aut. Szymon Palczewski 08.07.2020

CYBER (R)EWOLUCJA MARYNARKI WOJENNEJ. SZANSA CZY ZAGROŻENIE?

Obecnie jesteśmy świadkami procesu ewolucji marynarki wojennej, której podstawowym elementem staje się nowoczesna technologia. Innowacyjne rozwiązania zapewniają niespotykane do tej pory możliwości, zmieniając kształt operacji prowadzonych na morzu. Jednak za całym spektrum korzyści związanych z unowocześnieniem marynarki wojennej kryje się szereg zagrożeń o znaczeniu krytycznym. „Systemy morskie należące do wojska będą głównym celem cyberataków" – ostrzegają specjaliści jednego z francuskich think-tanków.

Specjaliści Fondation pour la Research Stratégique (FRS) w raporcie „Cyber, a particular field of naval thought" jednoznacznie podkreślili, że cyberprzestrzeń jest „szczególnym polem walki" również w kontekście operacji prowadzonych na morzu. W tym zakresie nie można pomijać istotnej roli technologii, która dostarcza innowacyjne rozwiązania takie jak sztuczną inteligencję czy smart urządzenia.

Wszystkie wspominane wyżej narzędzia polegają na wymianie danych między kilkoma platformami. W związku z tym postęp technologiczny jest kluczowym aspektem cyberprzestrzeni rozpatrywanej jako domena działania sił zbrojnych. To wszystko sprawia, że innowacje obejmują również strefę działań na morzu, dlatego też muszą one być uwzględnione w strategii morskiej.

Cyber at Sea: redefinicja marynarki wojennej?

„Integracja sfery cyberprzestrzeni w ramach infrastruktury morskiej jest znacznie większym wyzwaniem technologicznym i ekonomicznym niż rozmieszczenie sieci telekomunikacyjnych na lądzie" – tłumaczą eksperci FRS.

Wykorzystanie nowoczesnych technologii na lądzie gwałtownie wzrosło w ciągu ostatnich kilku lat, dzięki znacznym postępom w dziedzinie przesyłu informacji. Swoje stanowisko specjaliści argumentują dostępem do Internetu w wymiarze globalnym. „W ciągu dziesięciu lat, od 2007 do 2017 roku, odsetek światowej populacji korzystającej z Internetu wzrósł z 20% do prawie 50%" – wskazują. Wynika to z faktu, że stacje bazowe mogą być umieszczane na lądzie niemalże w dowolnym miejscu. Na morzu jest to znacznie utrudnione, dlatego też efektywne działanie cyberprzestrzeni w tej domenie jest dużo bardziej wymagające.

Platformy morskie polegają głównie na technologiach satelitarnych w celu zapewnienia przesyłu danych, w tym komunikacji głosowej, nawigacji itd. Są to rozwiązania znacznie droższe i bardziej zaawansowane technologicznie.

Rozpatrując funkcjonowanie cyberprzestrzeni w ramach marynarki wojennej należy traktować ją jak „każdy system przemysłowy". Musi on być w stanie wykonywać szereg zadań związanych z różnorodnymi operacjami w możliwie jak najbardziej zautomatyzowany sposób. Przykładem mogą być

misje bojowe prowadzone przez siły zbrojne. W tym kontekście domena cyberprzestrzeni odgrywa jeszcze większą dolę, ponieważ musi integrować działanie wielu podsystemów.

To wszystko sprawia, że obserwujemy fundamentalną zmianę paradygmatu w dziedzinie marynarki wojennej. „Tam, gdzie dotychczas była ona oparta na braku komunikacji, teraz zmierza w kierunku obfitej komunikacji" – podkreślają eksperci w raporcie.

Co więcej, zmiany dotyczą również integracji z innymi platformami i systemami zdalnymi, takimi jak chociażby drony. To wszystko sprawia, że statki nie są już tylko pływającymi systemami informatycznymi, ale przede wszystkim rdzeniem lokalnych mini-sieci. Dzięki wykorzystaniu innowacyjnych urządzeń okręty marynarki wojennej mogą stać się zaawansowanymi platformami wielozadaniowymi, prowadzącymi operacje na niespotykaną do tej pory skalę.

Nowe możliwości. Nowe zagrożenia

Cyberewolucja marynarki wojennej stwarza nie tylko możliwości, ale rodzi również kolejne zagrożenia. W przypadku wysoce zautomatyzowanych statków ryzyko związane z przejęciem przez wroga ich podsystemów nabiera coraz bardziej krytycznego znaczenia. Wielość połączeń i rozbudowana infrastruktura cyfrowa stwarza wiele możliwości na przeprowadzenie złośliwych cyberataków.

Cyberbezpieczeństwo okrętów morskich musi opierać się na częstych aktualizacjach systemów, które stanowią fundament sprawnego wykonywania działań przez dana jednostkę. Nie należy zaniedbywać tego aspektu, ponieważ każda luka lub podatność może przynieść bardzo poważne konsekwencje.

„Systemy morskie należące do wojska będą głównym celem cyberataków" – nie mają wątpliwości eksperci. Wielość komponentów oraz powiązań z innymi urządzeniami sprawia, że są one wrażliwe na wyrafinowane działania wroga. Należy również pamiętać, że wdrażanie rozwiązań bazujących na sztucznej inteligencji nie rozwiąże wszystkich problemów związanych z cyberbezpieczeństwem marynarki wojennej.