(CYBER)WYZWANIA DLA WOJSKA POLSKIEGO OCZAMI PRZEDSTAWICIELI ARMII

Jakie wydarzenia związane ze zmianami w Wojsku Polskim wywarły największy wpływ w 2020 roku? Jakie zagrożenia i wyzwania czyhają w nadchodzącym roku? O opinie zapytaliśmy przedstawicieli polskiej armii.

W mijającym roku w zakresie funkcjonowania armii, szkolnictwa wojskowego i budowy jednostek wspomagających zaszło wiele zmian. Jednocześnie dużym wyzwaniem dla funkcjonowania jednostek wojskowych, ale również placówek edukacyjnych była pandemia koronawirusa, z którą przyszło się zmierzyć zarówno obszarowi militarnemu jak i cywilnemu.

Na podsumowanie ostatnich 12 miesięcy oraz odnalezienia kluczowych wyzwań na rok kolejny postanowiliśmy spojrzeć „wojskowym okiem" a o dokonanie oceny prognozowanych trendów, zagrożeń i wyzwań na kolejny rok dla polskiej armii w cyberprzestrzeni poprosiliśmy przedstawicieli Wojska Polskiego:

- Gen. dyw. Jarosława Gromadzińskiego, dowódcę 18. Dywizji Zmechanizowanej im. gen. broni Tadeusza Buka;
- Gen. bryg. Roberta Kosowskiego, rektora-komendanta Akademii Sztuki Wojennej;
- Kadm. Tomasza Szubrychta, rektora-komendanta, Akademii Marynarki Wojennej;
- Gen. bryg. Karola Molendę, dyrektora Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni i płk rez. Pawła Dziubę, dyrektora Eksperckiego Centrum Szkolenia Cyberbezpieczeństwa;
- prof. Zbigniewa Tarapatę, dziekana Wydziału Cybernetyki WAT oraz Ppłk Rafała Kasprzyka, z-ca dziekana Wydziału Cybernetyki WAT.

Jakie wydarzenia związane ze zmianami w armii w Pana opinii wywarły największy wpływ w mijającym 2020 roku na cyberzdolności armii i cyberbezpieczeństwo kraju?

„W mojej opinii do najważniejszych wydarzeń mijającego roku należy zaliczyć ugruntowanie pozycji Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni, które odpowiada za kluczowe obszary związane z kryptologią i cyberbezpieczeństwem" – wskazuje gen. Jarosław Gromadziński.
Jak podkreśla, dzięki zaangażowaniu gen. bryg. Karola Molendy, centrum wyrasta na lidera regionu w środkowej Europie w domenie cyberbezpieczeństwa. Kolejnym ważnym wydarzeniem, na które zwraca uwagę gen. Gromadziński jest utworzenie Eksperckiego Centrum Szkolenia Cyberbezpieczeństwa. „Konsekwencją tych działań jest stabilny i niezachwiany rozwój Wojsk Obrony Cyberprzestrzeni, będących odpowiedzią na współczesne wyzwania i zagrożenia dla bezpieczeństwa cyberprzestrzeni" –podkreśla generał w ramach odpowiedzi.

Podobne zdanie na temat rozwoju Wojsk Obrony Cyberprzestrzeni przedstawili gen. bryg. Karol Molenda oraz płk rez. Paweł Dziuba. „Czołową potrzebą dla Polski, a zarazem jednym z głównych

przedsięwzięć realizowanych przez NCBC stało się formowanie Wojsk Obrony Cyberprzestrzeni, które przebiega zgodnie z harmonogramem" - tłumaczą przedstawiciele armii. Jak podkreślają, w roku 2020 fundamentalne znaczenie dla cyberzdolności armii i cyberbezpieczeństwa kraju miała decyzja podjęta przez kierownictwo resortu o sformowaniu ośrodka eksperckiego – Eksperckiego Centrum Szkolenia Cyberbezpieczeństwa (ECSC). „To właśnie Centrum ma zajmować się zapewnieniem dostępności szkoleń, kursów, treningów dla specjalistów sektora cyber w resorcie obrony narodowej. Za decyzją o sformowaniu ECSC szybko poszły praktyczne działania i od 9 listopada 2020 roku Centrum Eksperckie funkcjonuje, szkoli żołnierzy oraz pracowników wojska, rozwija się i stopniowo osiąga zaplanowane cele" - wskazują gen. bryg. Karol Molenda oraz płk rez. Paweł Dziuba. Ponadto, zwrócili również uwagę na postępy w zakresie budowania zespołu CSIRT MON, funkcjonującego w ramach Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni, a prowadzonego przez Ministra Obrony Narodowej.

„Konieczność wdrożenia zaleceń profilaktyki zdrowotnej skutkowała potrzebą wprowadzenia szeregu zmian w realizacji większości przedsięwzięć - czy to w obszarze wojskowym, czy też cywilnym. Zmianom musiały ulec także plany związane z funkcjonowaniem Akademii jako jednostki wojskowej oraz jako uczelni wyższej" – wskazuje gen. Kosowski, podkreślając jednocześnie, że wiele aktywności, w tym również zajęć edukacyjnych, zostało przeniesionych do przestrzeni wirtualnej. „Pracownicy administracyjni i dydaktyczni realizują swoje zadania w dużej mierze zdalnie. W podobny sposób funkcjonuje administracja publiczna. Taki nietypowy model funkcjonowania państwa z oczywistych względów zwiększa podatność na cyberzagrożenia i implikuje konieczność konsekwentnego podnoszenia cyberzdolności i cyberodporności w Siłach Zbrojnych oraz w innych kluczowych obszarach bezpieczeństwa narodowego" - dodaje generał. „Potwierdzeniem tego trendu jest budowanie cyberwojsk oraz rosnąca rola Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni (NCBC) czy Eksperckiego Centrum Szkolenia Cyberbezpieczeństwa (ECSC), które w realizacji swoich zadań wspierane są przez inne, wyspecjalizowane komórki, jak na przykład powołane w ASzWoj w tym roku Akademickie Centrum Polityki Cyberbezpieczeństwa (ACPC)" - podsumowuje.

„Na cyberzdolności armii największy wpływ w 2020 roku miało utworzenie Eksperckiego Centrum Szkolenia Cyberbezpieczeństwa" – wskazuje Kadm. Tomasz Szubrycht. Co podkreśla rektor-komendant Akademii Marynarki Wojennej podniesienie poziomu umiejętności i świadomości oraz kształcenie kadr są nieodzowne dla budowy cyberbezpieczeństwa. „Redukcji rosnącej asymetrii między wiedzą konieczną do popełnienia cyberprzestępstwa lub przeprowadzenia cyberataku, a umiejętnościami koniecznymi, by przed takim działaniem się obronić służyło uruchomienie w 2020 roku Morskiego Centrum Cyberbezpieczeństwa Akademii Marynarki Wojennej. Wydaje się również, że zmiana rozporządzenia MON w sprawie dodatków do uposażenia zasadniczego żołnierzy zawodowych zajmujący stanowiska w NCBC, WOC i CPI w obszarze cyberbezpieczeństwa, kryptologii lub projektowania i programowania może być skutecznym środkiem motywacyjnym do podejmowania służby na tych stanowiskach" – dodaje kontradmirał.

Na rolę Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni w planowaniu i programowaniu rozwoju zdolności Sił Zbrojnych RP wskazują również ppłk Rafał Kasprzyk oraz prof. Zbigniew Tarapata. „Utrzymanie istniejących zdolności, a tym bardziej pozyskanie nowych, możliwe jest tylko poprzez inwestycje w zasadnicze komponenty funkcjonalne zdolności, wśród których można wyróżnić: doktrynę, organizacje, szkolenie, sprzęt wojskowy, zasoby osobowe, przywództwo, infrastrukturę oraz interoperacyjność" – podkreślają. Jak wskazują przedstawiciele Wojskowej Akademii Technicznej, „kluczową inicjatywą wydaje się być powołanie Eksperckiego Centrum Szkolenia Cyberbezpieczeństwa".

Jakie wyzwania w obszarze rozwoju cyberzdolności i cyberbezpieczeństwa państwa stoją przed Wojskiem Polskim w nadchodzącym roku?

Generał Gromadziński wskazuje, że „cyberprzestrzeń jest jednym z kluczowych obszarów działań we

współczesnych konfliktach zbrojnych", dlatego też w jego opinii bardzo ważnym wyzwaniem jest kontynuowanie formowania dowództwa Wojsk Obrony Cyberprzestrzeni a także dynamiczny rozwój Eksperckiego Centrum Szkolenia Cyberbezpieczeństwa, które będzie szkoliło dla Sił Zbrojnych specjalistów z zakresu bezpieczeństwa cyberprzestrzeni.

Podobne stanowisko reprezentują gen. bryg. Karol Molenda oraz płk rez. Paweł Dziuba, którzy jednoznacznie ocenili, że z perspektywy NCBC oraz ECSC wielkim wyzwaniem dla Sił Zbrojnych RP będzie dalsze formowanie Wojsk Obrony Cyberprzestrzeni. Jak wskazują przedstawiciele armii, to proces kilkuletni, jednak już teraz wymagane jest inwestowanie w kadrę specjalistów i w przygotowywanie fachowców, którzy potem będą wyznaczani do WOC.

„Istotne jest, by rozwijać cyberzdolności w strukturach Sił Zbrojnych RP, nadając im odpowiednią formę organizacyjną. Ogromnym wyzwaniem jest i będzie również w przyszłości zasilenie tych struktur stałym dopływem wykwalifikowanych kadr - zarówno z rynku cywilnego, jak i tych, przygotowanych przez nowo powstałe Eksperckie Centrum Szkolenia Cyberbezpieczeństwa" – wskazuje natomiast gen. Kosowski. Co więcej, jak podkreśla generał, koniecznie jest przygotowanie takich zmian legislacyjnych, aby prawo nadążało za rozwojem technologii – „tu widzę ogromny potencjał wspomnianego już ACPC". „Polska powinna mieć cyberzdolności komplementarne z innymi państwami sojuszniczymi, zwłaszcza w kontekście geopolityki i naszego położenia na wschodniej flance NATO, a także mieć na uwadze nieustannie ewoluujące zagrożenia" – dodaje generał.

Na podobne aspekty wskazuje rektor-komendanta Akademii Marynarki Wojennej kadm. Tomasz Szubrycht, który zwraca uwagę, że największym wyzwaniem „jest pozyskanie i utrzymanie specjalistów z zakresu cyberbezpieczeństwa". „Ich brak pociąga za sobą zwiększone ryzyko zaistnienia cyberzagrożeń, złego monitorowania stanu cyberbezpieczeństwa oraz słabej reakcji na incydenty i przywracania działalności po zaistniałych incydentach" – tłumaczy kadm. Szubrycht. Rektor-komendant wskazuje również na wyzwanie, jakim jest zabezpieczenie krajowej infrastruktury krytycznej przed atakami grup sponsorowanych przez państwa – „coraz więcej ataków jest przypisywanych takim grupom. Ransomware, botnety, ataki DDoS (także w celu wymuszenia okupu) mogą jako cel ataku (świadomie lub nie) wybrać polskie siły zbrojne. W tym kontekście należy obawiać się, że te cyberataki będą atakami wielowektorowymi o dużej skali" – podsumował kontradmirał.

„Kluczowym wyzwaniem nie tylko w nadchodzącym roku, ale również w dłuższym horyzoncie czasowym jest pozyskiwanie i utrzymanie kadr stanowiących kluczowy komponent cyberzdolności" – wskazują przedstawiciele Wojskowej Akademii Technicznej. „Rynek cywilny w obszarze bezpieczeństwa teleinformatycznego jest bardzo atrakcyjny i niezwykle chłonny. Najbliższe lata prawdopodobnie powiększą już istotną lukę w podaży i popycie nie tylko wysokiej klasy specjalistów technicznych, ale również wykwalifikowanej kadry zarządzającej na różnych poziomach w pionach IT i cyberbezpieczeństwa" – dodają, jednocześnie wskazując, że wypracowano szereg mechanizmów, aby sprostać temu wyzwaniu - utworzenie ECSC, zwiększenie limitów przyjęć na studia wojskowe na kierunkach kształcących przyszłych „cyberżołnierzy" oraz wprowadzenie dodatku stałego dla żołnierzy wybranych grupach osobowych służących na stanowiskach wymagających kompetencji z obszaru informatyki oraz kryptologii i cyberbezpieczeństwa. „Przyszłość będzie jednak wymagała radykalnej zmiany podejścia do prowadzenia operacji w cyberprzestrzeni, a siły zbrojne gotowe do zmiany sposobu myślenia zyskają przewagę. Wyzwaniem jest więc wypracowanie tego radykalnie nowego podejścia wcześniej, niż zrobią to inni" – podsumowali przedstawiciele WAT.

Jakie największe zagrożenia w obszarze cyberbezpieczeństwa pododdziałów i oddziałów Sił Zbrojnych a także bezpieczeństwa kraju stoją przed armią w przyszłym roku?

„Łańcuch jest tak silny, jak jego najsłabsze ogniwo" – przypomina gen. Gromadziński w ramach

odpowiedzi na pytanie o największe zagrożenia dla polskiej armii. „W tym mniemaniu to żołnierz jest najsłabszym ogniwem, ponieważ nie zawsze zdaje sobie sprawę z konsekwencji, jakie niesie za sobą niewłaściwe użytkowanie Internetu" - stwierdził generał. Co to oznacza? „Powinniśmy dotrzeć do każdego pojedynczego żołnierza - użytkownika sieci i zbudować w nim świadomość o możliwych zagrożeniach w cyberprzestrzeni oraz skutecznego sposobu przeciwdziałania im. Uważam, że jednym z kroków w tym kierunku jest zapoznanie żołnierzy z problematyką zawartą w podręczniku >Bezpieczeństwo w sieci<, który stworzony został dla żołnierzy 18 Dywizji Zmechanizowanej" – dodaje Gromadziński. O tym, czym jest podręcznik pisaliśmy tutaj oraz tutaj.

Z kolei gen. bryg. Karol Molenda oraz płk rez. Paweł Dziuba wskazują na problem związany z prowadzeniem szkoleń wojskowych w domenie cyber przez prywatne podmioty. „Wcześniej prowadzone szkolenia dla NCBC i kandydatów do Wojsk Obrony Cyberprzestrzeni, ale również Sił Zbrojnych w zakresie kryptografii, IT i cyberbezpieczeństwa były w dużej mierze realizowane przez firmy komercyjne. Nie mogły one w pełni uwzględniać i zaspokajać potrzeb Sił Zbrojnych w tym obszarze" - tłumaczą przedstawiciele wojska. W związku z tym - jak dodają - konieczna będzie priorytetyzacja szkoleń ze szczególnym uwzględnieniem potrzeb NCBC. „Celem jest optymalizacja procesu szkoleń w sposób, który zapewni w najbliższej perspektywie realizację założeń szkoleniowych całego resortu" - tłumaczą gen. bryg. Karol Molenda oraz płk rez. Paweł Dziuba.

„W skali kraju niezmiernie istotne jest zapewnienie cyberodporności infrastruktury krytycznej na ataki hakerskie, w skali zaś Sił Zbrojnych – przeciwdziałanie zagrożeniom bezpieczeństwa informacji w wojskowych systemach teleinformatycznych" – wskazuje gen. Kosowski. „Bieżącym zagrożeniem jest dezinformacja związana z rozpowszechnianiem tzw. >fake newsów< ukierunkowana na kształtowanie opinii publicznej i morale Sił Zbrojnych. Połączenie jej z działaniami socjotechnicznymi pozwala na uwiarygodnienie przekazu. Można zaryzykować twierdzenie, że informacja jest w obecnie >bronią masowego rażenia<, a skutki jej oddziaływania również niekonwencjonalne, choć w innym, niż klasyczne znaczeniu" – podsumowuje generał.

„Zasadniczy trend, który daje się zaobserwować, już od kilku lat, to synchronizacja operacji na poziomie technicznym z operacjami na poziomie informacyjnym, co prowadzi do złożonych wielowymiarowych operacji CyberInfoOps. Polem walki staje się więc nie tylko twarda infrastruktura teleinformatyczna (operacje CyberOps), lecz wszystko, co do tej infrastruktury jest podłączone, a więc również ludzie (operacje InfoOps)" – wskazują ppłk Rafał Kasprzyk oraz prof. Zbigniew Tarapata. „Ten rodzaj zagrożeń jest szczególnie istotny, ponieważ nie dotyczy stricte systemu militarnego, ale całego systemu bezpieczeństwa państwa, będącego celem prowadzenia operacji CyberInfoOps w czasie "P" rozumianym klasycznie, z którym w rzeczywistości nigdy nie mamy do czynienia w cyberprzestrzeni" – dodają. „Zasadniczym zagrożeniem w obszarze cyberbezpieczeństwo pododdziałów i oddziałów Sił Zbrojnych jest z całą pewnością zapewnienie bezpieczeństwa łańcucha dostaw sprzętu i oprogramowania" – podkreślają przedstawiciele WAT.

Pełne odpowiedzi udzielone przez ekspertów znajdują się poniżej:

- Gen. dyw. Jarosław Gromadziński, dowódca 18. Dywizji Zmechanizowanej im. gen. broni Tadeusza Buka;
- Gen. bryg. Robert Kosowski, rektor-komendant Akademii Sztuki Wojennej;
- Kadm. Tomasz Szubrycht, rektor-komendant, Akademii Marynarki Wojennej;
- Gen. bryg. Karol Molenda, dyrektor Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni i płk rez. Paweł Dziuba, dyrektor Eksperckiego Centrum Szkolenia Cyberbezpieczeństwa;
- prof. Zbigniew Tarapata, dziekan Wydziału Cybernetyki WAT oraz Ppłk Rafał Kasprzyk, z-ca dziekana Wydziału Cybernetyki WAT.

Czytaj też: Wirus, wirus wszędzie! Jak dezinformacyjne narracje pokazały nasze słabości?