

CYBEROBRONA SIŁ POWIETRZNYCH USA. „AUTOMATYZACJA WSZĘDZIE TAM, GDZIE TO TYLKO MOŻLIWE”

„Nie chodzi o puste pozyskiwanie informacji, ale o to, jak sprawić, by właściwi piloci mogli użyć odpowiedniego algorytmu” – podkreślił gen. broni Timothy Haugh, dowództwa 16. Armii Powietrznej USA. Jak zadeklarował, cyberzespół do zadań defensywnych jego jednostki jest w stanie skutecznie obronić infrastrukturę przed operacjami wroga.

Współcześnie państwa aktywnie wykorzystują swoje cyberzdolności do prowadzenia działań poniżej progu wojny. Zaliczają się do nich m.in. kampanie cyberszpiegowskie wymierzone w podmioty wojskowe i cywilne, a także liczne próby włamań do wrażliwych systemów w celu zniszczenia lub zakłócenia ich pracy.

Chleb powszedni

Dla 16. Armii Powietrznej, będącej częścią [Sił Powietrznych Stanów Zjednoczonych](#), zmagania z tego typu operacjami adwersarzy to chleb powszedni. Jej żołnierze są odpowiedzialni za walkę informacyjną, obejmującą np. działania w cyberprzestrzeni.

Obrona wojskowej infrastruktury przed włamaniami oraz innymi incydentami jest dla dowództwa priorytetem. Potwierdził to gen. broni Timothy Haugh, stojący na czele 16. Armii Powietrznej w wywiadzie dla C4isrnet. Zaznaczył, że wiele wykorzystywanych rozwiązań pojawiło się jeszcze przed powstaniem [obecných cyberzagrożeń](#), które dodatkowo z czasem zostały utrwalone przez działania Rosji i Chin.

Przedstawiciel [sił zbrojnych USA](#) stwierdził, że cyberzespół do zadań defensywnych w ramach jego jednostki jest w stanie skutecznie obronić infrastrukturę przez operacjami wroga – całą sieć lub konkretny system uzbrojenia. Wojskowi specjaliści potrafią również przedstawić szczegółowe informacje na temat zagrożenia, co pomaga w podjęciu skuteczniejszych działań. W ten sposób amerykańska armia staje się mniej podatna.

Wsparcie USCYBERCOM

Zespół cyberobrony w ramach Sił Powietrzny USA składa się z wybitnych specjalistów, jest wspierany przez USCYBERCOM i z założenia ma zapewnić maksymalną ochronę prowadzonych misji pod kątem technicznym. Mowa tu o dbałości o zabezpieczenie infrastruktury krytycznej lub sprzętu powiązanego z samolotami i/lub pilotami.

Gen. broni Timothy Haugh zaznaczył, że współpraca z dowództwem cybernetycznym amerykańskiej armii pozwoliła żołnierzom cyberobrony Sił Powietrznych USA lepiej reagować na pojawiające się

zagrożenia.

„Automatyzacja procesów wszędzie tam, gdzie to tylko możliwe”

W tym miejscu należy odnieść się do m.in. „Unified Platform”, która stanowi centralny element programu USCYBERCOM, integrujący i analizujący razem z partnerami dane pochodzące z wojskowych operacji ofensywnych i defensywnych. Inicjatywa jest tworzona przez siły powietrzne w imieniu dowództwa cybernetycznego oraz połączonych sił i umożliwiła równoczesne udostępnianie danych i informacji o zagrożeniach, co „pozwała na automatyzację procesów wszędzie tam, gdzie to tylko możliwe” – wyjaśnił w rozmowie z C4isrnet gen. broni Timothy Haugh.

Nie chodzi o puste pozyskiwanie informacji, ale o to, jak sprawić, by właściwi piloci mogli użyć odpowiedniego algorytmu.

stwierdził gen. broni Timothy Haugh, dowódca 16. Armii Powietrznej USA

Technologia ta nieustannie się rozwija. Szczególnie ważne są rozwiązania z zakresu big data, chmury i sztucznej inteligencji, ponieważ to one pozwalają na tworzenie nowoczesnych platform z myślą o potrzebach sił zbrojnych.

Chcemy być także bliżej Państwa – czytelników. Dlatego, jeśli są sprawy, które Was nurtują; pytania, na które nie znacie odpowiedzi; tematy, o których trzeba napisać – zapraszamy do kontaktu. Piszcie do nas na: redakcja@cyberdefence24.pl. Przyszłość przynosi zmiany. Wprowadzamy je pod hasłem #CyberIsFuture.



OPERATOR
594

Pamiętaj że wszystko, czego pragniesz, jest po drugiej stronie strachu.

Sklep.Defence 24

Fot. Reklama