

Obszar cybernetyczno-informacyjny: nowa formacja w Bundeswehrze

Justyna Gotkowska

5 kwietnia powołano nową formację w ramach Bundeswehry – obszar cybernetyczno-informacyjny (Cyber- und Informationsraum, CIR). Jest ona równorzędna z innymi wyodrębnionymi strukturami w niemieckich siłach zbrojnych (Inspektoratem Wsparcia i Służbą Medyczną), funkcjonującymi obok trzech rodzajów sił zbrojnych (Wojsk Lądowych, Sił Powietrznych i Marynarki Wojennej). CIR będzie skupiać jednostki zajmujące się kwestiami informatycznymi, bezpieczeństwem cybernetycznym, rozpoznaniem wojskowym i geoinformacją oraz prowadzeniem działań psychologicznych na szczeblu operacyjnym i taktycznym. CIR ma za zadanie wzmacniać ochronę sieci informatycznych i systemów uzbrojenia Bundeswehry, ale też rozwijać zdolności do ofensywnych działań w cyberprzestrzeni.

Nowo powstałemu Dowództwu CIR będą podlegać m.in.: Dowództwo Rozpoznania Strategicznego, Dowództwo ds. Technik Informatycznych, Centrum Geoinformacji i podporządkowane im jednostki – wcześniej znajdujące się w strukturach Inspektoratu Wsparcia. Po integracji ww. jednostek w tym roku CIR ma liczyć ok. 14 tysięcy pracowników cywilnych i wojskowych; w planach jest dalsza rozbudowa. Inspektorem CIR jest gen. Ludwig Leinhos, który w latach 2013–2016 był dyrektorem NHQC3S (NATO Headquarters Consultation, Command and Control Staff) w kwaterze głównej NATO w Brukseli.

Nie tylko Bundeswehrę, ale również niemiecki resort obrony objęły przekształcenia związane z wyodrębnieniem obszarów cyberbezpieczeństwa i IT. Od października 2016 roku w strukturach ministerstwa funkcjonuje Departament CIT (Cyber/IT), który zajmuje się planowaniem i wdrażaniem narodowej strategii cyberbezpieczeństwa w sferze obronności oraz jest odpowiedzialny za bezpieczeństwo cybernetyczne w sieciach informatycznych Bundeswehry.

Komentarz

- Stworzenie nowej formacji w Bundeswehrze pokazuje, że Niemcy traktują kwestie cybernetyczne i informacyjne jako coraz istotniejsze dla funkcjonowania Bundeswehry, bezpieczeństwa RFN i prowadzenia konfliktów zbrojnych. Świadczą o tym również zapisy Białej księgi polityki bezpieczeństwa i przyszłości Bundeswehry z lipca 2016 roku. Wyzwania dla bezpieczeństwa cybernetycznego i przestrzeni informacyjnej znalazły się w niej na drugim miejscu na liście zagrożeń (po międzynarodowym terroryzmie). Według

wypowiedzi minister obrony tylko w styczniu–lutym br. Bundeswehra stała się obiektem ponad 280 tys. ataków cybernetycznych. Stworzenie Dowództwa CIR w Bundeswehrze odzwierciedla również tendencje w NATO. Przestrzeń cybernetyczna została uznana w Sojuszu za sferę działań operacyjnych na szczycie w Warszawie w lipcu 2016 roku.

- Powołanie Dowództwa CIR należy rozpatrywać również jako kolejny projekt mający pozytywnie wpłynąć na wizerunek Ursuli von der Leyen jako efektywnej i nowoczesnej minister obrony. Von der Leyen koncentrowała się do tej pory na wprowadzeniu nowych, bardziej przejrzystych i efektywnych procedur w obszarze przetargów na uzbrojenie i sprzęt wojskowy dla Bundeswehry oraz na zwiększeniu atrakcyjności służby w siłach zbrojnych (m.in. poprzez lepsze możliwości łączenia życia rodzinnego z pracą).
- Mimo dużego szumu medialnego wokół powstania CIR stworzenie nowej formacji w Bundeswehrze polega głównie na podporządkowaniu Dowództwu CIR dowództw i jednostek już funkcjonujących w strukturach sił zbrojnych (co w sumie daje prawie 14 tys. liczebność). Defensywne i ofensywne zdolności cybernetyczne rozwijały do tej pory tylko dwie jednostki liczące ok. 60 osób: zespół CERTBw (Computer Emergency Response Team) powstały w 2002 roku i reagujący na incydenty naruszające bezpieczeństwo w sieci; oraz jednostka CNO (Computer-Netzwerk-Operationen) podlegająca Dowództwu Rozpoznania Strategicznego i wypełniająca zadania walki elektronicznej. W przyszłości obie mają zostać rozbudowane i przekształcone odpowiednio w Centrum Bezpieczeństwa Cybernetycznego i Centrum Operacji Cybernetycznych. Według informacji medialnych CNO miała po raz pierwszy przeprowadzić atak cybernetyczny w 2015 roku (na sieć afgańskiego operatora telefonii komórkowej), w ramach niemieckich działań mających na celu uwolnienie obywatela RFN porwanego w Afganistanie.
- Niemiecka armia ma i nadal będzie mieć problemy z rozbudową defensywnych i ofensywnych zdolności cybernetycznych. Powodem są głównie trudności z pozyskaniem specjalistów IT, związane z konkurencyjnym rynkiem pracy w tym obszarze oraz małą popularnością społeczną służby w Bundeswehrze. Niemieckie Ministerstwo Obrony planuje więc otwarcie w 2018 roku nowego kierunku studiów „Cyber-Studies” na Uniwersytecie Bundeswehry w Monachium w celu pozyskania nowego personelu. Ponadto w marcu br. inspektor generalny Bundeswehry opublikował koncepcję dotyczącą wsparcia *cyber-community* w Bundeswehrze poprzez przyciągnięcie do współpracy żołnierzy rezerwy i środowisk niezwiązanych dotychczas z siłami zbrojnymi.
- Powstanie CIR ożywiło w RFN dyskusję na temat parlamentarnej zgody na prowadzenie ataków cybernetycznych przez Bundeswehrę (zgoda Bundestagu wymagana jest na prowadzenie operacji wojskowych poza granicami kraju). Z jednej strony możliwość prowadzenia ofensywnych działań w cyberprzestrzeni będzie prawdopodobnie ujęta w proponowanych w przyszłości przez rząd i zatwierdzanych przez Bundestag mandatach operacji zagranicznych (np. w Afryce czy na Bliskim Wschodzie). Z drugiej strony, według Ursuli von der Leyen Bundeswehra powinna mieć również możliwość „ofensywnej obrony”, tzn. prowadzenia w czasie pokoju kontrataków odpowiadających na agresywne działania cybernetyczne państw trzecich, które zagrażają zdolnościom do wypełniania zadań i gotowości bojowej niemieckich sił zbrojnych. W ramach obecnych rozwiązań prawnych Bundeswehra może wspierać inne organy administracji publicznej w

przeciwdziałaniu atakom cybernetycznym.

Aneks: Struktura Obszaru Cybernetyczno-Informacyjnego Bundeswehry (CIR)

