprzestrzeni RP. Studia te przygotowują do samodzielnego rozwiązywania problemów z zakresu inżynierii, organizacji i eksploatacji systemów bezpieczeństwa, w tym do pracy w zespołach interdyscyplinarnych z zakresu zarządzania ryzykiem, identyfikacji i prognozowania zagrożeń bezpieczeństwa cyberprzestrzeni RP.

W nowej edycji prowadzonych przez ASzWoj studiów MBA Security & Critical Infrastructure przewidziano w 2020 r. moduł audyt bezpieczeństwa, którego ukończenie przygotowuje kadrę menadżerską również w aspekcie zarządzania cyberbezpieczeństwem podmiotu zaliczanego do infrastruktury specjalnej, w szczególności infrastruktury krytycznej.

AKADEMIA SZTUKI WOJENNEJ

AWL AKADEMIA WOJSK LĄDOWYCH

W Akademii Wojsk Lądowych uruchomiono rekrutację na siedmiosemestralne studia inżynierskie na kierunku informatyka w roku akademickim 2020/21. W obecnym roku akademickim liczba miejsc wyniesie 30.

Międzynarodowe konferencje

W Wojskowej Akademii Technicznej na początku 2020 r. odbyła się międzynarodowa konferencja naukowa pt.: **Mathematical Cryptology and Cybersecurity (MC&C 2020)**, podczas której dokonano przeglądu najnowszych wyników badań w zakresie kryptologii matematycznej oraz rozwiązań z obszaru cyberbezpieczeństwa. Konferencja umożliwiła wymianę doświadczeń oraz pozwoliła na zainicjowanie współpracy kryptologów, matematyków i przedstawicieli podmiotów z obszaru kryptologii i cyberbezpieczeństwa z całego świata.

ASzWoj uczestniczy w projekcie Utworzenie międzynarodowej zintegrowanej komórki ds. działań w cyberprzestrzeni **(ang. Multinational Integrated Cyber Fusion Capability MNICF)**, który jest częścią Wielonarodowej Kampanii Rozwoju Zdolności 2015-2020 (ang. Multinational Capability Development Campaign MCDC 2015-2020). W ramach projektu w lutym br. odbyły się warsztaty z udziałem przedstawicieli: Kanady, Danii, Finlandii, Polski, Szwajcarii, Wielkiej Brytanii, Stanów Zjednoczonych oraz instytucji Unii Europejskiej i NATO.

Ośrodek badawczy i biblioteka cyfrowa

W Centrum Badań nad Bezpieczeństwem w ASzWoj zaczął funkcjonować ośrodek badawczy – **Centrum Studiów nad Cyberbezpieczeństwem**. Głównym zadaniem Ośrodka jest identyfikowanie, analizowanie i informowanie władz państwowych i wojskowych RP o kwestiach dotyczących aspektów prawnych cyberbezpieczeństwa. Ponadto Ośrodek

zajmuje się: opracowywaniem ekspertyz, opinii i stanowisk w sprawach regulacji prawnych dotyczących cyberbezpieczeństwa RP; organizowaniem szkoleń, warsztatów i wykładów dla pracowników administracji publicznej.

W ramach Portalu Bezpieczeństwa i Obronności Akademii Sztuki Wojennej wystartowała cyfrowa biblioteka cyberbezpieczeństwa, której zasoby dostępne są pod adresem **https://pbio.akademia.mil.pl/.**

Staże dla uczniów WOLI

Działające przy **WAT Wojskowe Ogólnokształcące Liceum Informatyczne (WOLI)** w styczniu br. podpisało list intencyjny z Wojskowym Centralnym Biurem Konstrukcyjno-Technologicznym S.A. Celem umowy jest nawiązanie współpracy umożliwiającej odbywanie zajęć praktycznych i staży przez uczniów WOLI oraz realizacji wspólnych projektów zawodowych.

W pierwszym kwartale 2020 r. Ministerstwo Obrony Narodowej rozszerzyło program „CYBER.MIL z klasą", skierowany do szkół średnich (licea i technika), które swoją

ofertę edukacyjną będą chciały poszerzyć w kolejnych etapach w takich obszarach jak cyberbezpieczeństwo i nowoczesne technologie informatyczne.

Celem programu jest kształcenie uczniów w wybranych szkołach, przygotowanie ich do służby w resorcie obrony narodowej oraz pozyskanie zasobów rezerw osobowych. Dzięki programowi na terenie każdego województwa powstanie jedna klasa o profilu cyberbezpieczeństwo i nowoczesne technologie informatyczne.

Praktyki on-line dla studentów

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 odbywają 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 przygotowują materiały edukacyjne i szkoleniowe do platformy e-learningowej.

Nagroda im. M. Rejewskiego

Ze względu na duże zainteresowanie w 2019 r., również w tym roku zorganizowany zostanie **konkurs o nagrodę im. Mariana Rejewskiego** za najlepszą pracę inżynierską, licencjacką, magisterską, a także rozprawę doktorską poświęconą kryptologii, cyberobronie, cyberbezpieczeństwu lub zwalczaniu cyberprzestępczości. W pierwszym kwartale br. opracowane zostały dokumenty organizacyjne pozwalające na uruchomienie konkursu. Konkurs ma na celu zainteresowanie studentów i doktorantów tematyką związaną z szeroko rozumianym cyberbezpieczeństwem.

Legia Akademicka

Realizując postanowienia decyzji MON w sprawie programu ochotniczego przeszkolenia wojskowego studentów cywilnych **„Legia Akademicka”**, Regionalne Centrum Informatyki Kraków (jednostka ze struktury NCBC) w lutym br. zorganizowało szkolenia dla uczestników nowo utworzonej platformy e-learningowej. Platforma ta została przygotowana przez RCI Kraków, jako nowoczesna metoda zdalnego szkolenia ochotników w ramach Legii Akademickiej. Dodatkowo w pierwszym kwartale 2020 r. NCBC opracowało program szkolenia uczestników LA z obszaru cyberbezpieczeństwa, które będzie realizowane w tym roku.

CYBER.MIL.PL

Targi pracy i konferencje

Aby przyspieszyć i ułatwić rekrutację do struktur związanych z cyberbezpieczeństwem w resorcie obrony narodowej, zespół Cyber.mil.pl w pierwszym kwartale 2020 r. był stałym uczestnikiem najważniejszych wydarzeń z obszarów cyber, krypto i IT – konferencji **ITechDay**, oraz targów pracy na Uniwersytecie Warszawskim, Politechnice Warszawskiej, Wojskowej Akademii Technicznej. Dodatkowo NCBC nawiązało współpracę z miesięcznikiem Głos Akademicki, którego odbiorcami są studenci i absolwenci Wojskowej Akademii Technicznej. W magazynie publikowane są aktualne informacje z obszaru cyber, krypto i IT opracowywane przez ekspertów z Centrum.

3.

Współpraca i budowa silnej pozycji międzynarodowej Polski

Rozwijając współpracę i budując silną pozycję międzynarodową Polski w obszarze cyberbezpieczeństwa, w styczniu br. podczas wizyty w Warszawie wiceministra obrony narodowej Republiki Korei Południowej – Jungsup Kima, zawarliśmy porozumienie o współpracy naszych resortów obrony w dziedzinie cyberbezpieczeństwa. To kolejne porozumienie międzynarodowe, po zawartych w ubiegłym roku, z NATO i Dowództwem Sił USA w Europie (US EUCOM).

W lutym, w murach Akademii Sztuki Wojennej odbyły się tygodniowe warsztaty cyberbezpieczeństwa zorganizowane na potrzeby realizacji dwuletniego projektu Multinational Integrated Cyber Fusion Capability. Celem projektu jest zapewnienie zdolności do zwiększania zbiorowej świadomości sytuacyjnej w cyberprzestrzeni poprzez udostępnianie, łączenie i rozpowszechnianie informacji o zagrożeniach. Podczas międzynarodowych warsztatów, w Warszawie gościliśmy przedstawicieli U.S. Cyber Command, na czele z gen. bryg. Paulem Peytonem – wiceszefem J5.

W marcu br., w Zagrzebiu, zawarliśmy **porozumienie o współpracy (MoU)** z szefami resortów obrony: Chorwacji, Estonii, Litwy, Holandii i Rumunii, dotyczące 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.

Przedstawiciele resortu obrony narodowej wzięli udział w bilateralnych rozmowach ze stroną izraelską, których celem jest podpisanie w 2020 r. **porozumienie o współpracy (MoU)**. Dokument będzie regulował zagadnienia związane ze współpracą POL-IZR w obszarze cyberbezpieczeństwa, ze szczególnym uwzględnieniem wymiany doświadczeń oraz szkolenia ekspertów.

W pierwszym kwartale 2020 r. zainicjowano także współpracę NCBC z niemieckim odpowiednikiem – **Cyber Command**, która pozwoli na efektywną wymianę informacji oraz budowanie zdolności do obrony systemów teleinformatycznych, w ujęciu krajowym oraz sojuszniczym.

4.

Podnoszenie poziomu bezpieczeństwa resortowych i wojskowych sieci oraz systemów

Czwarty obszar naszej aktywności to działania w większości niejawne. Ich celem jest podniesienie poziomu bezpieczeństwa resortowych i wojskowych sieci oraz systemów teleinformatycznych.

W styczniu, w obecności Ministra Mariusza Błaszczaka, znacząco przed planowanym terminem, oddaliśmy do użytku nowo wybudowane na potrzeby NCBC dwa nowoczesne ośrodki w Legionowie - **Centrum Obliczeniowo-Projektowe i Projektowo-Konstrukcyjne**, które w istotny sposób przyczyniają się do podniesienia potencjału resortu w obszarze cyberbezpieczeństwa i kryptologii.

W ramach stałego podnoszenia poziomu bezpieczeństwa resortowych i wojskowych systemów teleinformatycznych opracowano studium wykonalności oraz wstępne założenia taktyczno-techniczne (WZTT) 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.

Ponadto w pierwszym kwartale 2020 r. w resorcie obrony narodowej kontynuowane były prace nad:

- opracowaniem narzędzi do bezpiecznej komunikacji, Pozwoli to na zebranie doświadczeń przed uruchomieniem komunikatora w docelowej konfiguracji,
- 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 i SKW.

CYBER.MIL.PL

MINISTERSTWO OBRONY NARODOWEJ

2020

WWW.CYBER.MIL.PL

MINISTERSTWO OBRONY NARODOWEJ