aut. Szymon Palczewski 23.11.2020

ĆWICZENIA DROGĄ DO TRANSFORMACJI NATO. CYBER COALITION 2020 WAŻNYM KROKIEM NAPRZÓD

1000 specjalistów ds. cyberbezpieczeństwa z 29 państw członkowskich oraz 4 krajów partnerskich, zaawansowane symulacje przeprowadzone w kontrolowanym środowisku w Tallinie, wykorzystanie najnowocześniejszych rozwiązań, scenariusze oparte na analizie realnych zagrożeń – to bilans najnowszej edycji największych wirtualnych ćwiczeń NATO „Cyber Coalition 2020". Sojusz w ramach podsumowania podzielił się z nami kilkoma faktami.

Zakończone ćwiczenia Cyber Coalition 2020 zgromadziły specjalistów ds. cyberbezpieczeństwa organów NATO, państw sojuszniczych oraz krajów partnerskich w celu wzmocnienia zdolności Sojuszu w zakresie odstraszania, obrony i przeciwdziałania cyberzagrożeniom za pomocą rozwijania współpracy oraz wirtualnych zdolności. Wydarzenie to istotny wkład w transformację NATO.

W najnowszą edycję ćwiczeń obrony zbiorowej w cyberprzestrzeni zaangażowanych było łącznie 29 krajów członkowskich oraz 4 państwa partnerskie (Finlandia, Irlandia, Szwecja i Szwajcaria). Udział w nich wzięło 1000 specjalistów, a sam scenariusz symulował realistyczne zdarzenia. Głównym założeniem wydarzenia było usprawnienie koordynacji, współpracy i wymiany informacji w całej wirtualnej domenie NATO – wynika materiałów, które Sojuszu udostępnił CyberDefemce24.pl.

> *We współczesnym świecie NATO ma do odegrania trzy kluczowe role w cyberprzestrzeni:*
> *1. Napędzać postęp w całym Sojuszu;*
> *2. Działać jako centrum wymiany informacji, szkoleń i wiedzy specjalistycznej;*
> *3. Chronić nasze sieci*
>
> *Jens Stoltenberg, Sekretarz Generalny NATO*

Ćwiczenia zbiorowej cyberobrony odbyły się pod opieką i kontrolą NATO Cyber Range w Estonii, a podczas ich trwania wykorzystano również inne kanały komunikacyjne Sojuszu. Scenariusze obejmowały m.in. cyberataki na infrastrukturę krytyczną, włamania do sieci, szpiegostwo, zagrożenia wewnętrzne, kradzież informacji czy manipulację danymi – wskazują materiały NATO.

W tym miejscu warto podkreślić, że Cyber Range, to specjalne centrum szkoleniowe NATO

usytuowane w Tallinnie, które powstało w 2014 roku. Zarządza nim estońskie Ministerstwo Obrony. Jego podstawowym zadaniem jest stworzenie bezpiecznego środowiska do ćwiczeń, co ma pozwolić na podniesienie cyberzdolności Sojuszu.

Równie ważnym podmiotem zaangażowanym w Cyber Coalition 2020 było NATO Cyber Security Centre (NCSC). Z założenia ma stanowić ośrodek wiedzy technicznej w zakresie cyberbezpieczeństwa Sojuszu. Odpowiada m.in. za kierowanie współpracy technicznej wewnątrz struktur NATO, jak i ze specjalistami z państw członkowskich.

NCSC ma również utrzymywać i rozwijać cyberbezpieczeństwo sieci podmiotów NATO oraz sprzyjać dostarczaniu i nabywaniu nowych zdolności oraz usług w zakresie cyberobrony.

> *Zapewnienie skutecznej, sprawnej i odpornej cyberobrony w celu umożliwienia bezpiecznego wykonywania misji oraz konsultacji, operacji i działań NATO, wzmacniając kolektywną cyberobronę Sojuszu*
>
> *Ian J West, szef NCSC*

W ramach najnowszej edycji Cyber Coalition przeprowadzono 3 eksperymenty. Pierwszy dotyczył konieczności zweryfikowania platform służących do oszustw. W ramach działań należało ocenić ich wartość operacyjną, w tym przede wszystkim rozpoznać wroga oraz zagrożenie dla sieci i systemów.

Drugi scenariusz obejmował weryfikację wykorzystania koncepcji świadomości sytuacyjnej (ang. situational awareness – SA) w cyberprzestrzeni. Szczególną rolę w tym zakresie ogrywała komunikacja z dowódcami oraz wspieranie procesu podejmowania decyzji.

Ostatni eksperyment skupiał się na wykorzystaniu analizy social mediów w odniesieniu do świadomości sytuacyjnej w kontekście dowodzenia, tak aby m.in. skutecznie wykrywać kampanie dezinformacyjne czy prowadzić operacje rozpoznania przeciwnika.

> *Świadomość sytuacyjna (SA) to efektywne zrozumienie i projekcja wszystkiego, co jest związane z globalną domeną cyberprzestrzeni, co może mieć wpływ na bezpieczeństwo, misje i / lub środowisko, w którym działa Sojusz*
>
> *Definicja NATO*

NATO dostrzega szczególne znaczenie ćwiczeń w budowaniu skutecznej cyberobrony. Sojusz z założenia eksperymenty i praktyczną analizę stawia ponad długookresowe badania naukowe. Takie podejście pozwala na przyspieszenie rozwoju oraz tworzenie nowych możliwości znacznie szybciej niż bazowanie na teoretycznych wnioskach.

Czytaj też: Trwają największe ćwiczenia NATO w cyberprzestrzeni. „Cyberobrona priorytetem

sojuszu”