Janusz MIRASZEWSKI

60-LECIE INFORMATYKI WOJSKOWEJ W REGIONIE BYDGOSZCZ

W maju 2026 roku w Regionalnym Centrum Informatyki Bydgoszcz obchodziliśmy 60-lecie Informatyki Wojskowej w Regionie Bydgoszcz – sześć dekad służby, odpowiedzialności i nieprzerwanego rozwoju w obszarze informatyki i systemów teleinformatycznych. To czas, który buduje historię, ale przede wszystkim świadczy o trwałości naszej misji i znaczeniu, jakie pełnimy w strukturach Sił Zbrojnych. Od momentu powstania w 1966 roku „Zespołu" jednym z kluczowych zadań było wsparcie administracji wojskowej oraz zapewnienie ciągłości działania systemów teleinformatycznych. W realiach współczesnego pola walki i funkcjonowania państwa to właśnie sprawna, bezpieczna i niezawodna infrastruktura informatyczna stanowi fundament dowodzenia, komunikacji oraz podejmowania decyzji.

Nasza służba często pozostaje niewidoczna, ale jej znaczenie jest nie do przecenienia. To my dbamy o to, aby systemy działały bez zakłóceń, aby informacje docierały na czas i w sposób bezpieczny, aby administracja wojskowa mogła funkcjonować sprawnie w każdych warunkach – zarówno w czasie pokoju, jak i w sytuacjach kryzysowych.

Przez 60 lat zmieniały się technologie, skala działania oraz charakter zagrożeń. Od prostych systemów łączności i przetwarzania danych przeszliśmy do zaawansowanych, zintegrowanych środowisk teleinformatycznych. Niezmienne pozostały jednak wartości, które nas definiują – dyscyplina, odpowiedzialność, profesjonalizm i gotowość do działania w każdej sytuacji.

Utrzymanie systemów teleinformatycznych w strukturach wojskowych to zadanie wymagające najwyższej precyzji, niezawodności i ciągłej gotowości. To służba, w której nie ma miejsca na błędy, a każda decyzja i każde działanie mają realny wpływ na bezpieczeństwo naszego kraju.

Zespół Zarządzania Wsparciem Teleinformatycznym (ZZWT) w Bydgoszczy jest ostatnią nazwą instytucji informatycznych funkcjonujących w latach 1966-2017 jako samodzielna jednostka w kompleksie wojskowym przy ul. Dwernickiego w Bydgoszczy. Rok 1966 przyjęto za symboliczny początek informatyzacji wojskowej regionu Bydgoszcz. Instytucja ta, w wyniku zmian

podporządkowania oraz zmian organizacyjno-etatowych przyjmowała następujące nazwy:

Stacja Maszyn Licząco-Analitycznych (SML-A) – 1966÷1968;

Ośrodek Przetwarzania Informacji Pomorskiego Okręgu Wojskowego (OPI POW) – 1968÷1975;

Zespół Informatyki Pomorskiego Okręgu Wojskowego (ZI POW) – 1975-2007;

Zespół Wdrożeniowy Nr 2 (ZW Nr 2) – 2007÷2011;

Zespół Zarządzania Wsparciem Teleinformatycznym w Bydgoszczy (ZZWT) – 2011÷2017.

Zmiany strukturalne oraz charakter prowadzonej działalności, powodowane były potrzebami Sił Zbrojnych oraz ciągłym rozwojem technik i technologii informatycznych. Głównym zadaniem wszystkich tych jednostek było przyczynianie się do informatyzacji Sił Zbrojnych.

Stacja Maszyn Licząco-Analitycznych (1966–1968)

Historia powstania organu wykonawczego informatyki wojskowej w regionie bydgoskim wiąże się z Pomorskim Okręgiem Wojskowym. W dniu 04.05.1966 r. rozkazem Dowódcy POW została sformowana grupa organizacyjno–przygotowawcza pod kierownictwem mjr. Andrzeja Różań-skiego. Grupa działała na terenie Dowództwa POW, gdzie we wrześniu tego samego roku utworzyła Stację Maszyn Licząco-Analitycznych (SML-A). Etat nowej instytucji obejmował 17 żołnierzy zawodowych oraz 17 pracowników wojska.

SML-A została w pełni zorganizowana i przekazana do eksploatacji w dniu 15.03.1967 r. Uroczystego otwarcia hali „maszyn ciężkich” (taką nazwę nosił wówczas ośrodek przetwarzania danych) dokonał Szef Sztabu POW gen. bryg. Józef Stebelski. W dniu 02.01.1968 r. obowiązki Szefa SML-A objął ppłk Sergiusz Cielesz. W marcu 1967 roku zostały uruchomione i przekazane do eksploatacji maszyny i urządzenia stanowiące wyposażenie hali maszyn ciężkich i hali maszyn lekkich. Maszyny licząco-analityczne były urządzeniami liczącymi oraz wspomagającymi obliczenia używające jako nośnik informacji kartę perforowaną. Oprogramowanie polegało na odpowiednim upięciu kabli tablicy programowej wstawianej do tabulatora.

Wyposażenie SML-A

Hala maszyn	Urządzenia
maszyny lekkie	dziurkarki i sprawdzarki kart perforowanych perforatory i czytniki taśmy papierowej
maszyny ciężkie	sortery – urządzenia służące do rozdzielania kart reproducery – urządzenia do kopiowania kart tabulatory – do drukowania zawartości kart kolatory – do łączenia kart w pliki według określonych reguł

Ośrodek Przetwarzania Informacji POW (1968–1975)

W lipcu 1968 r. powołana została grupa organizacyjno-przygotowawcza Ośrodka Przetwarzania Informacji. Kierownikiem grupy został kpt. Tadeusz Kaszubski. Grupa przystąpiła do opracowania projektów koncepcyjnych systemów na małe Elektroniczne Maszyny Cyfrowe. Pod koniec 1968 roku utworzono Ośrodek Przetwarzania Informacji POW (OPI), którego Szefem został ppłk Sergiusz Cielesz. OPI składał się z kilku wydziałów: projektowania, programowania, przygotowania danych, eksploatacji oraz wydziału technicznego. Informatyka wojskowa w regionie zaczęła się rozwijać w coraz szybszym tempie. Zapotrzebowanie na usługi informatyczne rosło. W ślad za tym projektowano i wdrażano do użytku coraz więcej systemów praca na 3 zmiany).

Pierwsza mała elektroniczna maszyna cyfrowa, produkcji ELWRO WROCŁAW, wykonana w technologii tranzystorowej, pojawiła się w OPI POW w styczniu 1969 roku. Był to, współpracujący z maszynami licząco-analitycznymi, Elektroniczny Kalkulator Dziesiętny (EKD) ODRA-1103 przeznaczony do przetwarzania danych. Eksploatację EKD ODRA-1103 zakończono w 1974 roku. Przełom w rozwoju narodowych systemów dowodzenia nastąpił po skonstruowaniu i wyprodukowaniu przez ELWRO w 1967 roku komputera ODRA 1204. To przełomowe wydarzenie przyczyniło się do rozpoczęcia prac badawczych dotyczących zbudowania rodzimego zautomatyzowanego systemu dowodzenia. W latach 70. w Wojskowej Akademii Technicznej podjęto prace nad zautomatyzowanym systemem dowodzenia szczebla operacyjno-taktycznego o kryptonimie CYBER-W.

Unikatowy system wdrożono do pracy operacyjnej w 1983 roku na SD 2 KOPK w Bydgoszczy.

Podstawowe parametry EKD ODRA-1103 (1969-1974)

Element / parametr systemu	Specyfikacja
Jednostka centralna	Pamięć operacyjna ferrytowa 1024 słowa (8 bit.), czas dostępu 8 μs
Szybkość liczenia	5 000 dodawań na sekundę
Urządzenia zewnętrzne	Pamięć zewnętrzna bębnowa – 256K słów (8 bitowych), czas dostępu 10 ms
Urządzenia we/wy	Współpraca z maszynami analityczno-liczącymi
Programowanie	Język wewnętrzny (PJN – Podstawowy Język Numeryczny) z adresacją w systemie ósemkowym

Zespół Informatyki POW (1975–2007)

W marcu 1975 r. rozkazem Dowódcy POW, Ośrodek Przetwarzania Informacji został przeformowany w Zespół Informatyki POW. Istotną zmianą był rozdział na dwa piony funkcjonalne: Projektowo-Programowy i Ośrodek Przetwarzania Informacji. Na stanowisko Kierownika ZI POW wyznaczony został płk Sergiusz Cielesz. W kolejnych latach ZI POW podlegał zmianom organizacyjnym i kadrowym, łącznie ze zmianami na stanowiskach kiero-wniczych. Ciągle jednak podlegał Dowództwu POW. Merytorycznie łączony był z Oddziałem V Sztabu POW, a na szczeblu Sztabu Generalnego – z Zarządem XIV. W 1993 roku Zespół zostaje podporządkowany pod utworzone w Dowództwie POW Szefostwo Wojsk Łączności i Informatyki. Jest to pierwsza formalna integracja informatyki z łącznością, przynajmniej w naszym regionie.
Elektroniczna Maszyna Cyfrowa ODRA-1304, tranzystorowy komputer drugiej generacji, został oddany do eksploatacji w OPI POW w marcu 1972 roku. Uruchomienie zestawu EMC ODRA-1304 umożliwiło realizację prac projektowo-programowych. Już w 1972 roku powstały pierwsze systemy informatyczne autorstwa OPI POW.

Podstawowe parametry EMC ODRA-1304

Element / parametr sys-temu	Specyfikacja
Jednostka centralna	pamięć operacyjna ferrytowa 16 Ksłów następnie 32 Ksłowa czas dostępu 6 μs konsola operatora CONSUL
Pamięć masowa	pamięć taśmowa PT-2 albo PT-3 7 MB pamięć dyskowa (bębnowa) 8 MB
Szybkość operacji	50 000 dodawań na sekundę
Urządzenia we/wy	monitor – elektryczna maszyna do pisania (dalekopis) czytnik taśmy perforowanej CT-304 czytnik kart perforowanych CK-304 perforator taśmy PT-304 drukarka wierszowa DW 304 terminale
Programowanie	Języki programowania: Fortran1900, PLAN, ALGOL, COBOL
System opera-cyjny	EXEC



Hala EMC przed uruchomieniem zestawu ODRA 1304



Wydział Techniczny przekazuje do eksploatacji zestaw ODRA-1304



Jednostka centralna ODRA-1305

Elektroniczna Maszyna Cyfrowa ODRA-1305 została przekazana do eksploatacji w ZI POW w czerwcu 1977 roku. Był to komputer III generacji zbudowany na układach scalonych TTL. ODRA-1305 podobnie jak ODRA-1304 była zgodna logicznie i programowo z angielskim komputerem ICL 1904. Była jednak szybsza i znacznie mniejsza niż pierwowzór

Podstawowe parametry EMC ODRA-1305 (1977÷1999)

Element / parametr systemu	Specyfikacja
Jednostka centralna	pamięć operacyjna ferrytowa i półprzewodnikowa – 32 do 256 Ksłów; cykl odczytu pamięci operacyjnej 1 µs; słowo maszynowe długości 24 bity;
Pamięć masowa	pamięć taśmowa PT-3 7 MB; pamięć dyskowa (bębnowa) 8 MB;

Interfejsy urządzeń zewnętrznych	kanał priorytetowy – współpraca z Systemem Modułowej Automatyki; kanał monitora (obsługa konsoli FACIT) – 2 kanały; kanał znakowy o szybkości 100 000 znaków 6-bitowych/sekundę (czytnik/ perforator taśmy papierowej lub kart, drukarka wierszowa itp.) – 10 kanałów; kanał multiplekserowy – kanał znakowy mogący obsługiwać multiplekser wraz z maksymalnie 32 terminalami; kanały autonomiczne o szybkości 500 000 znaków 6-bitowych /sekundę (pamięci taśmowe PT-3, napędy dyskowe, itp.); kanały znakowe (zewnętrzne) – 7 kanałów.

W 1982 roku na zestawie ODRA-1305 uruchomiono system operacyjny GEORGE-3. Wdrożenie tego systemu umożliwiło współbieżne przetwarzanie systemów użytkowych. Zwiększyło to efektywność pracy zestawu, dzięki czemu czas przetwarzania spadł poniżej dwóch zmian.





Pamięci taśmowe i dyskowe zestawu ODRA-1305

Od 1992 roku następowała stopniowa modernizacja technologii przetwarzania na zestawie ODRA-1305 polegająca na:

- przekazywaniu zbiorów danych i wynikowych na dyskietkach, co zmniejszyło ilość wydruków;
- zastąpieniu starych urządzeń wejścia/wyjścia, takich jak karty i taśmy perforowane emulacją mikrokomputerową.

Po ponad 20 letnim okresie eksploatacji ostateczne zakończenie pracy zestawu ODRA-1305 nastąpiło w 1999 roku. Symbolicznego wyłączenia zestawu dokonał dowódca POW gen. dyw. Tadeusz Bazydło.



Przetwarzanie danych na hali EMC

W 1979 roku Zespół Informatyki wyposażono w Ruchomy Ośrodek Obliczeniowy (ROO), którego głównym elementem była jednostka centralna EMC ODRA-1325. Zestaw komputerowy zainstalowany był w specjalnie do tego przeznaczonym kontenerze, całość była zamontowana na podwoziu samochodu Jelcz.

Podstawowe parametry EMC ODRA-1325 (1979-1989)

Element / parametr systemu	Specyfikacja
Jednostka centralna	pamięć operacyjna 32 Ksłów cykl odczytu pamięci operacyjnej: 1 µs słowo maszynowe długości 24 bity
Pamięć masowa	pamięć dyskowa (2 jednostki po 8 MB)
Urządzenia	monitor ekranowy, terminale wynośne (DZM, monitory ekranowe), urządzenie transmisji danych, klimatyzator
System operacyjny	MINIMOP

MERA-9150 (1980÷1999)

W 1980 roku ZI POW wyposażono w pierwszy wielostanowiskowy komputerowy system rejestracji danych MERA-9150.

System składał się z:

- jednostki centralnej, zawierającej moduł procesora, układy wejścia/wyjścia, zasilacz, zespół 3 dysków twardych 21 MB każdy;
- pamięci taśmowej PT-105;
- końcówek operatorskich z 71 klawiszową klawiaturą oraz monitorem 9 cali.

Uruchomiony zestaw posiadał 10 stanowisk do wprowadzania informacji. Był to przełom w sposobie wprowadzania danych do komputera ODRA-1305 – wyeliminowano karty perforowane jako podstawowy nośnik informacji. Dane z dokumentów wprowadzano bezpośrednio na taśmę magnetyczną.

Zestaw przekazano do eksploatacji w grudniu 1981 r. Drugi zestaw MERA-9150 służył między innymi do kontroli dostępu na teren dowództwa POW. Współpracował z czytnikami kart zintegrowanych z przepustkami osobowymi i umożliwiał rejestrację czasu pracy.



Końcówka operatorska MERA-9150



Pamięć taśmowa PT 105-2 - MERA 9150

W drugiej połowie lat 80. XX wieku następuje rewolucja w zakresie możliwości wykorzystania i powszechnego dostępu do komputerów. Do czasu pojawienia się w Polsce mikrokomputerów personalnych klasy IBM PC, od 1984 r. w niewielkich ilościach przekazywano do ZI POW kolejne generacje pierwszych

polskich rozwiązań techniczno-technologicznych. W 1984 roku ZI POW otrzymał pierwszy mikrokomputer PSPD-90, na który opracowano oprogramowanie wspomagające pracę dyżurnej służby operacyjnej. Rozwiązanie to przeprogramowano w 1986 roku na mikrokomputer następnej generacji MK-4502. W 1986 roku otrzymano również 6 mikrokomputerów UNIPOLBRIT, które po zainstalowaniu oprogramowania szkolnego przekazano do pracowni mikrokomputerowej w klubie POW – udzielając pomocy w jej organizacji i prowadzeniu zajęć z młodzieżą.

W latach 1987–1991 pojawiają się pierwsze komputery osobiste oparte na procesorach firmy Intel klasy X86 i innych, zgodnych: z IBM PC/XT, IBM PC/AT oraz mikrokomputery AMSTRAD. ZI POW zostaje stopniowo wyposażany w nowe komputery działające pod kontrolą systemu DOS. Zmieniło to diametralnie sposób pracy programistów, zaczęły powstawać pierwsze autorskie programy Zespołu przeznaczone na komputery osobiste.

Podstawowe parametry modelu PC/XT 286 z roku 1990

Element / parametr systemu	Specyfikacja
Procesor	Intel 80286 6 MHz
RAM	640 kB
Dysk twardy	10 – 20 MB
Pamięć zewnętrzna	stacja dyskietek 5,25”, 1.2 MB
System operacyjny	DOS 2.0, DOS 3.2.

W 1992 roku nastąpił istotny postęp w wyposażeniu w komputery osobiste ZI POW oraz komórek funkcjonalnych Sztabu POW. Dowódca Pomorskiego Okręgu Wojskowego przydzielił 1 mld złotych na pozyskanie sprzętu mikrokomputerowego z których zakupiono kilkanaście zestawów 386/SX i 386/DX oraz wyposażono i uruchomiono ośrodek szkolenia komputerowego przy ZI POW. W następnych latach pojawiły się mikro-komputery kolejnych generacji (klasy 486, Pentium) charakteryzujące się dużą mocą obliczeniową i nowymi możliwościami multimedialnymi. W Zespole prowadzone były prace

projektowo-programowe i eksploatacyjne równolegle na mikrokomputerach wyposażonych w system operacyjny DOS i UNIX.

W 1993 roku w ZI POW został uruchomiony zestaw komputerowy nowej generacji IBM AS/400 model 9406/F-45. AS/400 zbudowany był na procesorze Power PC z techniką RISC i sterowany za pomocą systemu operacyjnego OS/400.

Komputer AS/400 został podłączony do pierwszej sieci komputerowej dowództwa POW, której uruchomienie nastąpiło w 1994 roku. W ZI POW opracowano pierwszy sieciowy system dotyczący gotowości bojowej oraz wykorzystania czasu pracy. Podstawowymi systemami eksploatowanymi na komputerze AS/400 były systemy opracowane dla służb logistyki.

Zespół Wdrożeniowy Nr 2 (2007–2011)

Rok 2007 przynosi radykalne zmiany w podległości służbowej i strukturach Zespołu. Został on podporządkowany Dyrektorowi Departamentu Informatyki i Telekomunikacji Ministerstwa Obrony Narodowej (DIiT). Zmienił też nazwę na Zespół Wdrożeniowy Nr 2. Nazwa ta mogła sugerować zmarginalizowanie znaczenia Zespołu w procesie informatyzacji wojskowej regionu sprowadzając go do roli wdrożeniowca. W istocie – globalizacja, podobnie jak w innych dziedzinach, dotknęła też informatyki wojskowej. Główne kierunki rozwoju były wytyczane centralnie, co nie oznacza, że Zespół był traktowany przedmiotowo. Nadal miał realny wpływ na kreowanie rzeczywistości informatycznej w regionie bydgoskim.

Zespół Zarządzania Wsparciem Teleinformatycznym (2011–2017)

Po czterech latach, w 2011 roku, ZW Nr 2 przeformowano w Zespół Zarządzania Wsparciem Teleinformatycznym w Bydgoszczy (ZZWT), który w dalszym ciągu wykonywał swoje zadania zgodnie z przeznaczeniem. Postępujący wzrost świadomości użytkowników oraz wprowadzenie etatów informatycznych w jednostkach wojskowych (administratorzy lokalni, lokalne grupy wdrożeniowe) spowodowały znaczne usamodzielnienie jednostek w zakresie wdrażania i eksploatacji systemów informatycznych. Proces ten jednak w dalszym ciągu wymagał wsparcia i koordynacji.

W latach 2008-2012 przekazano z innych instytucji do ZZWT w Bydgoszczy 3 zestawy IBM AS/400 wraz z systemami logistycznymi. Od 2012 roku wszystkie systemy logistyczne działające na AS/400 były przetwarzane

w ZZWT w Bydgoszczy, który stał się jedyną instytucją w WP eksploatującą tego typu zestaw. Na podstawie Rozkazu Szefa Inspektoratu Wsparcia Sił Zbrojnych w listopadzie 2016 r. zakończono eksploatację systemów klasy LO-GIS, co spowodowało wycofanie komputera IBM AS/400 działającego od 1993 roku. Ostateczny demontaż sprzętu nastąpił w grudniu 2017 roku.





Zestaw minikomputerowy IBM AS/400

W dniu 31.12.2017 r. ostatni Komendant Zespołu – ppłk Andrzej Malinowski „gasi światło". ZZWT w Bydgoszczy zostaje rozformowany i wchodzi w skład nowej struktury – Regionalnego Centrum Informatyki Bydgoszcz.

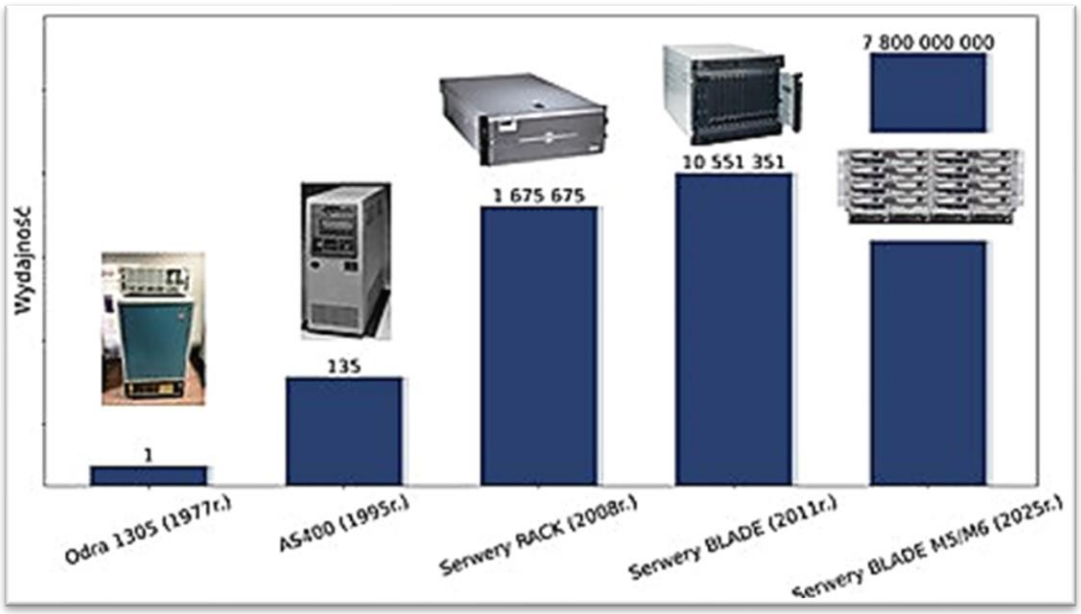
Demontaż Zestawu IBM AS/400



Po 2011 roku infrastruktura serwerowa podlegała sukcesywnym modernizacjom:

- rok 2013 – rozbudowano serwerownię o macierz Hitachi VSP o pojemności 350TB (352 dyski w tym w technologii SSD), która w 2015 roku została powiększona do 555TB (462 dyski w tym w technologii Flash Module Drive);
- rok 2014 – rozbudowano macierz IBM DS5100 do pojemności 105TB (190 dysków);
- rok 2015 – rozpoczęto modernizację pomieszczeń serwerowni, systemu zasilania oraz systemu chłodzenia, inwestycja została zakończona we wrześniu 2016 roku;
- rok 2016 – uruchomiono Data Center dla systemów jawnych i niejawnych.

Wydajność serwerowni w Bydgoszczy w latach 1977÷2025 w porównaniu do Odry-1305



Dynamika rozwoju techniki komputerowej, w okresie od powstania w 1966 roku Stacji Maszyn Licząco-Analitycznych do dnia dzisiejszego, jest nieporównywalna z innymi dziedzinami. W ciągu 60 lat informatyka przeszła od wiedzy dostępnej dla nielicznych specjalistów przez erę komputerów osobistych, rewolucję internetową i mobilną aż do ery danych, chmury i sztucznej inteligencji.

W regionie bydgoskim, w wojskowych centrach przetwarzania danych – serwerowniach, czy jak je wcześniej nazywano – ośrodkach obliczeniowych lub halach maszyn, na przestrzeni 60 lat znalazł zastosowanie sprzęt informatyczny i systemy operacyjne następujących generacji:

- maszyny licząco-analityczne oraz Elektroniczny Kalkulator Dziesiętny ODRA-1103 (1966÷1971);
- Elektroniczne Maszyny Cyfrowe: ODRA-1304, ODRA-1305, ODRA-1325 oraz MERA-9150 (1972÷1999);
- mikrokomputery klasy IBM PC (od końca lat 80. XX wieku);
- komputer AS/400 (od 1992 roku);
- urządzenia sieciowe: routery, switche, mediakonwertery, modemy, szyfratory (od połowy lat 90. XX wieku);
- serwery (RACK, BLADE), macierze dyskowe (początek XXI w.);
- CISCO ACI dla rozwiązania Data Center (od 2021 r.);
- SDD-WAN – wirtualna nakładka na fizyczne sieci teleinformatyczne (od 2025 r.);
- klienckie systemy operacyjne: DOS 2.0, DOS 3.0, DOS 3.2, UNIX, AIX, Windows 3.0, 3.1, Windows 95, Windows 98, Windows NT 3.5,, 4.0, Windows 2000, Windows Millenium, Windows XP, Windows Vista, Windows 7, Windows 10; Windows 11;
- serwerowe systemy operacyjne: Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows Server 2025.

Regionalne Centrum Informatyki Bydgoszcz (RCI Bydgoszcz) rozpoczęło działalność 1 stycznia 2018 r. Obecnie podlega bezpośrednio Dowództwu Komponentu Wojsk Obrony Cyberprzestrzeni z siedzibą w Legionowie. RCI Bydgoszcz stanowi kluczowy element systemu wsparcia teleinformatycznego Sił Zbrojnych RP, łącząc tradycję z nowoczesnością i aktywnie budując zdolności obronne państwa w cyberprzestrzeni. Siedziba RCI Bydgoszcz znajduje się w Bydgoszczy na terenie jednego z największych garnizonów wojskowych w Polsce, w którym stacjonują liczne jednostki i instytucje RON oraz struktury sojusznicze NATO. Podległe komórki organizacyjne rozmieszczone są na terenie czterech województw: kujawsko-pomorskiego, zachodniopomorskiego, wielkopolskiego i pomorskiego.

Stoimy dziś w obliczu nowych wyzwań, które redefiniują współczesne środowisko bezpieczeństwa. Cyberprzestrzeń stała się kolejnym wymiarem działań operacyjnych – obok lądu, morza i powietrza. To obszar, w którym zagrożenia są dynamiczne, często niewidoczne, ale niezwykle groźne.

Dlatego rozwój zdolności w zakresie cyberbezpieczeństwa jest dziś jednym z naszych priorytetów. Musimy nie tylko chronić infrastrukturę i dane, ale również budować zdolności do wykrywania, reagowania i przeciwdziałania zagrożeniom w czasie rzeczywistym.

Równocześnie dynamiczny rozwój sztucznej inteligencji otwiera nowe możliwości dla Sił Zbrojnych. AI może wspierać analizę informacji, automatyzację procesów, zwiększać efektywność działania systemów oraz wspomagać podejmowanie decyzji. To narzędzie, które – właściwie wykorzystane – stanie się jednym z kluczowych elementów przewagi technologicznej.

Przyszłość RCI Bydgoszcz to dalszy rozwój kompetencji w obszarach cyber i AI, budowanie nowoczesnych, odpornych systemów oraz kształcenie kadr gotowych sprostać wyzwaniom współczesnego pola walki.

Jubileusz 60 lat Informatyki Wojskowej jest dla RCI Bydgoszcz powodem do dumy, ale również zobowiązaniem – do dalszej służby, doskonalenia i umacniania bezpieczeństwa naszej Ojczyzny.












Zdjęcia z uroczystości 60-lecia Informatyki Wojskowej w Regionie Bydgoszcz. Wśród uczestników i wyróżnionych znalazł się przedstawiciel Światowego Związku Polskich Żołnierzy Łączności p. Wojciech Reszka.





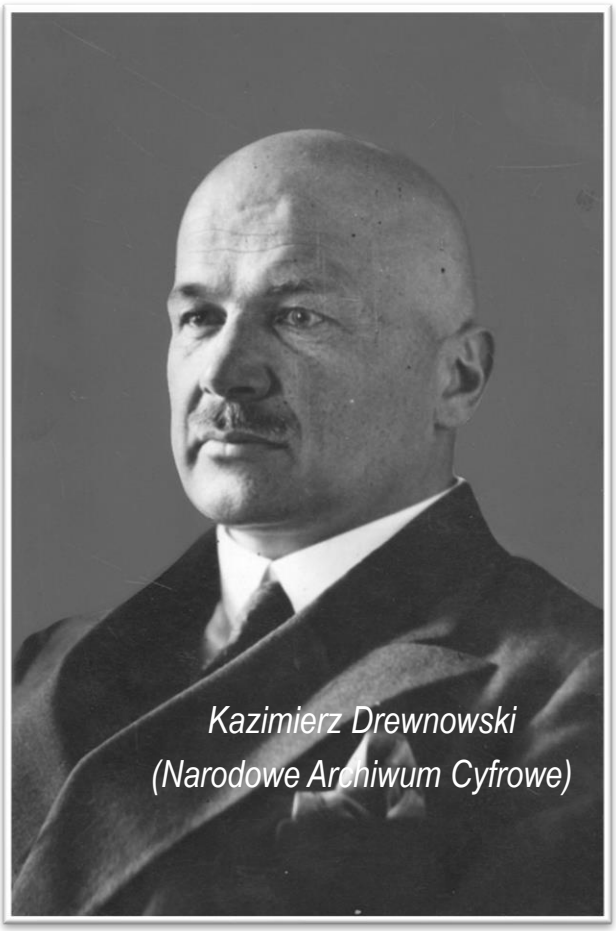

WSPOMIENIA ŁĄCZNOŚCIOWCÓW

Kamila OCHWAT

PATRON REGIONALNEGO CENTRUM INFORMATYKI WARSZAWA

Płk prof. inż. Kazimierz Bolesław DREWNOWSKI (4.03.1881-22.08.1952) –w marcu 2026 roku obchodzono 145. rocznicę urodzin patrona Regionalnego Centrum Informatyki Warszawa.

Urodzony w Stanisławowie - syn Ignacego, inżyniera kolejowego. Studia odbył na politechnikach we Lwowie (1903), Zurychu (1905) i na politechnice w Darmstadt (1914).



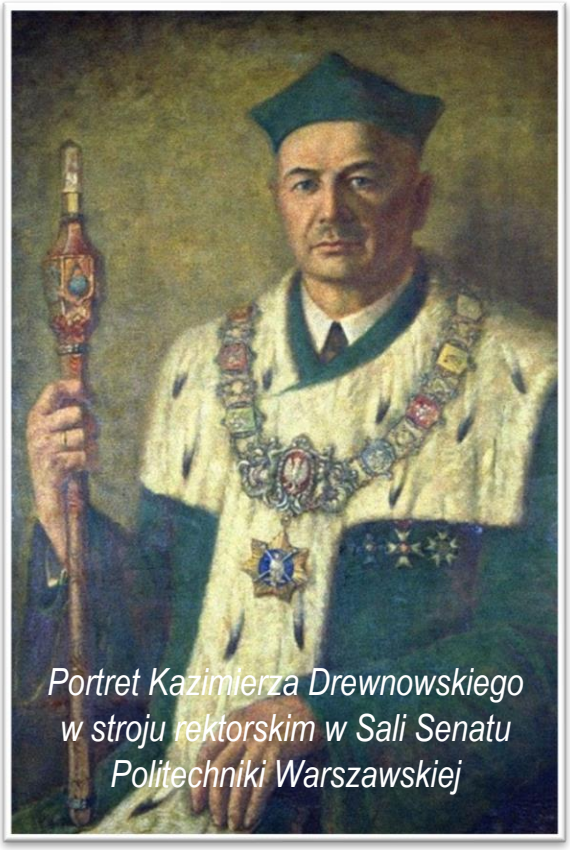
Kazimierz Drewnowski
(Narodowe Archiwum Cyfrowe)

Legionista, wybitny inżynier miernictwa elektrycznego, techniki wysokich napięć i elektrotechniki. Pułkownik odrodzone-go Wojska Polskiego i twórca Wojsk Łączności po 1918 roku. Dziekan Wydziału Elektrycznego a następnie Rektor Politechniki Warszawskiej. Taternik i miłośnik gór.

Decyzją Ministra Obrony Narodowej Nr 9/MON z dnia 18 stycznia 1999 imię płk. prof. inż. Kazimierza Drewnowskiego otrzymał Centralny Węzeł Łączności Ministerstwa Obrony Narodowej w Warszawie. Jego imieniem nazwane zostały ulice w Warszawie, Poznaniu i Zegrzu.

Jest patronem Zespołu Szkół Energetycznych w Lublinie (od 1994 r.), a także Regionalnego Centrum Informatyki Warszawa (od 2019 r.).

Działalność wojskowa Kazimierza Drewnowskiego w latach 1914–1922



Portret Kazimierza Drewnowskiego w stroju rektorskim w Sali Senatu Politechniki Warszawskiej

Wybuch I wojny światowej w 1914 r. otworzył nowy etap w życiu Kazimierza Drewnowskiego. Dotychczas związany głównie z działalnością techniczną i naukową, zaangażował się w działania niepodległościowe, wstępując do Legionów Polskich. Jego przygotowanie inżynierskie sprawiło, że został skierowany do organizacji wojskowych służb łączności, które odgrywały coraz większą rolę w nowoczesnych działaniach wojennych.

W okresie służby legionowej Drewnowski uczestniczył w tworzeniu i rozbudowie systemów komunikacji wykorzystywanych przez oddziały wojskowe. Na początku XX wieku skuteczność dowodzenia zależała w coraz większym stopniu od sprawnego funkcjonowania sieci telefonicznych i telegraficznych. Rozwój techniki wojskowej powodował, że służby łączności stawały się jednym z podstawowych elementów organizacji armii, a specjaliści posiadający wykształcenie techniczne byli szczególnie cenieni.

Po odzyskaniu przez Polskę niepodległości w listopadzie 1918 r. Drewnowski pozostał w służbie wojskowej. W nowo tworzącym się Wojsku Polskim powierzono mu organizację struktur odpowiedzialnych za łączność.

Zadanie to było niezwykle trudne ze względu na konieczność połączenia doświadczeń i wyposażenia pochodzącego z armii trzech państw zaborczych. W latach 1919–1921 pełnił funkcję pierwszego dowódcy Wojsk Łączności Wojska Polskiego oraz inspektora tej formacji.

Szczególne znaczenie działalność Drewnowskiego miała podczas wojny polsko-bolszewickiej. W konflikcie tym sprawna wymiana informacji pomiędzy sztabami a oddziałami walczącymi na rozległym froncie miała zasadniczy wpływ na skuteczność działań bojowych. Organizowane przez niego jednostki

łączności zapewniały funkcjonowanie sieci telefonicznych, telegraficznych oraz innych środków komunikacji wykorzystywanych przez armię polską. Dzięki temu możliwe było sprawniejsze dowodzenie oraz koordynacja działań operacyjnych.

Równolegle z działalnością organizacyjną Drewnowski uczestniczył w szkoleniu kadry technicznej wojsk łączności. Tworzenie nowoczesnej armii wymagało bowiem odpowiednio przygotowanych specjalistów zdolnych do obsługi coraz bardziej zaawansowanych urządzeń technicznych. Jego doświadczenie inżynierskie oraz umiejętności organizacyjne przyczyniły się do ukształtowania podstaw polskich wojsk łączności w pierwszych latach niepodległości.

Za zasługi dla Wojska Polskiego oraz udział w walkach o niepodległość został odznaczony 7 maja 1922 r. Orderem Wojennym Virtuti Militari V klasy. Odznaczenie to należało do najwyższych wyróżnień wojskowych przyznawanych za wybitne zasługi dla państwa i armii. W tym samym okresie Drewnowski osiągnął stopień pułkownika oraz pełnił funkcję komendanta Głównej Szkoły Artylerii i Inżynierii w Warszawie.

Działalność naukowa i dydaktyczna Kazimierza Drewnowskiego w Politechnice Warszawskiej

Zdobyte doświadczenia wojskowe wykorzystał następnie w działalności naukowej i organizacyjnej na Politechnice Warszawskiej, gdzie odegrał istotną rolę w rozwoju polskiej elektrotechniki i szkolnictwa technicznego.

W Politechnice Warszawskiej był współinicjatorem powstania Wydziału Elektrycznego. Zorganizował Zakład Miernictwa Elektrycznego i Wysokich Napięć (1923)oraz Laboratorium Wysokich Napięć - pierwszą tego typu placówkę w Polsce. Wykładał podstawy elektrotechniki i miernictwo elektrotechniczne.

Był pionierem oryginalnych metod badawczych pola elektrycznego i nowoczesnych metod pomiarowych. Stworzył 3 szkoły: miernictwa elektrycznego, techniki wysokich napięć i materiałów elektrotechnicznych. Utworzył pracownię probierczą, która miała być zaczątkiem Instytutu Elektrotechnicznego.

Przyczynił się walnie do wybudowania w latach 1930-34 gmachu elektrycznego Politechniki Warszawskiej. Pełnił funkcję dziekana Wydziału Elektrycznego, a w 1939 r. został rektorem Politechniki Warszawskiej. Po wojnie (1945) w Brukseli założył Ośrodek Studiów Wyższych Polskich, w którym

kształcono zdemobilizowanych żołnierzy polskich, których losy wojny rzuciły do Europy Zachodniej.

Po powrocie do kraju (1947) podjął pracę na Politechnice Warszawskiej, przystąpił do odtworzenia zniszczonego laboratorium Zakładu Miernictwa Elektrycznego. W pracy naukowo-dydaktycznej kładł szczególny nacisk na pracę zespołową. Najważniejsze jego prace dotyczyły badania rozkładów napięcia w układach izolacyjnych i metod pomiarów wysokiego napięcia. Metoda kompensacyjnego pomiaru rozkładu pola elektrycznego, zwana jest w literaturze technicznej Jego metodą. Opublikował ponad 100 prac naukowych, podręczników i skryptów akademickich.

Był miłośnikiem Tatr, członkiem Klubu Wysokogórskiego i Towarzystwa Tatrzańskiego. Zmarł nagle w Tatrach 22 sierpnia 1952 r. i został pochowany na zabytkowym cmentarzu w Zakopanem na Pęksowym Brzyzku.

Regionalne Centrum Informatyki Warszawa jest jednostką wojskową Wojsk Obrony Cyberprzestrzeni, przeznaczoną do zapewnienia wsparcia teleinformatycznego dla potrzeb kierowania, dowodzenia i współdziałania SZ RP w czasie pokoju, kryzysu i wojny w systemie stacjonarnym, dla potrzeb najważniejszych instytucji, sztabów, dowództw Państwa Polskiego i Sił Zbrojnych, tj.m.in.: Prezydenta RP, Ministerstwa Obrony Narodowej, Sztabu Generalnego Wojska Polskiego, Dowództwa Generalnego Rodzajów Sił Zbrojnych, Dowództwa Operacyjnego Rodzajów Sił Zbrojnych, Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni. Komendantem Regionalnego Centrum Informatyki Warszawa jest płk Robert STAŃCZYK.

RCI Warszawa w ramach Wojsk Obrony Cyberprzestrzeni ma za zadanie zabezpieczenie, utrzymanie niezawodności, rozwój i modernizację eksploatowanych nowoczesnych i innowacyjnych systemów teleinformatycznych (jawnych, niejawnych, narodowych i sojuszniczych) oraz systemów wsparcia dowodzenia dla potrzeb kierowania i dowodzenia na szczeblu polityczno – wojskowym, strategiczno-operacyjnym i taktycznym, ze szczególnym uwzględnie-

niem bezpieczeństwa w cyberprzestrzeni, aby zachować poufność, integralność i dostępność przekazywanych informacji – co wymiernie przekłada się na umocnienie systemu obronnego i bezpieczeństwa kraju.

RCI Warszawa jest właściwe w zakresie utrzymania niezawodnego funkcjonowania systemów łączności radiowej, radiotelefonicznej, satelitarnej, systemów bezpieczeństwa i wojskowej poczty polowej. Realizuje także zadania związane z zapewnieniem bezpieczeństwa w cyberprzestrzeni i zabezpieczenia kryptograficznego.

Krzysztof KRZĄSTEK

PRZYWRÓCIĆ PAMIĘĆ
MJR INŻ. ANDRZEJ GARBOŚ – ŻOŁNIERZ ŁĄCZNOŚCI I WSPÓŁWYNALAZCA WYKRYWACZA MIN



Historia powstania i budowy wykrywacza min w czasie II wojny światowej była przez okres PRL przemilczana. Jego wynalazca prof. inż. Józef Kosacki został przywrócony do świadomości społecznej stosunkowo niedawno. Wydane zostały historyczne publikacje naukowe. Zrealizowano filmy dokumentalne oraz audycje radiowe. Opowieść o dwójce Polaków, którzy w Szkocji opracowali rewolucyjny wynalazek, który zmienił losy II wojny światowej, zagościła na stałe pośród opinii społecznej. We wszystkich powstałych opracowaniach i notatkach prasowych w Internecie pojawiało się nazwisko współpracownika Józefa Kosackiego – plut. Andrzeja Garbosia. Nikt jednak nie poświęcał mu wystarczająco dużo uwagi, bądź też nie mógł dotrzeć do źródeł historycznych, aby go zidentyfikować. Nazywano go przez to „złotą rączką", próbując w pewien sposób tłumaczyć, co kierowało Kosackim w wyborze go na swojego współpracownika. Zbieg okoliczności pozwolił mi zgłębić jego historię oraz stał się przyczynkiem do opracowania jego biografii.

Andrzej Garboś urodził się 26 września 1906 roku we wsi Jadachy w ówczesnym powiecie tarnobrzeskim w Galicji pod zaborem austriackim. Pochodził z biednej rodziny, która utrzymywała się z półhektarowego gospodarstwa rolnego. W 1927 roku po osiągnięciu dorosłości los skierował jego kroki

w stronę Wojska Polskiego. Trafił do 2 Pułku Łączności w Jarosławiu. Od tego momentu związał się na resztę służby z korpusem łączności. Zajmował stanowiska instruktora wyszkolenia teletechnicznego i dowódcy drużyny. W 1929 roku przeniesiony do 4 Batalionu Łączności w Przemyślu na stanowisko dowódcy kompanii szkolnej oraz wykładowcy łączności i aparatoznawstwa, a w 1932 roku do 6 Batalionu Telegraficznego jako podoficer sprzętu łączności i instruktor napraw i konserwacji. Jego służba opierała się na szkoleniu żołnierzy i dokonywaniu napraw bieżących uszkodzonych urządzeń łączności. To doświadczenie i zdobyta praktyka umożliwiły mu ukończenie kursu Majstrów Wojskowych Tele- i Radiotechników w Centrum Wyszkolenia Łączności w Zegrzu, po którym objął tam funkcję Kierownika Warsztatów Szkolnych.

W CWŁ dostrzeżono jego talent i zaangażowanie w pracy. Przydzielony został do zespołu pracującego nad Przystawką OPL, którego celem było skrócenie czasu przepływu meldunków telefonicznych systemu dozorowania o wykrytych nalotach. System ten wykorzystywał pocztową sieć telefoniczną, która opierała się na sieci central, które zestawiały połączenie. Opracowana Przystawka OPL to urządzenie umożliwiające pominięcie na krótki czas określonej relacji wszystkich centrali telefonicznych znajdujących się na drodze połączenia w sieci telefonicznej międzymiastowej na jednym łączu. Dzięki temu posterunek dozorowania uzyskiwał błyskawiczne połączenie ze zbiornicą i przekazywał odpowiedni meldunek. Jeśli w tym czasie na danym łączu była prowadzona rozmowa telefoniczna, to była ona przerywana, a następnie samoczynnie ponownie połączenie było wznawiane. W tym czasie rozmawiający otrzymywali sygnał akustyczny informujący o chwilowym przerwaniu połączenia. Rola Andrzeja Garbosia w pracach nad Przystawką OPL była podkreślana po latach przez oficerów kierujących tym projektem tj. mjr. Henryka Naimskiego oraz por. Wincentego Laska. Opracowane urządzenie ostatecznie trafiło do produkcji w Polskich Zakładach Tele- i Radiotechnicznych w Warszawie, gdzie wprowadzono poprawki konstrukcyjne i uzyskano patent Rzeczpospolitej Polskiej. Dzięki wprowadzonej Przystawce OPL udało się skrócić czas przekazywania meldunków o wykryciu nalotu z 5 minut do 30-45 sekund.

II wojna światowa zastała Andrzeja Garbosia w CWŁ w Zegrzu. W relacji zawartej w jego życiorysie opisywał, że 2 i 3 września brał udział w obronie Zegrza. Następnie wycofany został w kierunku granicy węgierskiej, którą przekroczył 20 września. Internowany był w obozie w Nagycenk, z którego uciekł

i przez Budapeszt trafił do obozu dla cywilów w Barcs, skąd przekroczył „zieloną granicą" z Jugosławią, by w marcu 1940 roku dotrzeć do Francji. Tu przydzielony został do odtworzonego w Wersalu Centrum Wyszkolenia Łączności, gdzie po raz pierwszy spotkał się z ppor. Józefem Kosackim. Tuż przed kapitulacją Francji ewakuowany do Szkocji statkiem, gdzie kontynuował służbę w CWŁ w warsztatach szkolnych, gdzie odpowiadał za naprawę i utrzymanie sprzętu łączności.

W Szkocji jako kierownik warsztatów stanął przed kolejnym wyzwaniem – budową od zera infrastruktury szkoleniowej. Zadanie nie łatwe, gdyż w warunkach braku dostępnego sprzętu i minimalnych nakładów finansowych otrzymywanych na ten cel od wojska pozostawało tylko jedno wyjście – samodzielne zbudowanie urządzeń i przyrządów szkoleniowych z dostępnego złomu elektrotechnicznego. W to zadanie zaangażowanych było wielu oficerów i techników, a kierował nim mjr Stanisław Mrazek. W skład zespołu wchodził także Kosacki, który w CWŁ zajmował stanowisko wykładowcy. W ten sposób narodził się niezwykle efektywny i skuteczny duet Kosacki-Garboś. Na początku 1941 roku za sprawą kpt. Tadeusz Lisickiego, a później gen. Kossowskiego do CWŁ trafiło zadanie opracowania wykrywacza min. Z powołanego zespołu inżynierów i techników pozostało tylko dwóch. Byli to właśnie: Kosacki i Garboś.

Historia prowadzonych prac nad budową wykrywacza min doczekała się filmu dokumentalnego z komentarzem historyków, a także wielu opracowań. Rola Andrzeja Garbosia w tym procesie była do tej pory nieznana. W jego teczce osobowej w Archiwum Politechniki Warszawskiej zachowało się wspomnienie dotyczące tych prac. Oto fragment:

Materiały użyte na prototyp były przeważnie ze starych odbiorników. Wtyczki wykonałem z cokołów lamp radiowych borując z boku otwór na kabel, a wierzch zalałem smołą uzyskaną z wyczerpanych ogniw elektrycznych. Trudności z materiałami były tak duże, że oś wariometru i inne części izolacyjne wykonałem z kości po mięsie ze stołówki (…). Największe trudności jakie napotykaliśmy po ustaleniu schematu elektrycznego i przeprowadzeniu prób przed ujęciem urządzenia w kształt przenośnego przyrządu, było uzyskanie ciszy, a z kolei uciszenia harmonicznych, co jednak po mozolnych próbach doprowadziliśmy do całkowicie pożądanych wymagań.

Prototyp urządzenia wykonany przez dwóch Polaków był bezkonkurencyjny w stosunku do innych urządzeń prezentowanych podczas konkursu. Stanęły do niego instytucje posiadające wykwalifikowaną kadrę i specjalistyczne laboratoria, m.in. Messers A.C. Cossor Ltd, The British Electrical and Allied Industries Research Association, British Thomson-Houston Co. Ltd. Wynalazek Polaków był bezkonkurencyjny. Brytyjczycy bardzo szybko wdrożyli go do produkcji seryjnej z niewielkimi zmianami i skierowali do użycia na polu walki. Zaznaczyć należy, że Kosacki był pomysłodawcą rozwiązań technicznych i przekazał pełne prawa do wynalazku nieodpłatnie władzom brytyjskim.

Aby chronić tożsamość konstruktorów w komunikacie prasowym o dokonanym osiągnięciu użyto pseudonimów. Józef Kosacki był określony jako Józef Kos, a Andrzej Garboś jako Adam Garb. Pojawiały się również formy Adam Galb oraz Adam Garg. Należy zaznaczyć, że stopień plutonowy, przetłumaczony został na język angielski jako: „seargant" i czasami spotyka się informację, że Garboś był sierżantem, co wynika z błędnego tłumaczenia z powrotem na język polski.



Absolwenci I Promocji Szkoły Podchorążych Łączności w Szkocji

Po zakończeniu prac nad wykrywaczem min Andrzej Garboś ukończył Szkołę Podchorążych Łączności i był absolwentem I turnusu. Skierowany został do 11 Kompanii Łączności wchodzącej w skład I Korpusu Pancerno-Motorowego na stanowisko zastępcy dowódcy plutonu technicznego i w 1944 roku

otrzymał promocję na pierwszy stopień oficerski. W czasie wolnym od obowiązków służbowych opracował kolejne rozwiązania techniczne, które zostały wprowadzone do użytkowania. Jednym z nich była tzw. ruchoma rozgłośnia, zaprojektowana przez niego jeszcze w 1943 roku. Była ona zabudowana na samochodzie i umożliwiała wydawanie komend do pododdziałów w marszu przed i za pojazdem. Posiadała zabudowany patefon, mikrofony oraz odbiornik radiowy. Wykorzystywana była również do nagłaśniania apeli. Garboś zaprojektował ją tak, że możliwe było przemawianie przez mikrofon i jednoczesne odtwarzanie nagrania z patefonu lub z odbiornika radiowego z ustawieniem różnych poziomów głośności. Rozgłośnia posiadała również aparat telefoniczny, który umożliwiał wpięcie się w linię podczas postoju i udostępnienie głosu rozmówcy w głośnikach. W ten sposób możliwe było przemawianie przez dowódcę do żołnierzy przez telefon z wykorzystaniem nagłośnienia.

Po zakończeniu wojny powrócił do Polski i po przejściu weryfikacji objął przydział kolejno w Szkolnym Pułku Łączności na stanowisku Kierownika Warsztatów Technicznych i Magazynów Sprzętu Łączności oraz w Szkolnym Pułku Telegraficzno-Telefonicznym w Zgierzu koło Łodzi, w Centralnej Składnicy i Warsztatach Łączności w Zegrzu Południowym, aby ostatecznie trafić do Oficerskiej Szkoły Łączności Radiowej w Zegrzu na stanowisko wykładowcy. W okresie służby w WP PRL również opracowywał kolejne urządzenia. W 1948 roku samodzielnie zaprojektował i wykonał „Poligon Szkolny". Była to nowoczesna jak na tamte lata baza szkoleniowa. Dziś nazwalibyśmy ją laboratorium szkolnym lub symulatorem. Poligon Szkolny służył głównie do szkolenia służby ruchu telegraficznego. W salach wykładowych znajdowały się aparaty telegraficzne BODO i ST-35 do szkolenia bieżącego. Funkcjonowała też generatornia, która pracowała na rzecz aparatowni sal wykładowych oraz polowych węzłów łączności. Poligon Szkolny działał na zasadach samodzielnej kompanii i był przystosowany do przebazowania i rozwinięcia na polowych węzłach łączności z własnym zasilaniem. Za osiągnięcia zawodowe otrzymał awans na stopień porucznika. Opis Poligonu Szkolnego nazwanego później Telegraficznym został opublikowany przez Andrzeja Garbosia w Przeglądzie Łączności. Z powodu represji politycznych aparatu bezpieczeństwa Komisja Opiniująca skierowała wniosek o usunięcie go ze stanowiska. W uzasadnieniu decyzji podano, że powodem zwolnienia jest jego przeszłość oraz brak zaufania.

W pracy cywilnej odnalazł się bardzo szybko. Został zatrudniony w Stołecznych Zakładach Elektrotechnicznych Przemysłu Terenowego w Warszawie. Po pewnym czasie przeniósł się w rodzinne strony i pracował w Zakładach Metalowych w Dębie aż do przejścia na emeryturę. W trakcie pracy cywilnej realizował się w obszarze racjonalizacji, wprowadzając co rusz szereg zmian w zakładach pracy, za co otrzymywał nagrody i wygrywał konkursy. Jak sam napisał w swoim życiorysie, udało mu się wprowadzić w życie ponad 100 ulepszeń oraz wynalazków. Zmarł w 1973 roku w Nowej Dębie

Historia pracy przy wykrywaczu min nie była znana w czasach PRL. Andrzej Garboś nie opowiadał o niej w towarzystwie. Wspominał tylko w sytuacjach zawodowych, gdy przedstawiał swój dorobek zawodowy. W swoim domowym archiwum rodzinnym przechowywał kilka wycinków z gazet angielskich, które przywiózł ze sobą powracając do kraju. Sam uznawał ten wynalazek za najważniejsze wydarzenie swojego życia. Niestety nie dożył czasów, gdy można było o tym opowiadać z dumą. Z tych też powodów jego historia pozostawała nieznana nawet w tak małym środowisku, jakim jest dwunastotysięczne miasto Nowa Dęba, a tym bardziej w skali ogólnopolskiej.

W opracowaniach dotyczących historii polskiego wykrywacza min udział Andrzeja Garbosia był znany, lecz często marginalizowany. Nikt jednak nie mógł o nim powiedzieć nic więcej, gdyż umarł dosyć wcześnie. Ograniczano się tylko do podania stopnia (nie zawsze poprawnie), pseudonimu bądź imienia i nazwiska. Osobą, która wielokrotnie przypominała o wynalazku dwóch Polaków i zawsze wspominała przy tym udział Andrzeja Garbosia był ppłk. Antoni Rogoziński, który był naocznym świadkiem powstawania wynalazku w Szkocji.

W czasach PRL, będąc na emigracji, propagował wiedzę o wynalazku dwóch Polaków w wydawnictwach polonijnych za granicą, m.in. w Dzienniku Związkowym Polish Daily Zgoda w 1979 roku, czy w Przeglądzie Kawalerii i Broni Pancernej w 1983 roku. Wydawał także własne wydawnictwo Pancerniak, w którym również opisał historię powstania wykrywacza. Po 1989 roku publikował także w Polsce w Komunikacie wydawanym przez Zarząd Główny Światowego Związku Żołnierzy Łączności. Organizacja ta podjęła również próbę poznania losów Andrzeja Garbosia, jednak udało się jej pozyskać tylko szczątkowe informacje o służbie wojskowej, co i tak było dużym krokiem przybliżającym postać Garbosia.

8 kwietnia 2026 roku w Samorządowym Ośrodku Kultury w Nowej Dębie odbyła się promocja biografii majora Andrzeja Garbosia[1]. Zawiera ona szczegółowy opis służby wojskowej, procesu powstawania wykrywacza min widzianego oczami Andrzeja Garbosia,a także jego pracy cywilnej i społecznej. Książka ta powstała po wnikliwej kwerendzie źródłowej przeprowadzonej w Centralnym Archiwum Wojskowym w Rembertowie, Instytucie Polskim i Muzeum im. gen. Sikorskiego w Londynie, w The National Archive w Londynie, Archiwum Politechniki Warszawskiej, Archiwum Zakładów Metalowych Dezamet w Nowej Dębie i innych. Szczególną uwagę pragnę zwrócić na Bibliotekę Centrum Szkolenia Łączności i Informatyki w Zegrzu, która przechowuje Archiwum Światowego Związku Polskich Żołnierzy Łączności. Dzięki jasnym i łatwym procedurom miałem możliwość zapoznania się z tym zbiorem. W mojej opinii zawarte tam są bardzo cenne dokumenty tj. opisy, relacje, życiorysy i sprawozdania, które w przyszłości pozwolą na opracowanie biografii innych żołnierzy łączności.

Na łamach tego wydawnictwa składam serdeczne wyrazy podziękowania Komendantowi CSŁiI oraz pani Kierownik Biblioteki, która służyła mi fachową pomocą i radą podczas prowadzenia kwerendy, wskazując materiały, które uciekały mojej uwadze. Wyrazy podziękowania kieruję również do Prezesa Zarządu ŚZPŻŁ w Zegrzu za wsparcie merytoryczne oraz okazanie zaufania. Pominąć nie mogę sponsorów, którzy przyczynili się do wydania książki: Starostwo Powiatowe w Tarnobrzegu, Zakłady Metalowe Dezamet S.A., Zakłady Mechaniczne Siarkopol S.A. Gmina Nowa Dęba oraz Samorządowy Ośrodek Kultury w Nowej Dębie. Serdecznie dziękuję wszystkim z okazaną pomoc.

[1] K. Krząstek, Mjr inż. Andrzej Garboś – żołnierz łączności i współwynalazca wykrywacza min, Wydawnictwo Samorządowe, Nowa Dęba 2026, ISBN 978-83-62300-29-7, ss.168.

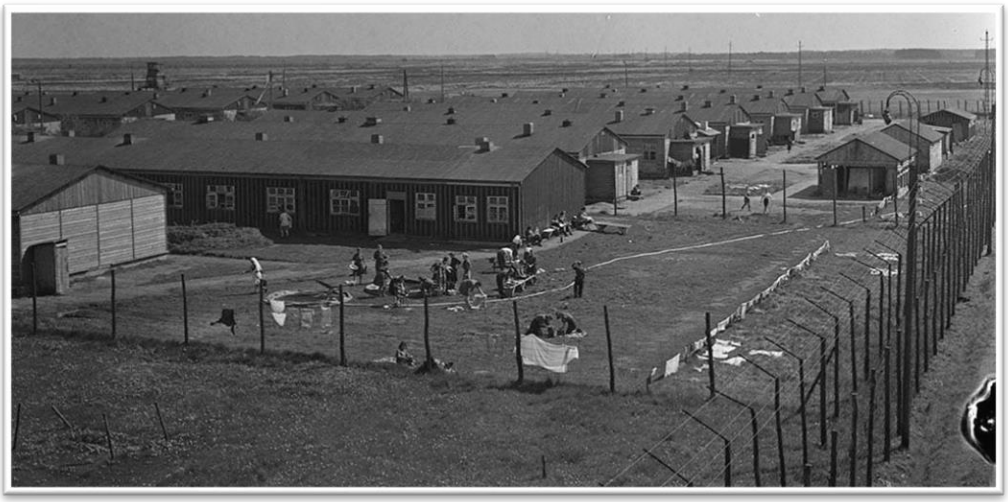
Małgorzata KACZYŃSKA

Z OBERLANGEN DO MACZKOWA

Historia walczących w czasie Powstania Warszawskiego żołnierzy Armii Krajowej nie skończyła się w dniu podpisania aktu kapitulacji 2 października 1944 r. Dokładnie nie wiadomo ile kobiet walczyło w powstaniu; podaje się liczby od 12 tys. do nawet 22 tys. Miały one te same prawa i te same obowiązki, co mężczyźni. Brały udział we wszystkich akcjach Armii Krajowej. Pracowały i pełniły niezwykle ważne funkcje w służbach organizacji, kwatermistrzostwa, łączności, sabotażu, medycznej, informacji, propagandy. Akt kapitulacyjny przyznał jednakowe prawa jenieckie mężczyznom i kobietom walczącym w Warszawie. Kobiety miały wybór - mogły wyjść z ludnością cywilną albo pójść do niewoli, jak żołnierze. Był to pierwszy w historii przypadek, kiedy kobiety znalazły się za drutami obozów jeńców wojennych - najpierw przejściowych w Polsce, a później w Niemczech.

W grudniu 1944 r. ponad 1700 kobiet - żołnierzy Armii Krajowej przywieziono do Stalagu VIC w Oberlangen, w Dolnej Saksonii. Pierwsze słowa, które usłyszały od komendanta obozu brzmiały: walczyłyście z nami, będziecie traktowane jak wojsko! A warunki w obozie były przerażające. Ponieważ obóz został wcześniej wykreślony z ewidencji właśnie ze względu na tragiczne warunki, nie docierała żadna pomoc humanitarna. Obóz głodu i chłodu. Przegniłe drewniane baraki z nieszczelnymi oknami i drzwiami, pomieszczenia z pryczami, najczęściej bez sienników, żelazne piecyki opalane mokrym torfem, które bardziej dymiły, niż grzały, kilka prymitywnych latryn. Codziennie po porannym apelu rozpoczynały prace - głównie na terenie obozu m.in. obsługiwały kuchnię, pralnię, szwalnię, magazyn, szpital, ale również prace związane ze zbieraniem i przewożeniem torfu i chrustu, odśnieżaniem torów kolejowych, czyszczeniem i wywożeniem nieczystości z latryn. Wyżywienie głodowe: rano i wieczorem letnie ziółka, czasem spleśniały chleb, czasem kawałek margaryny lub łyżka marmolady z brukwi, na obiad zupa z gorzkiego jarmużu lub brukwi lub robaczywego grochu, czasem oprócz robaków z kawałkiem ziemniaka w niej.

Nieliczny czas wolny wykorzystywały na prace codzienne: prały, cerowały ubrania.



Obozowa codzienność. Zdj. Adrian Pohl, FB Polish First Armoured Division.

Komendantka obozu por. hm. Maria Irena Mileska ps. Jaga zorganizowała wg wcześniejszych schematów konspiracyjnych tajne nauczanie oraz życie patriotyczne, kulturalne, sportowe, religijne. Powołała Radę Instruktorską, do zadań której należało m.in. utrzymanie cech formacji wojskowej poprzez odpowiednie struktury organizacyjne, szkolenia, dyscyplinę. Zainicjowała funkcjonowanie w obozie tzw. Ministerstwa Oświaty, którego celem było rozpoznanie struktury zawodowej i poziomu wykształcenia. Analiza ta pozwoliła nakreślić kierunki prowadzenia edukacji. Powołano „Wszechnicę Obozową", w ramach której wieczorami prowadzone były zajęcia oświatowe i kulturalne: odbywały się pogadanki, wykłady, zajęcia artystyczne. Tematyka była zróżnicowana i dotyczyła m.in. języka polskiego, historii, filozofii, fizyki, astronomii, muzyki. Przy pomocy wyciągniętego z pryczy gwoździa na kubkach powstawały ryngrafy i obrazki, z materiałów prostych, jak stare puszki konserw, skrawki materiałów, słoma. Opowieści o teatrze snuła Helena Zelwerowiczówna (aktorka, reżyser, scenograf), wiersze recytowała Zofia Książek (aktorka, częściowo niewidoma po wybuchu pocisku Berta w powstaniu). Śpiewały powstańcze piosenki, w tym ułożone przez siebie słowa do melodii żołnierskiej piosenki „Szwoleżerowie". Wszystko to pozwalało choć na chwilę zapomnieć im o gehennie obozowej.

Kiedy komendantka powiedziała na apelu, że rodzi się dziecko, będzie gołe, bo matka nie ma nic, to wystarczyło. Każda, która miała cokolwiek zapasowego: kawałek prześcieradła, chustkę, bluzkę, koszulę - pruła, szyła, prała. Dla pierwszego niemowlaka było tyle kaftaników, czepeczków, pieluszek, że wystarczyło dla następnych dzieci. A urodziło się ich tutaj kilkoro - część kobiet była w ciąży, gdy w październiku zostały umieszczane w obozach.

Dzień 12 kwietnia 1945 r. był zwykłym ich codziennym dniem. Aż do późnego popołudnia, kiedy siedząc w barakach usłyszały warkot pojazdów. Po zlokalizowaniu obozu padły strzały z wieży wartowniczej, na które krótką serią odpowiedział Sherman. Ppłk Stanisław Koszutski zdecydował się staranować czołgiem bramę i znaleźli się za drutami. Wybiegły z baraków i ku swojemu zdumieniu zobaczyły kolumnę alianckich pojazdów. „English? Francais? Americano? Canada? Sind Sie? Polacy! Polacy, panienko! Pierwsza Dywizja Pancerna, kochanie! - krzyczał Witkowski. Polacy! Boże! Polacy! A my tu z Armii Krajowej! Z powstania, z Warszawy. Panowie Polacy! To cud!" Jakież było ich zdziwienie, że to polscy żołnierze. A jak do tego doszło? Po informacji uzyskanej od Holendrów o znajdującym się w pobliżu obozie dowódca 2. pułku pancernego ppłk Stanisław Koszutski ps. Szczutek postanowił utworzyć patrol zwiadowczy: kilkunastu żołnierzy wyruszyło czołgiem Sherman, dwoma scout-carami, jeepem i motocyklem i po odnalezieniu tego miejsca zadziałali. Niemcy poddali się - to był koniec ich niewoli. Radości i wzruszeń nie było końca, tym bardziej, że wyzwolenie przyszło od rodaków. Wielu żołnierzy odnalazło w obozie swoje krewne i znajome. Po tej chwili wielkiej radości komendantka wydała rozkaz sformowania zbiórki składając raport ppłk. Koszutskiemu o stanie obozu, który odpowiedział: „Żołnierze Armii Krajowej i Towarzysze Broni. To historyczny moment spotkania na ziemi niemieckiej dwóch Polskich Sił Zbrojnych. Jesteście wolne. Niech żyje Polska!" Powiewała polska flaga, ze wzruszonych ust popłynął Mazurek Dąbrowskiego.



Raport po wyzwoleniu obozu ppłk. Stanisławowi Koszutskiemu ps. Szczutek składa komendantka obozu por. hm. Maria Irena Mileska ps. Jaga.
Zdj. Domena publiczna Wikimedia Commons.

Następnego dnia na rekonesans przyjechał do obozu dowódca 1. Dywizji Pancernej gen. Stanisław Maczek. Powiedział wtedy: „Jeśli za straty i trudy polskiej dywizji pancernej należały się jakieś kwiaty rzucone serdeczną ręką, to tymi kwiatami rzuconymi rękoma losu było uwolnienie w wyniku działań dywizji tego obozu.” Z okazji wyzwolenia obozu ukazało się Wydanie Specjalne Dziennika Żołnierza 1. Dywizji Pancernej, obwieszczające ten chwalebny fakt. Ale to nie był jeszcze koniec wojny - żołnierze musieli iść dalej, walcząc. Powstał Polski Ośrodek Wojskowy, gdzie zaczęto prowadzić kompanie szkolne, które zorganizowały nauczanie na poziomie gimnazjalnym i licealnym oraz szkolenia zawodowe z kursami m.in. ogrodnictwa, mleczarstwa, krawiectwa, hodowli drobiu, kosmetyczne czy kursy nauki jazdy.

Różne rodzaje i kierunki odkomenderowań kobiet spowodowały, że ich stan liczebny uległ znacznemu zmniejszeniu. Grupa kobiet wraz z komendantką w listopadzie 1945 r. do Ośrodka Wojskowego nr 102 w Hange. Od sierpnia 1946 r. ośrodek ten zaczął podlegać Inspektoratowi Kobiet - Żołnierzy AK, który funkcjonował do maja 1947 r.

Gdy 8 maja 1945 r. zakończyła się wojna 1. Dywizja Pancerna na ok. dwa lata otrzymała teren okupacyjny w Dolnej Saksonii, a jednemu z miasteczek - Haren nadano nazwę Maczków, na cześć dowódcy. Pojawiły się polskie nazwy ulic i placów, jak np. 1. Dywizji Pancernej, Armii Krajowej, Legionów, Jagiellońska, Lwowska, Wileńska.

Dziewczyny z Oberlangen w znacznej części dołączyły do swych oswobodzicieli, podejmując naukę i pracę. Narodziły się też wówczas uczucia, których ukoronowaniem były zawierane małżeństwa i narodziny dzieci. W okresie dwóch lat zarejestrowanych zostało 289 ślubów, 497 aktów urodzenia, 101 pogrzebów - w formalnie nieistniejącym mieście Maczków.

Podstawowe znaczenie dla organizacji życia polskiej społeczności miało utworzenie administracji, systemu szkolnictwa, zapewnienie opieki zdrowotnej, a także ośrodków kulturalnych. Wybrano burmistrza i 12-osobową radę miejską, zaprojektowano pieczęć z nowym herbem, w którym umieszczono kwiat maku, hełm czołgisty i skrzydło husarskie jako symbole 1. Dywizji Pancernej. Do podstawowych zadań władz miasta należało rozdzielanie żywności, świadczeń rzeczowych, organizowanie zbiorowego żywienia, przydział mieszkań.

Po zakończeniu wojny wiele osób szukało możliwości uzyskania lub uzupełnienia wykształcenia. Organizację oświaty wsparły brytyjskie władze okupacyjne, 1. Dywizja Pancerna oraz UNRRA. W krótkim czasie w Maczkowie otwarto przedszkola, dwie szkoły podstawowe, gimnazjum, liceum oraz szkołę zawodową (Polskie Gimnazjum Mechaniczne), a także Uniwersytet Ludowy. Program nauczania i wykładów obejmował przedmioty humanistycznej i ścisłe: język polski, historię, geografię, chemię, matematykę, religię; chętnie też uczono się języków obcych, zwłaszcza języka angielskiego, przydatnego w przypadku dalszej emigracji. Polscy duchowni zorganizowali życie religijne.

Jednym z największych problemów był brak zatrudnienia - w Emslandzie średnio jedynie 10-15% osób znalazło zajęcie w jednostkach sił sojuszniczych. Wielu mieszkańcom Maczkowa nie udawało się znaleźć pracy. Większość osób nadających się do pracy wykonywała ją w obozach w różnych formach: od administracji po wywóz śmieci. Organizowano także kursy szkoleniowe i dokształcające, wspierane przez władze okupacyjne i opiekuńcze, na których uczono konkretnych fachów m.in. krawiecki, zabawkarski, zegarmistrzowski. Dużym zainteresowaniem cieszyła się praca w warsztacie samochodowym, gdyż można tam było dodatkowo uzyskać prawo jazdy. Produkty wytwarzane w warsztatach służyły za niewielką opłatą całej społeczności. Podjęcie pozadomowej aktywności, nawet w formie udziału w kursach pozwalało odpocząć psychicznie i przygotować się do samodzielnego życia po opuszczeniu miasta.

W 1947 r. zmieniła się polityka zatrudniania. Władze okupacyjne zdecydowały się na zatrudnianie ich w gospodarce niemieckiej. W ten sposób chciały zmniejszyć wysokość obciążeń i skalę swej odpowiedzialności za los tych ludzi. Jednak oni nie godzili się na nową politykę. Mieli bowiem zarabiać w niemieckich markach, których nie mogli zamieniać na walutę obcą. Poza tym nie wolno im było kupować wartościowych przedmiotów, a w razie repatriacji nie mogli wywozić pieniędzy.

Bardzo ważną kwestią pozostawały sprawy zdrowotne. Już w kwietniu 1945 r. władze okupacyjne przekazały na potrzeby Polaków szpital w Haren. A była to konieczność, gdyż w mieście przebywało wiele osób chorych. Lata pobytu w obozach, poniewierki i ciężkiej pracy odbiły się na ich zdrowiu; wiele z nich było wycieńczonych wymagających szybkiej pomocy medycznej. Dużą uwagę przykładano do zachowania czystości, by nie dopuścić do wybuchu epidemii. Wprowadzono obowiązkowe szczepienia przeciwko tyfusowi, ospie i dyfterytowi.

W mieście rozwijało się prężnie życie kulturalne. Chętnie czytano prasę - w Maczkowie ukazywał się „Biuletyn", sięgano też po „Dziennik Żołnierza 1. Dywizji i tygodnik „Defilada". Przybywali także artyści z bardzo bogatym repertuarem obejmującym różne typy występów i przedstawień - od musicali przez wieczory baletowe i kabaretowe. Działał Teatr Ludowy im. Wojciecha Bogusławskiego i teatrzyk kukiełkowy „Kukiełki Maczkowskie". Działało kino, biblioteka z czytelnią, świetlice. Dużym powodzeniem cieszyły się także lokale rozrywkowe - dancingi odbywały się trzy razy w tygodniu, a tańczącym przygrywała specjalnie utworzona orkiestra.

Nowym władzom w Polsce zależało na szerokiej repatriacji wojennych wychodźców. Agitacji towarzyszyły próby politycznej indoktrynacji i rozbijania polskich środowisk kształtujących się na Zachodzie. Sytuacja polityczna w kraju, zmiana granic i związana z nią utrata domów powodowały, że wielu Polaków do tych wezwań podchodziło bardzo nieufnie. Decydowali się oni swój powrót najpierw odłożyć, by po jakimś czasie całkiem z niego zrezygnować. Po uznaniu przez Wlk. Brytanię rządu w Warszawie latem 1945 r. coraz częściej wywierano nacisk na Polaków, by wracali do kraju. Masy uchodźców stanowiły bowiem nie tylko problem polityczny, ale i ekonomiczny. Na tym tle dochodziło do sporów; zdawano sobie sprawę z potrzeb zrujnowanego kraju, tęskniono za rodzinami, z drugiej jednak strony rządy komunistów, jak i polityka nie znajdowały akceptacji. Polacy musieli jednak podporządkować się. Losy dziewczyn ze Stalagu VIC Oberlangen i chłopaków z 1. Dywizji Pancernej potoczyły się różnymi drogami: część z nich zdecydowała się na emigrację, część wróciła do Polski.

Te, które wróciły założyły w Warszawie Środowisko Żołnierzy Kobiet AK - Więźniów Stalagu VIC Oberlangen, które funkcjonuje do dziś, a jego obecnym prezesem jest kol. Hanna Kanieska - córka dwojga Maczkowców: matki por. Anny Haliny Kowalskiej z d. Jakubowskiej, w konspiracji od 1941 r. - ZWZ, a następnie w AK-Kedyw, żołnierza Powstania Warszawskiego, więźnia stalagu, po zakończeniu wojny żołnierza 8. Batalionu Strzelców 1DPanc oraz ojca sierż. Eugeniusza Kowalskiego - łącznościowca 1DPanc.

Mężczyźni natomiast, zgodnie z wolą ich dowódcy, na Wyspach Brytyjskich zaczęli tworzyć koła pułkowe i oddziałowe - powstał Światowy Związek Kół 1. Dywizji Pancernej, którego od 1948 r. prezesem był gen. Stanisław Maczek. W latach 60-tych idee organizowania się żołnierzy dotarły do Polski; stop-

niowo i u nas tworzyły się koła: 24. Pułku Ułanów w Kraśniku, 10. Pułku Strzelców Konnych w Łańcucie, Stołeczne w Warszawie, Beskidzkie w Jaworzu, Katowice, Toruń, Gdańsk (cztery pierwsze funkcjonują do dziś).

W 1991 r., zgodnie z wolą gen. Stanisława Maczka i Zarządu Światowego Związku Kół 1DPanc oraz decyzją Ministra Obrony Narodowej RP spadkobiercą tradycji 1DPanc została 11. Lubuska Dywizja Kawalerii Pancernej w Żaganiu. W 2008 r. została powołana z inicjatywy dowódców 11LDKPanc i kombatantów, z udziałem przedstawicieli stowarzyszeń zrzeszonych w Światowym Związku Kół 1DPanc Federacja Organizacji Polskich Pancerniaków, z siedzibą w żagańskim Centrum Tradycji Wojsk Pancernych, której prezesem został gen. bryg. Zbigniew Szura, a której jako córka plut. Wacława Musiała, żołnierza 1DPanc mam zaszczyt być jednym z dwóch wiceprezesów. FOPP w chwili obecnej liczy ok. 500 członków, zarówno z Polski, jak i spoza granic.

We wrześniu 1947 r. brytyjskie władze okupacyjne przekazały administrację miasta w ręce niemieckie. 10 września 1948 r. miastu przywrócono niemiecką nazwę Haren. Z przestrzeni miejskiej zaczęto usuwać wszystkie polskie ślady. Zniknęły polskie tablice informacyjne, przywrócono dawne nazwy ulic, zamalowano napisy, a o polskim pobycie w tym miejscu nie informowała żadna tablica pamiątkowa. Co zresztą specjalnie nie dziwi, bo przez zwykłych mieszkańców byliśmy postrzegani jako okupanci. Rozmowy z Niemcami były z początku bardzo trudne, jednak z biegiem czasu pokonano i tę przeszkodę. Milowym krokiem było w dniu 8 maja 1995 r., w 50-tą rocznicę zakończenia II wojny światowej zostało uroczyste odsłonięcie tablicy pamiątkowej, przy udziale m.in. więźniarek tegoż obozu i innych w powiecie Emsland oraz ich wyzwolicieli z 1. Dywizji Pancernej. Odsłonięto wówczas obelisk z tablicą z napisem: „Pamięci polskich jeńców wojennych 2000 podchorążych więzionych w l. 1940-1941 w nieludzkich warunkach w obozach Oberlangen, Fullen i Wesuwe zmuszanych do pracy na bagnach oraz 1728 kobiet - żołnierzy i oficerów Armii Krajowej z Powstania Warszawskiego przywiezionych tu od grudnia 1944 r. w hołdzie wyzwolicielom obozu żołnierzom 1 Polskiej Dywizji Pancernej gen. Stanisława Maczka. 8.5.1995 - Rodacy”. Od tamtej pory odbywają się tu uroczystości rocznicowe. W kwietniu 2023 r. swe podwoje otworzyło Centrum Dokumentacji i Spotkań„ Haren Maczków 45/48”, ukazujące tę historię z dwóch perspektyw: Polaków, którzy osiedlili się w Haren w 1945 r. oraz niemieckich mieszkańców miasta.

Podczas ubiegłorocznej VIII edycji Historii Frontowych w Porąbce, których współorganizatorem jest Beskidzkie Stowarzyszenie Maczkowców jedna z siedmiu inscenizacji zadedykowana została życiu w Stalagu VIC i jego wyzwoleniu, w 80-tą rocznicę tych wydarzeń.



Pamiątkowe zdjęcie z Historii Frontowych, Porąbka sierpień 2025.
Marcin Ratajczak/Jurassic Photo Team.

Wraz z kol. Hanną Kanieską - co należy podkreślić, że jako córki żołnierzy łącznościowców 1DPanc obie jesteśmy członkami Światowego Związku Polskich Żołnierzy Łączności O/Zegrze - miałyśmy zaszczyt wziąć w niej udział, wcielając się w postacie więźniarek. To była zupełnie inna inscenizacja niż pozostałe, w których pojawia się wiele dynamicznych akcji. Była cicha, ale jakże wymowna i wzruszająca w tej ciszy.

To na naszym pokoleniu spoczywa obowiązek, by pamięć o naszych bohaterskich dziewczynach i chłopakach, walczących o naszą dzisiejszą niepodległość nie zaginęła. Walczących zarówno w Powstaniu Warszawskim, jak i na wszystkich frontach II w. świat. oraz czynie orężnym na przestrzeni wieków. Tak więc kontynuujemy tę pamięć, angażując w działania kolejne pokolenia młodzieży. A pamięć można nieść na wiele sposobów i każdy z nich jest bardzo ważny. Organizujemy i bierzemy udział w wielu uroczystościach, zarówno w Polsce, jak i poza granicami; są to m.in. kongresy, sesje popularnonaukowe, spotkania, wyprawy, rekonstrukcje historyczne, pikniki, kwesty, akcje pomocowe.

płk w st. spocz. mgr inż. Marian TUREK

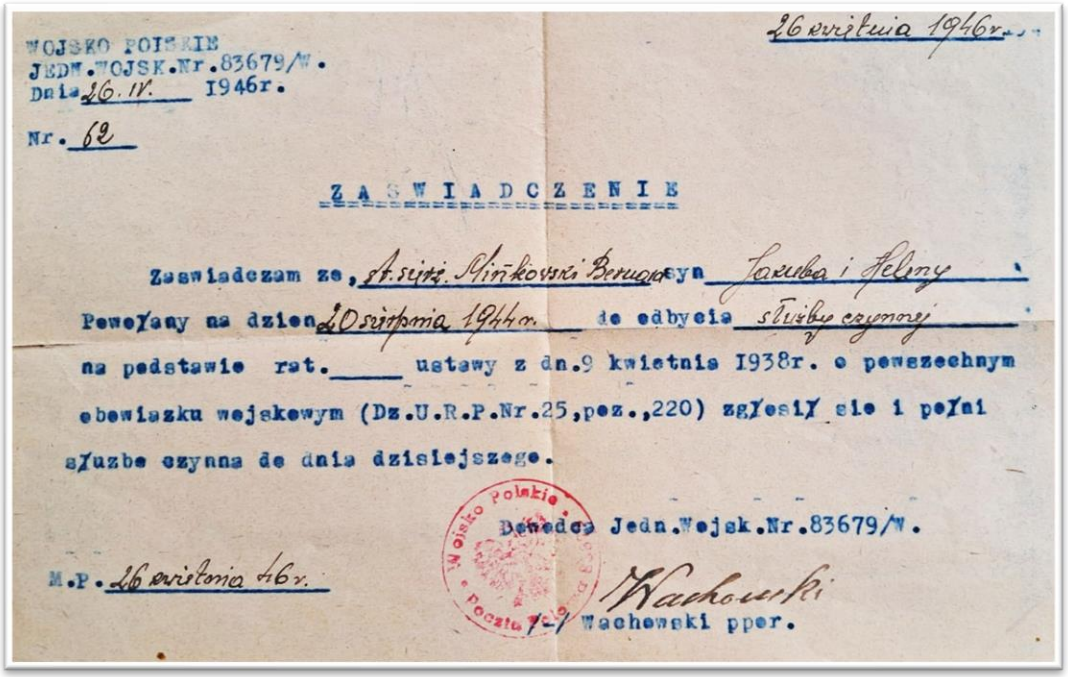
PUŁKOWNIK BERNARD MIEŃKOWSKI - PATRON ODDZIAŁU WARSZAWA ŚZPŻŁ

W dniu 17 kwietnia 2024 r., na uroczystym zebraniu z okazji XXX - lecia Oddziału Warszawa, członkowie podjęli uchwałę o ustanowieniu śp. płk. mgr. inż. Bernarda Mieńkowskiego patronem Oddziału Warszawa.



płk mgr inż. Bernard Mieńkowski

Płk Bernard Mieńkowski urodził się 8 lutego 1923 r. w m. Jaszkiewicze, pow. Wołożyn, woj. Nowogródek. Tam uczęszczał do szkoły podstawowej, a następnie kontynuował naukę w gimnazjum w Mołodecznie. Po otrzymaniu świadectwa maturalnego dostał nakaz pracy jako pomocnik maszynisty parowozowego. W 1944 r. wstępuje ochotniczo do służby wojskowej w 16. kompanii łączności w 9. Dywizji Piechoty II Armii Wojska Polskiego. Jako żołnierz był dowódcą radiostacji RSB-F i brał udział w walkach przeciwko Niemcom hitlerowskim nad Nysą Łużycką, pod Dreznem i Pragą. Podczas wojny został szybko awansowany od szeregowca do sierżanta.



26 września 1946r.

WOJSKO POLSKIE
JEDN.WOJSK.Nr.83679/W.
Dnia 26.IX. 1946r.

Nr. 62

ZAŚWIADCZENIE

Zaświadczam że, st.sierż. Mińkowski Bernard syn Jakuba i Heleny
Powołany na dzień 20 sierpnia 1944r. do odbycia służby czynnej
na podstawie art.____ ustawy z dn.9 kwietnia 1938r. o powszechnym
obowiązku wojskowym (Dz.U.R.P.Nr.25,poz.,220) zgłosił się i pełni
służbę czynną do dnia dzisiejszego.

Dowódca Jedn.Wojsk.Nr.83679/W.

M.P. 26 września 46r.

Wojsko Polskie Poczta

z/ Wachowski ppor.

Po wojnie pełnił dalej służbę wojskową, awansował do stopnia chorążego i został dowódcą plutonu radiostacji dużej mocy w Pułku Łączności w Zgierzu.

W 1948 r. otrzymał awans na stopień podporucznika i dalszą służbę pełnił w Zegrzu, w Szkolnym Pułku Radio. W 1949 r. został skierowany na studia do Wojskowej Inżynieryjnej Akademii Łączności w Leningradzie, którą ukończył w 1954 r. z dyplomem magistra inżyniera. Po studiach pracował w Poligonie Naukowo- Badawczym Sprzętu Łączności w Zegrzu Południowym kolejno na stanowiskach: kierownika pracowni i kierownika zakładu, a następnie zastępcy komendanta Poligonu do spraw naukowo badawczych. Zastąpił na tym stanowisku mjr Tadeusza Niewiadomskiego, który został wyznaczony na komendanta Poligonu. W tym czasie głównym zadaniem pracowników Poligonu było opracowanie koncepcji i wdrożenie nowego rodzaju łączności, jakim była łączność radioliniowa. W 1955 r. wykonano 12 ośmiokanałowych mobilnych stacji radioliniowych o nazwie RVG-902C, które transportem kolejowym zostały przewiezione do Sieradza, gdzie w 1956 r. został utworzony 56. Batalion Radioliniowy. Dowódcą Batalionu został mjr Bernard Mieńkowski. W 1964 r., po ośmioletnim czasie dowodzenia 56. Batalionem w Sieradzu, wraca do Zegrza Południowego na stanowisko zastępcy komendanta. Następnie zostaje komendantem utworzonego w 1965 r. Wojskowego Instytutu Łączności. Pełnił tę funkcję do 1969 r.



Komenda Poligonu Naukowo-Badawczego Sprzętu Łączności w Zegrzu
od lewej - płk B. Mieńkowski, płk. T. Niewiadomski, ppłk J. Górecki

W tym czasie kontynuował naukę na Podyplomowym Studium Badań Operacyjnych w Warszawie. Następnie objął obowiązki zastępcy Szefa Wojsk Łączności w Ministerstwie Obrony Narodowej.



Od lewej: gen. bryg. Leon Kołatkowski, płk Bernard Mieńkowski

W 1975 r. uległ wypadkowi, w wyniku którego w 1976 r. przeszedł w stan spoczynku. W 1977 r. podjął pracę w Ośrodku Badawczym „Telkom-Telpro”

w Warszawie jako kierownik Pracowni Normalizacji, a od 1992 r. pracował w Ośrodku Badawczym „Tekoma" jako główny specjalista. Koordynował prace normalizacyjne w przemyśle pod wymagania wojska. Przewodził polskim delegacjom podczas uzgodnień norm wojskowych Układu Warszawskiego.

Podczas swojej służby wojskowej otrzymał szereg odznaczeń państwowych oraz resortowych: Krzyż Oficerski Orderu Odrodzenia Polski, Krzyż Kawalerski Orderu Odrodzenia Polski, Krzyż Walecznych, Brązowy Medal Zasług na Polu Chwały, Medal „Za Zwycięstwo", Medal „Za Odwagę", Medal „ Za Odrę, Nysę i Bałtyk, Srebrny Krzyż Zasługi, Złoty Medal za Zasługi dla Obronności Kraju, Złoty Medal Siły Zbrojne w Służbie Ojczyzny.

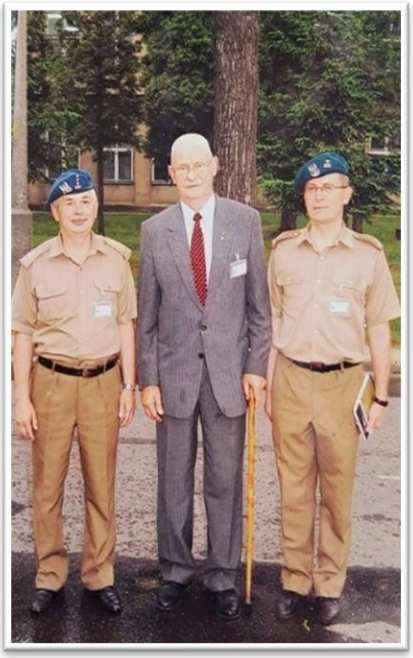
W 1969 r. uhonorowany został nagrodą II stopnia przez Ministra Obrony Narodowej. W 1989 r. otrzymał nagrodę Przewodniczącego Komitetu Przemysły Obronnego Rady Ministrów /wiceprezesa Rady Ministrów/ „W uznaniu zasług włożonych w dzieło rozwijania przemysłu obronnego i umacnianiu obronności państwa".

Będąc na emeryturze angażował się również działalność społeczną. W 1981 r. wstąpił do Związku Byłych Żołnierzy Zawodowych, gdzie w latach 1988 -1994 pełnił funkcję prezesa w Kole nr 41 przy Sztabie Generalnym WP. W sierpniu 1992 r. powstała koncepcja utworzenia Światowego Związku Polskich Żołnierzy Łączności. Pułkownik w stanie spoczynku Bernard Mieńkowski czynnie uczestniczył w pracach przygotowawczych i był członkiem Komitetu Założycielskiego tego Związku. Z chwilą jego powstania w 1993 r. wszedł w skład Rady Związku, w której działał od I do VI kadencji tj. do roku 2012 r.

W 1994 r. został wybrany prezesem powstałego Oddziału Warszawa Rakowiecka i funkcję tę pełnił nieprzerwanie przez 17 lat do 2011 r.



od lewej:Płk Bernard Mieńkowski, Prezes Oddziału Warszawa do 2011 roku i płk Zbigniew Kosobucki, Prezes Oddziału Warszawa od 2011roku



od lewej: płk Sobotka, płk. Bernard Mieńkowski, mjr Błaszczyk, Sieradz 2005 r.

Koledzy z Oddziału docenili duże zaangażowanie płk. Bernarda Mieńkowskiego oraz pracę w Zarządzie i uhonorowali Go tytułem „Honorowego Prezesa Oddziału".

Płk. Bernard Mieńkowski interesował się turystyką, był aktywnym członkiem Wojskowego Koła PTTK nr 3 przy Wojskowym Instytucie Łączności w Zegrzu Płd. Od 2006 r. był członkiem „Stowarzyszenia Przyjaciół 15. Sieradzkiej Brygady Wsparcia Dowodzenia. Cieszył się dużym uznaniem jako specjalista oraz szacunkiem zarówno przełożonych, jaki i podwładnych. Był zawsze wspaniałym Kolegą.

Pan Pułkownik zmarł w dniu 27 kwietnia 2020 r. Został pochowany z honorami wojskowymi na Cmentarzu Komunalnym Północnym w Warszawie.



Jako Patron Oddziału Warszawa ŚZPŻŁ zawsze zostanie wśród nas.
Cześć Jego pamięci!

Rafał MAGOŃ

Z ŻYCIA ŻOŁNIERZA - OD SZEREGOWEGO DO OFICERA STARSZEGO, cz. IV

Kontynuuję opowiadania o życiu żołnierza od szeregowego do oficera starszego.

Zachłysnęliśmy się sprzętem i usługami dziedzinowymi NATO. Tak naprawdę, w większości ich nie potrzebujemy. Mamy swoje aplikacje, systemy, czy sprawne nikt się nie przyzna, bo pieniądze wydane. Niech ktoś mi pokaże system, który scala Siły Specjalne, Wojska Obrony Terytorialnej, Siły Powietrzne, Marynarkę Wojenna i Wojska Lądowe – no nie ma takiego. Cóż taka nasza mentalność.

Często na treningach i ćwiczenia z wojskiem udział w nich biorą nasi koalicjanci, i aby zsynchronizować działanie oraz realizację epizodów prowadzi się odprawy koordynujące. Na takich odprawach mówimy w języku angielskim, aby każda nacja mogła się odnaleźć, nasi wojskowi nie mają z tym problemu, muszę powiedzieć, że naprawdę stanowimy wzór do naśladowania, a co do niektórych to można powiedzieć, że mają tak opanowany język angielski jakby był ich językiem naturalnym.

Podczas ćwiczenia Bagram, certyfikującego żołnierzy naszych wyjeżdzających do Afganistanu na kolejną rotacje, udział brali Amerykanie oraz Brytyjczycy, no i w sumie nic w tym dziwnego, gdyby nie to, że część z nich pochodziła ze Szkocji. Ja byłem wtedy tzw. klikaczem na odprawie, Agenda dotyczyła kolejnych epizodów oraz usługi funkcjonalnej JCATS. Rozpoczął Dowódca 2 Korpusu, następnie kolejno meldowali ćwiczący dowódcy, kolejne slajdy, nudne tematy kolejny raz kolejna certyfikacja, znużony już byłem. Gdy nagle Anglicy mieli przedstawić plan na kolejny dzień i podsumowanie działań w obecnym. Do mównicy podszedł szkocki kapitan. Kliknąłem na pierwszą stronę jego prezentacji i koniec, bełkot jaki zacząłem słyszeć nic mi nie przypominał język angielski, nic w sumie nie rozumiałem, jak zauważyłem po minach żołnierzy na odprawie nie byłem jedyny, a zjawisko to stało się powszechne. Tylko z mimiki twarzy i ruchu rąk rozumiałem, że chce kolejny slajd trwało to

około 10 minut. Nie wiadomo o co mu chodziło, a jego angielski to można porównać gwarę kaszubską i śląską i to chyba razem pomieszaną. Wstał płk Cz. i poprosił najwyższego rangą przedstawiciela ich o zwrócenie uwagi, że my nic nie rozumiemy i prosi o innego spikera. Uważam, że każdy powinien uczyć się języków, dzisiaj są tłumacze symultaniczne i elektroniczne, każdy powinien umieć posługiwać się formą języka urzędowego, zwłaszcza przy wystąpieniach publicznych.

Ćwiczenia z wojskami to nie tylko odprawy, najważniejszy jest żołnierz w polu na rubieży, tam też największa odpowiedzialność i najwięcej potu wylewamy.

Gdy już dowodziłem kompanią, raz w roku 5pchem robił zgrupowanie poligonowe, gdzie certyfikował kompanie chemiczne, a właściwie kolejny okres szkolenia. Najczęściej pułk wyjeżdżał na Dębę.

I owego zgrupowania podczas zajęć taktycznych z OPBMR zostały wykorzystane środki szkolne – chemiczne, w miejscach odosobnionych i do tego przeznaczonych. Nic w tym nie było ciekawe, ani dziwnego, gdyby nie fakt, że zapalonym grzybiarzem był szef sztabu ppłk M., często przemierzał las poligonowy w poszukiwaniu tego właśnie runa leśnego.

Moja kompania zakończyła już zajęcia, dowódca konwoju zabrał potrzebne mu pozostałe elementy po szkoleniu – sporządził odpowiednie dokumenty i pojechał zdać do magazynu. Pododdział w tym czasie zaczął przemieszczać się na obozowisko, zostałem tylko ja i mój szef kompanii. Nagle widzimy, że w miejscu, gdzie były wykorzystywane do szkolenia środki, idzie sobie szef sztabu i podnosi coś … to raz za razem. Patrzymy, a on ma całe wiaderko grzybów, oczywiście nas nie widział. Co mieliśmy śmiechu, nazwaliśmy go chemiczny grzybek. Teraz trochę zastanawiam się czy warto by nie było mu o tym powiedzieć, jednak z drugiej strony dobrze mu tak. Nie był lubiany. Podsumuje żyje do dziś.



Ze zbiorów własnych. Podczas zajęć taktycznych.

Stanowisko szefa sztabu wg mnie w jednostkach jest bardzo trudne i wymagające, Żołnierz na takim stanowisku odpowiada za pracę sztabu. Brzmi prosto, przecież ma ludzi do pracy, … czyżby? To nie tylko sprawy personalne, sprawy szkoleniowe, operacyjne, logistyczne, rozpoznania, łączności, planowanie, mobilizacja, powołania do służby, rozliczenie amunicji i środków pozoracji, służby, aż w końcu rozliczenie mienia i pododdziałów.

Znałem takiego żołnierza – oficera starszego płk K., który, żeby wszystko połapać i mieć wiedzę, czyli pod kontrolą zapisywał w TEWO, a zeszyt ten miał 500 stron. Codziennie przepisywał sprawy nie zrealizowane na następny dzień, spraw przybywało a kartek ubywało. Któż, by chciał ciągle dopisywać, tak żeby sprawy nie schodziły, a nowe dochodziły.

Na ćwiczenie międzynarodowe mieli przyjechać amerykanie, a było to wtedy, kiedy jeszcze tak powszechnie u nas nie stacjonowali, dostał za zadanie rozliczyć ich. Jak myślicie co taki oficer zrobił, zadzwonił do operacyjnych, ci mu podali kto jest odpowiedzialnym oficerem łącznikowym, no i oczywiście że nazwiska potwierdził logistyk, i tu sprawa wydawała się by prosta, jednak nie.

Ponieważ logistyk podał 42 żołnierzy i nazwiska jak usłyszał, a nie znał angielskiego, porównał to operacyjny który pozyskał od kogoś z przełożonych, dość, że nie zgadzała się liczba, to jeszcze nazwiska. Postanowili zmiksować dane i co wyszło wyszła lista 50 żołnierzy, każdy inne nazwisko. W tym czasie jako szef sekcji administracyjnej odpowiadałem, mimo, że byłem w oddziale łączności i informatyce za rozkaz dzienny, ale to już z wcześniejszych opisów kto śledzi to wie. Przyszło oficjalne pismo z ambasady amerykańskiej ilu jest wydzielonych żołnierzy na to zadanie, i takie też nazwiska i imiona wpisałem do Rozkazu. Z rozkazem przed podpisaniem w 2 KZ zapoznawał się szef sztabu, tak więc jak już był zredagowany poszedłem do niego. No i co okazało się, spisał on listę 50 – a u mnie było 42. Kazał zawołać operacyjnego i logistyka i ustalić którzy to są prawdziwi i którzy przyjeżdżają, a którzy z i za jakiej przyczyny nie pojawią się. Cała afera nabierała rozpędu, gdy ten kazał napisać pismo o wyjaśnienie, dlaczego pozostali nie pojawia się, co ciekawe z 42 oczywiście było jeszcze kilku innych niż obydwoje mieli nazwiska.

Pyta się mnie czy jestem pewien nazwisk, chciał nie chciał musiałem uratować sytuacje – powiedziałem, że tak, dalej pyta się skąd mam te informację to ja mu pokazuje pismo. Specyficzne miał poczucie humoru szef sztabu, kazał

im wyjaśnić czemu nie przyjeżdżają pozostali, oczywiście bez powiadamiania i przygotowania pisma do ambasady.

Ten sam szef sztabu codziennie chodził na pieszo do pracy na Rakowicką w Krakowie, każdorazowo służba wypatrywała, kiedy będzie szedł, a meldowanie mu przeszło do rytuału na służbie, oficjalnie powinni się tylko Oficerowie dyżurni przestawić, u nie go nie tylko, padały pytania kontrolne. Często pytał o rzeczy niespotykane, nietuzinkowe. Raz zapytał, ile jest lamp i ile z nich jest spalonych lub ile jest hydrantów i ile z nich jest sprawnych, biada, żeby któryś nie wiedział, musiał kilka krotnie przychodzić do niego przed zdaniem służby. Oczywiście pytania wtedy już padały kolejne.

No dobra ale dajmy już mu spokój oficer doszedł do Generała, kto go pamięta będzie na pewno go wspominał.





Przeprawa przez Wisłę wojsk NATO.

Gdy po EXCON MOBILE GROUP - DRAGON – 24, skierowano mnie na WZZ Podlasie, byłem zaskoczony, dobrze nie przyjechałem z jednego już jechałem na drugi kierunek i to dłuższy czas.





Stanowisko Kierowania na EMB-DRAGON24

Nie było źle Wydział Komunikacji Społecznej był bardzo prężny, zabezpieczał czas wolny, czasem wyjście do kina, a czasem coś innego. Czasem dało się wypisać na wyjście na zabezpieczone prze ratowników jezioro Dojlidy.



Tęcza nad Obozowiskiem WZZ Podlasie oraz emblemat III zmiany – łączność i informatyka.

Jako szef wydziału łączności, nie było mi łatwo. Ugrupowania były z różnych jednostek, każda miała inny poziom łączności pod względem sprzętu i wyszkolenia ludzi. Do tego dochodziło zakłócenie naszych wojsk radiotechnicznych oraz radarów białoruskich, a w tym wszystkim brak roamingu krajowego między operatorami sieci komórkowej. Często też uwarunkowania terenowe tworzyły czarne dziury z zasięgami radia, czy też sieci komórkowej. Walka trwała, w telefonach dokładaliśmy drugie karty SIM, a w wielu miejscach stawialiśmy dodatkowe maszty antenowe. Tak, więc po ciężko pracowitym tygodniu, czasem trzeba było zresetować mózg, wybraliśmy się nad jezioro, wynajęliśmy łódkę, no i co w tym dziwnego, gdyby nie to, że przy kolejnym manewrze zawracając łódkę przed samą główną plażą przewróciliśmy łajbę. Wszyscy w wodzie, widownia w postaci plażowiczów, a było ich bardzo dużo, pogoda dopisała.

Tylko nasza przytomność pozwoliła w miarę wszystko uratować, portfele, komórki, klapki, które same pływały, no i łódkę. Brakowało tylko aby wszyscy byli nam brawo.

Gdy byłem na studium oficerskim, dumnym kierunku: eksploatacja systemów łączności, było tam wielu ciekawych wykładowców, ale tylko kilku zasługiwało na uwagę, jednym z nich był niejaki dzisiaj pewnie płk M. – wuefista. Gość naprawdę ma autorytet i specyficzne poczucie humoru. Postanowiliśmy zaliczyć sprawdzian z pływania i wiedzieliśmy, że zalicza chorąży, więc poszliśmy do niego, poszło szybko i sprawnie i wszyscy mieli pozaliczane. Ktoś powie i co w tym dziwnego. No tak w sumie nic, jednak Pan M. postanowił o godzinie 4 z minutami zadzwonić i przekazać informację, na służbę dyżurną, że

egzamin na oficera zdaje się u oficera i on teraz ma czas. Wszyscy myśleli, że to żart. Zagroził, że kto nie przyjdzie to ma nie zaliczone. Szybkie ubieranie się i na basen pędem, a on tam już czekał. Rachu ciachu i wszyscy meldowali się na basenie, tempo zaliczenia było drastyczne, bo do śniadania wszyscy byliśmy i w wodzie i zaliczyliśmy tą konkurencję. Terrorysta.

W grupie łączności było 8 osób, na walce wręcz kazał wymieniony oficer dobrać się w pary, oczywiście nie byłbym sobą gdybyśmy coś nie wymyśleli, aby sobie ułatwić. Otóż w padliśmy z kolegą na pomysł, że najpierw ja zrobię ruchy karrrraaate i on się przewróci, a potem on to samo i ja się przewrócę. Nasze super zrozumienie tak nas wyprowadziło, że przy pierwszym ruchu obydwoje leżeliśmy jak te biedrony. Och żebyście wtedy widzieli jak się on nakręcił, już nie zdawaliśmy w parze, a z nim, uwierzcie mi lub nie, wszystko mnie bolało i bałem się, że żeber już nie mam.

Kolejną konkurencja było słynne 3 tysiące metrów marszobiegiem, ciekawe, że nazywa się to marszobieg, a nie widziałem nikogo kto by maszerował poniżej 10 minut 3 tysiące metrów.

Biegało się po parku, wokół lasu i jeziorka.

Na tamte czasy wykręcałem ponad 12 minut. Nasz oficer, żeby nas pilnować i nadzorować zasuwał za nami na rowerze, no cóż są równi i równiejszy.

Po tak ambitnych konkurencjach na zaliczenie w korpusie oficera, trzeba było wyjść i odświeżyć głowę na tzw. miasto. Człowiek miał w głowie, że już tylko promocja i jest oficerem, więc i zakrapiało się dosyć wyskokowym trunkiem. A że trunek zacny to i głowę można było stracić. I tak się ze mną stało. Po takiej żywej imprezie zgubiłem, gdzie pieniążki, a trzeba było wrócić do szkoły. Nie było sił, żeby wracać na nogach, więc wsiadłem w pierwszą taksówkę i poprosiłem na Akademie, taksówkarz wykonał polecenie i mnie przywiózł. Przyszło do zapłaty i wtedy zorientowałem się, że portfela, kasy brak. Już miałem czarne myśli. Izba wytrzeźwień, policja i bóg wiedzieć co jeszcze.

Spojrzał na nie taksówkarz, nie był zły, nie jakiś warczący i mówi - ze słowem podchorąży …? i mówi dalej …. wysiadaj, powodzenia żołnierzu. Jezu jakie mnie dorwało zdziwienie. Dzisiaj bym mu podziękował za jego elokwencję.

Tak więc są różni ludzie, różnie charakterni, różne mają autorytety i kierunku życia.

Weźmy taki nietypowy przykład, zmiany PKW często trwają ponad 6 miesięcy, mnóstwo tam ludzi z różnych środowisk i z różnymi charakterami. I wiecie co, tam dopiero widać kto nadaje się do łączności – do wojska. Często oficerowie potrafili się pokłócić o sprzątanie po sobie, jakby to było przyczyną wojny i konfliktu kraju, w którym jest misja. A ustalenie te prozaiczne, z reguły rozstrzyga dowódca kontyngentu, ludzie ludziska co z wami. Jest taka przypadłość – syndrom starego sierżanta – wypalenie zawodowe, na misji widać takich żołnierzy, często przymyka się oko, żeby dotrwać do końca zmiany dla spokoju.

MOTTO – misyjne – przyjąć – utrzymać – nie popsuć – przekazać, czasem znajdzie ktoś z większym zapałem i próbuje wprowadzić zmiany lub wyprostować zastane zaległości i różnice.

Nie oceniam, ale słów brak.

Błażej MOŚCIPAN

NA SZLAKU PODRÓŻY Z ŁĄCZNOŚCIĄ W TLE – LUBUSKIE MUZEUM WOJSKOWE W ZIELONEJ GÓRZE Z/S W DRZONOWIE

W Komunikacie nr 41 pani Małgorzata Kaczyńska opublikowała swoje relacje z podróży po muzeach, skansenach i izbach (i nie tylko), w których zobaczyć można szeroko rozumiany sprzęt łączności wojskowej. Artykuł ten zainspirował mnie do szerszego przedstawienia Czytelnikom Komunikatów jednej z placówek znajdujących się na szklaku ww. podróży. Mianowicie chodzi o powstałe w 1985 r. Lubuskie Muzeum Wojskowe w Zielonej Górze z/s w Drzonowie, gdzie znajdziemy całkiem sporo ciekawostek związanych z łącznością.



Lubuskie Muzeum Wojskowe, rzut przestrzenny, 2015 r. rys. Robert M. Jurga

Muzeum to mieści się w zabytkowym, klasycystycznym założeniu parkowo-pałacowym we wsi Drzonów, położonej kilkanaście kilometrów od jednej z dwóch stolic województwa lubuskiego. Drzonowski majątek nie miał wcześniej szerszego powiązania z wojskowością i do 1945 r. był typową ziemiańską posiadłością rodzinną… choć oczywiście wśród dawnych właścicieli znajdziemy wyższych oficerów jak choćby generalleutnanta Karla von Klinckowstroema, który nabył drzonowską posiadłość w 1853 r. Z kolei krótko po zakoń-

czeniu II wojny światowej w pałacu stacjonowali żołnierze Armii Czerwonej. Następnie budynek ten zaadaptowano na potrzeby szkoły, a po budowie „tysiąclatek", krótko mieściły się tu pomieszczenia spółdzielni rolniczej. W 1973 r. podupadający już pałac został przekazany na własność Muzeum Ziemi Lubuskiej w Zielonej Górze z myślą stworzenia w tym miejscu magazynu dla muzeum archeologicznego. Koncepcję tę zmieniono w 1978 r. za sprawą inicjatywy bronioznawcy dr. Włodzimierza Kwaśniewicza, wówczas kierownika nowopowstałego Działu Braterstwa Broni, który to głównie z braku lepszego miejsca, zaczął ustawiać przy nim pozyskane do zbiorów muzeum eksponaty ciężkiego sprzętu wojskowego – czołg T-34-85, samolot Ił-28 czy śmigłowiec SM-2. A zbiory te pozyskiwał by stworzyć nowe muzeum, które w swoich założeniu miało przede wszystkim upamiętnić walki 1945 roku.

Dziś placówka jest instytucją kultury miasta Zielona Góra, należy do elitarnego grona tzw. muzeów rejestrowanych (czyli znajduje się w państwowym rejestrze muzeów o szczególnym znaczeniu dla historii i dziedzictwa kraju) i posiada w swoich zbiorach przeszło 4 000 pozycji inwentarzowych (tj. pojedynczych eksponatów, ale i zespołów pamiątek). Wizytówką instytucji jest – czołowa w kraju – kolekcja ciężkiego sprzętu wojskowego, w której znajduje się wiele unikatów takich jak dwa radzieckie (z jedynie trzech zachowanych na świecie) działa samobieżne SU-152 czy prototyp jednomiejscowej Iskry BR 200. Znaczna część tej kolekcji rozstawiona jest w przypałacowym parku w stylu angielskim. Tworzy to dość ciekawą i niespotykaną kompozycję zabytków. Duża przestrzeń pełna zieleni i cienia, zwłaszcza w sezonie wiosenno-letnim, jest doskonałym miejscem do spędzenia czasu dla rodzin z dziećmi. Trzeba jednak uczciwie dodać, że takie połączenie rodzi również wiele problemów konserwatorskich dla muzealników.

Przedłużeniem parkowej ekspozycji ciężkiego sprzętu wojskowego jest jeszcze wystawa pawilonowa, w której schowano (przed warunkami atmosferycznymi) bardziej delikatne wojskowe konstrukcje. Z kolei na parterze, wspomnianego wcześniej pałacu zorganizowano pięć wystaw stałych: „Dawna broń", Żołnierz polski 1914-1945", „Kobiety-żołnierze", „Wojsko Polskie po 1945 r.", „Gabinet myśliwski" oraz wydzielono salę wystaw czasowych.



Drzonowski pałac, fot. z 2024 r. M. Zawada

W sposób oczywisty, w muzeum tak szeroko opowiadającym o wojsku, znajdują się także pamiątki związane z historią łączności wojskowej. Do najstarszych należą te używane w okresie II wojny światowej. Przegląd tych pamiątek rozpoczniemy od kurtki mundurowej (z naszytymi wtórnie oznakami łączności na kołnierzu) st. szer. Celiny Klawisz (z domu Denkiewicz), żołnierza plutonu łączności 1. Samodzielnego Batalionu Kobiecego im. E. Plater, z którym przeszła cały szlak bojowy od Sielc do Warszawy. Obok tego munduru prezentowany jest jeszcze – powstały w 1942 r. w Zakładach Elektromechanicznych w Taszkiencie – telegraf taśmowy Mors'a M 42 oraz przenośna, plecakowa radiostacja A7B. W dalszej części opowieści o losach ludowego Wojska Polskiego prezentowana jest jeszcze radiostacja 10-RT, stosowana do komunikacji w czołgach i pojazdach opancerzonych. W gablocie z pamiątkami wojsk alianckich zobaczyć można amerykańską radiostację agenturalną AR-11 (opracowaną w 1942 dla wojsk wywiadowczych, a wykorzystywaną także w strukturach podziemnych m.in. w Polsce i we Francji) oraz polowy aparat telefoniczny EE-8-A. Kolejny telefon polowy M 33 (Feldfernspecher 33), wyprodukowany w 1937 r. w zakładach Richard Bosse & Co. w Berlinie oraz Telefonbau Normalzeit GmbH we Frankfurcie nad Menem, zobaczyć można w gablocie z wyposażeniem Państw Osi. Z kolei na wystawie Wojsko Polskie po 1945 r. stworzono niewielką gablotę w całości poświęconą łączności tego okresu i prezentowane są w niej radiostacje R-108 i R-126, łącznica telefoniczna ŁP-10 oraz telefon polowy AP-48 z Państwowej Wytwórni Urządzeń Te-

lefonicznych. Nieco większe przedmioty zgromadzone są w pawilonie ekspozycyjnym, gdzie zobaczyć można m.in. łącznicę polową ŁP-40 czy bębny z kablem telefonicznym PTF-7 wraz ze zwijarką oraz kabel dalekosiężny.



Gablota ze sprzętem łączności na wystawie Wojsko Polskie po 1945 r.

Na ww. wystawach siłą rzeczy (ze względu na szczupłą ilość miejsca wystawienniczego) prezentowana jest tylko część kolekcji. Pozostałe przedmioty oczom zwiedzających ukazywane są w trakcie wystaw czasowych własnych oraz w zaprzyjaźnionych muzeach. Przede wszystkim w tej grupie przedmiotów znajdują się liczne radiostacje używane przez polskie wojsko po II wojnie światowej, raczej popularnych wzorów. Najciekawszy jest jednak niemiecki odbiornik radiowy WR 1/P Phillipsa z 1943 r., używany przez niemiecką armię głównie do celów rozrywkowych i propagandowych, popularnie określany przez żołnierzy jako „Rudi". Kolejną sporą grupą są memorabilia (medale pamiątkowe, ryngrafy, miniatury sztandarów itp.), oznaki i odznaki związane z wojskami łączności oraz oficerską szkołą radiotechniczną. Na koniec warto wspomnieć także o nielicznych, ale bardzo interesujących muzealiach papierowych. Wyróżnić tu należy choćby zdjęcie żołnierzy 1. Pułku Łączności z Zegrza z 1924 r., książeczkę wojskową Józefa Powchowicza z pieczęcią tego samego pułku czy wspomnienie Michaliny Pierożek, radiotelegrafistki 19. kompanii łączności z 10. dywizji piechoty, którego fragment pozwolę sobie tu przytoczyć:

„*W czerwcu 1944 r. zostałam zmobilizowana do Ludowego Wojska Polskiego, utworzonego w Związku Radzieckim. Nasza szkoła radiotelegrafistów*

mieściła się za Kijowem, miejscowości już teraz nie pamiętam. Tam odbyła się nasza przysięga. Po trzech miesiącach powróciliśmy do kraju (…) po egzaminach pod koniec października 1944 r. ruszyliśmy na front (…) do radiostacji małej mocy były nas trzy osoby – były dwie skrzynki – radiostacja ważyła 25 kg i zapas energii w drugiej skrzynce ok. 20 kg, w tym całe wyposażenie wojskowe. Na froncie radiostacja była jedyną łącznością, bo linie telefoniczne były wciąż poprzecinane …"



Zdjęcie żołnierzy 1. Pułku Łączności. Na odwrocie podpis: Zegrze 1924

Radiostacje oraz telefony wewnętrzne, często znajdują się także we wnętrzach samolotów, śmigłowców, czołgów, transporterów i samochodów wojskowych prezentowanych na wystawie plenerowej. O ich obecności jednak świadczą co najwyżej sterczące z pojazdów anteny. Przy grupowym zwiedzaniu z przewodnikiem czy w trakcie muzealnych pikników można wejść do niektórych wnętrz i zobaczyć m.in. radiostację R-113 w transporterze BTR-152 czy R-123 w czołgu T-72. Jednak na ekspozycji plenerowej znajdują się jeszcze dwa bardzo cenne eksponaty związane z łącznością, o których warto napisać nieco szerzej. Są to wozy dowódcze BTR-50 PU oraz BTR-60 PU12. Oba oparte na podwoziach pojazdów nietypowych i bardzo nielicznie używanych w Wojsku Polskim, które na wyposażeniu posiadało ich polsko-czechosłowac-

kie odpowiedniki – TOPASy i SKOTy. Niestety oba do muzeum trafiły pozbawione swojego „serca”, a więc wyposażenia wewnętrznego świadczącego przecież o ich funkcji w wojsku.



Transporter opancerzony BTR-50 PU

BTR-50 wyprodukowany został w Wołgogradzkiej Fabryce Traktorów w l. 60. XX w. Stanowił on wyposażenie 23. kompanii łączności z 7. Łużyckiej Dywizji Desantowej, która stacjonowała w Gdańsku-Wrzeszczu. Był to jeden z trzech wozów wyposażonych w radiostacje standardu najpierw R-2, a w latach 1980-82 zmodernizowane do standardu R-3 (pozostałe dwa wozy oparte były na transporterach TOPAS). Do muzeum transporter przekazany został latem 1991 r. przez JW 2201 ze Słupska, gdzie gromadzono wycofywany ze służby w jednostce obrony wybrzeża sprzęt. Wkrótce potem został poddany zewnętrznej konserwacji. Wewnątrz pozostał jedynie rozkładany stół sztabowy, nad którym w stropie kadłuba umieszczono – dla wygodnego opracowywania map – duży świetlik kryty zamykaną, pancerną osłoną. Opracowana w 1959 r. wersja PU przeznaczona była do przewozu do 10 żołnierzy, w tym trzech w przedziale kierowania (kierowca, dowódca wozu oraz nawigator), trzech operatorów radiostacji, radiotelegrafisty oraz trzech oficerów. Oryginalnie w przedziale desantowym na bocznych burtach znajdowały się półkomplet radiolinii R-403 M, radiostacje R-112 i R-113, oraz dwie radiostacje R-105d, w tym jedna ze wzmacniaczem UM-1, łącznica ŁP-10-MR oraz odbiornik ra-

diowy R-311. W ramach modernizacji do standardu R3M wymieniono radiostacje na nowsze typy. Wszystkie te urządzenia zasilane były z czterech akumulatorów. W trakcie postoju ładowane one były z agregatu AB-1, który przewożono w skrzyni na zewnątrz pojazdu nad przedziałem silnikowym. Znajdowały się tam jeszcze trzy skrzynie na dodatkowy osprzęt. Uzbrojenie stanowił karabin PK kal. 7,62 mm.



BTR-60 PU 12

BTR-60 PU 12 powstał w 1977 r. w Gorkowskij Awtomobilnyj Zawod w Niżnym Nowogrodzie. Na bazie transportera BTR-60 powstała cała rodzina pojazdów specjalistycznych, w tym omawiana tutaj wersja PU 12 (oznaczana również jako 9S482). Wiemy, iż w Polsce używane były one w bateriach dowodzenia systemu rakiet przeciwlotniczcyh 9K33 OSA (choć zakupiono je najprawdopodobniej wraz z system 9K31 Strzała-1) W tego typu wyrzutnie rakiet wyposażone były cztery pułki artylerii przeciwlotniczej. Z pewnością trzy z nich posiadały po jednym wozie tego typu (w baterii dowodzenia), który komunikował się z kolejnymi czterema wozami dowodzenia (WD-”Rekin”?) działającymi przy bateriach bojowych.

Drzonowski egzemplarz oznaczony numerem rejestracyjnym UEZ 2301 trafił do 128. Pułku Artylerii Przeciwlotniczej w Czerwieńsku w 1983 r. Nie był to wówczas wóz nowy, z książki pojazdu wynika, iż w momencie przyjęcia na

stan pułku miał przejechane przeszło 1000 km. Jako podstawowy wóz w baterii dowodzenia używany był do 1989 r., a od tego czasu funkcjonował on równolegle z testowanym wówczas w pułku nowym system dowodzenia „Zenit".

Wóz komunikował się ze stacjami radiolokacyjnymi oraz bateryjnymi wozami dowodzenia przy pomocy trzech radiostacji R-123M, jednej R-111 oraz radiolinii R-407. Dodatkowo na wyposażaniu znajdowały się przenośne radiostacje R-107 członków załogi. Anteny radiostacji zamontowane były bezpośrednio w stropie wozu, zaś anteny radiolinii zakładane były na wysuwany maszt. W stropie wozu w miejscu, w którym zwykle znajduje się wieżyczka strzelnicza przewożono skrzynię z agregatem (prawdopodobnie agregat o niskiej mocy AB-1). Na bocznych burtach dodatkowe włazy wejściowe dla desantu, zastąpiły włazy z gniazdami, umożliwiające zewnętrzne zasilanie ww. urządzeń.

Do dowodzenia niezbędne były także: planszet (na który planszecista nanosił położenie celów lotniczych) oraz automatyczna stacja przekazywania danych ASPD-12, która komunikowała się z bateryjnymi wozami dowodzenia i informowała m.in. o aktualnej liczbie załadowanych rakiet bojowych. Załogę wozu stanowili kierowca, planszecista, starszy radiotelefonista dowódca drużyny oraz dowódca lub zastępca dowódcy plutonu/pułku Wóz w muzealnym parku cieszy oko zwiedzających od 1991 roku.

Na zakończenie chciałbym jeszcze dodać, że muzeum to nie tylko wystawy i zwiedzanie eksponatów, ale też działalność popularyzatorska, w której drzonowska placówka nie zapomina o może mniej popularnym w społeczeństwie, ale niezwykle istotnym elemencie wojskowości jakim jest historia wojsk łączności. Warto tu choćby nadmienić, iż od kilku lat w trakcie muzealnych pikników historycznych czy nocy muzeów, nasi wolontariusze organizują zabawy dla najmłodszych pn. „Sztab łączności". Do zabawy tej używają oni łącznicy ŁP-40 oraz telefonów polowych TAP-67. Dzięki niej dzieci znające współczesne smartfony mogą poznać działanie dawnych, prostych systemów komunikacji, a te nieco starsze dowiedzieć się o tym jak systemy te działały. Z kolei w kwietniu tego roku w muzealnej sali rycerskiej zrealizowana została prelekcja pn. „Technologia łączności wojskowej i cywilnej od I wojny światowej do współczesności". Jesteśmy przekonani, że dzięki nawiązaniu bliższej współpracy ze Światowym Związkiem Polskich Żołnierzy Łączności nasza działalność w tym zakresie nabierze szerszego kształtu.

płk w st. spocz., hm. Marek RUSZCZAK
ppłk w st. spocz., hm. Roman SOROCZYŃSKI

RWIE SIĘ DO SŁOŃCA, RWIE SIĘ DO GWIAZD SYGNAŁ HARCERSKIEJ POBUDKI …

Mamy nadzieję, że tytułowy cytat z harcerskiej piosenki obudzi w wielu czytelnikach ważne wspomnienia z młodości. Wielu z nas przed założeniem wojskowego munduru nosiło z dumą mundur harcerski. Wielu z nas z dumą umieszczało miniaturkę krzyża harcerskiego na kieszeni wyjściowego munduru. Wreszcie wielu łączyło czynną służbę wojskową z działalnością instruktorską w Harcerstwie, zazwyczaj w zakresie wychowania obronnego.

Umożliwiały to postanowienia pragmatyki służbowej, decyzje dowódców różnych szczebli, a przede wszystkim istnienie Wojskowych Kręgów Instruktorskich jako pełnoprawnych podmiotów ruchu młodzieżowego w Wojsku Polskim.

Mój macierzysty krąg instruktorski (przy Wojskowej Akademii Technicznej w Warszawie) powstał w 1965 roku i początkowo miał w nazwie przymiotnik Studencki, by po ponad dziesięciu latach zmienić ją na Wojskowy Krąg Instruktorski przy WAT. 4 grudnia 1970 roku SKI przy WAT otrzymał imię „Czwartaków AL”. Głównym gościem honorowym na tej uroczystości był generał brygady harcmistrz Edwin ROZŁUBIRSKI – kiedyś dowódca plutonu „Czwartaków”, później dowódca 6 Pomorskiej Dywizji Powietrzno-Desantowej. W 1972 roku nasza uczelnia została odznaczona Krzyżem „Za Zasługi dla ZHP”. W uzasadnieniu wniosku zapisano między innymi „za działalność Studenckiego Kręgu Instruktorskiego na rzecz wychowania obronnego harcerzy Chorągwi Stołecznej”. Dziś trudno szukać śladów tej działalności, nie ma ich w Sali Tradycji, nie ostały się w pamięci obecnych podchorążych i studentów …

Krąg druha Romana działał przy ALMA MATER wielu wojskowych łącznościowców – w Zegrzu. Dokonał niebywałego wyczynu zdobywając trzy razy z rzędu tytuł WZOROWEGO WOJSKOWEGO KRĘGU INSTRUKTORSKIEGO! A końcowe lata jego działalności – przy Komendzie Hufca w Serocku – giną w mroku niepamięci …

Z kwerendy w materiałach Muzeum Harcerstwa w Warszawie wynika, że już w 1968 roku, wśród ponad stu tysięcy instruktorów ZHP, aż dwa tysiące

stanowili żołnierze w czynnej służbie wojskowej. W 1973 roku Wojskowe Kręgi Instruktorskie działały we wszystkich dziewiętnastu chorągwiach ZHP. W roku 1984 roku w SZ działało 258 kręgów instruktorskich, skupiających około 3700 osób. W dokumentach przewijają się: Krąg Instruktorski przy Wojskowej Akademii Medycznej, Wojskowy Krąg Instruktorski przy Wyższej Oficerskiej Szkole Wojsk Łączności w Zegrzu, także kręgi przy Wyższej Oficerskiej Szkole Wojsk Radiotechnicznych w Jeleniej Górze, przy Wyższej Szkole Marynarki Wojennej, przy jednostce wojskowej w miejscowości Irena (przedmieście Dęblina), przy jednostkach Wojsk Ochrony Pogranicza, a nawet - na okręcie ORP „Warszawa".

Z dokumentów wynika, że liczba zespołowych oraz indywidualnych Odznak Honorowych „Za Zasługi dla ZHP" przyznanych osobom i podmiotom z Wojska Polskiego w latach 1965-1989 przekracza pół tysiąca. Ale ustalenie konkretnych danych osobowych, dorobku instruktorskiego, szczególnych zasług jest po tylu latach bardzo trudne. Tylko w Chorągwi Wielkopolskiej powstało opracowanie dotyczące pracy WKI w latach 1960-1990 (autor mjr dr med. hm. Tadeusz Böhm).

Jako oficerowie w stanie spoczynku i czynni instruktorzy, współpracując z Muzeum Harcerstwa w Warszawie podjęliśmy próbę zebrania materiałów i relacji o Wojskowych Kręgach Instruktorskich, a może - również o oficerach i żołnierzach działających w ZHP poza strukturami WKI.

Zwracamy się zatem do czytelników z apelem: przywróćmy razem pamięć o ludziach, zdarzeniach, sukcesach instruktorów ZHP w wojskowych mundurach; jeśli pamiętacie swoją działalność harcerską, jeśli pamiętacie działalność swoich Kolegów, jeśli macie dostęp do dokumentów, zdjęć, dyplomów, plakietek i innych materialnych artefaktów – podzielcie się nimi z Muzeum Harcerstwa w Warszawie albo z Komisjami Historycznymi poszczególnych chorągwi ZHP.

Druhowie – POBUDKA!

SPRZĘT ŁĄCZNOŚCI I INFORMATYKI

gen. dyw. Krzysztof KOCIUBA

ENABLING MULTIDOMAIN OPERATION THROUGH DIGITAL RESILIENCE



NCIA Chief of Staff Major General **Krzysztof Kociuba** highlights NCIA's role in enabling NATO's ability to conduct multi-domain operations while remaining ever ready to face challenges across all its operating

Executive summary

Over the past decade, NATO has adapted its strategic posture to address a complex security environment. Following Russia's annexation of Crimea in 2014, NATO approved the Readiness Action Plan, enhancing deterrence, responsiveness, and forward presence. This paved the way for Multi-Domain Operations (MDO), integrating land, sea, air, space, and cyber capabilities to ensure operational efficiency and rapid crisis response.

NCIA plays a central role in enabling MDO by designing secure communication networks, integrating C4ISR capabilities, and safeguarding NATO's digital infrastructure. Through cybersecurity provided by the NATO Cyber Security Centre (NCSC), NATO ensures that its systems remain resilient and operational even in the face of cyber threats. Exercises like Steadfast Defender and CWIX validate network readiness under realistic conditions.

Emerging technologies like artificial intelligence, cloud computing, and automation accelerate NATO's decision-making processes. NCIA's partnerships with private industry enhance innovation while maintaining interoperability and

resilience. The Readiness and Response Concept of Operations (R2 CONOPS) further ensures NCIA's crisis response capability by defining roles, enhancing situational awareness, and supporting decision-making during contingencies.

Despite these advancements, challenges remain in overcoming interoperability gaps among legacy platforms and rapidly evolving domains like space and cyber. Strategic competition and hybrid attacks test NATO's adaptability. To counter these threats, NATO's readiness must prioritize connection, resilience, and innovation. Through cutting-edge technology and strong partnerships, NCIA ensures NATO remains prepared for future challenges.

W ciągu ostatniej dekady NATO znacząco zmieniło swoją strategiczną postawę, stawiając na adaptację w obliczu dynamicznie zmieniającego się środowiska bezpieczeństwa. Wyzwaniami, jakie przed Sojuszem stoją, są rosnąca liczba zagrożeń hybrydowych, intensyfikuje się konkurencja geopolityczna, a technologie, szczególnie w obszarze cyberprzestrzeni i przestrzeni kosmicznej gwałtownie zmieniają sposób prowadzenia operacji. W obliczu tych wyzwań NATO nie tylko dostosowuje swoje struktury wojskowe, ale również inwestuje w mechanizmy pozwalające na lepszą współpracę między państwami członkowskimi, co ma kluczowe znaczenie dla zachowania wspólnego bezpieczeństwa.

W 2014 roku, po nielegalnej aneksji Krymu przez Rosję, która była rażącym pogwałceniem prawa międzynarodowego, sojusznicy zaakceptowali Plan Gotowości (Readiness Action Plan). Plan ten był odpowiedzią na rosnące zagrożenie ze strony Moskwy i zakładał działania pozwalające NATO na wzmocnione odstraszanie, bardziej efektywne reagowanie oraz zwiększenie obecności na wschodnich krańcach Sojuszu. Wprowadzenie planu stało się ważnym krokiem ku budowaniu elastycznej i gotowej do działania struktury, która może sprostać różnorodnym wyzwaniom od tradycyjnych operacji wojskowych po reakcje na ataki cybernetyczne czy wyzwania związane z bezpieczeństwem energetycznym.

NATO zdaje sobie sprawę, że kluczem do skuteczności nie jest sam liczebność wojsk, czy ilość sprzętu, ale również zdolność do szybkiego i precyzyjnego działania w oparciu o dostęp do najnowszych i najbardziej wiarygodnych informacji. Współczesne operacje wojskowe nie ograniczają się już

tylko do domen powietrza, lądu i morza; coraz większe znaczenie zyskuje cyberprzestrzeń oraz przestrzeń kosmiczna. Zdolność sojuszu do łączenia i analizowania danych w czasie rzeczywistym, dzielenia się nimi między sojusznikami oraz podejmowania skoordynowanych decyzji jest fundamentem sukcesu. Gotowość NATO zależy więc w równym stopniu od infrastruktury fizycznej, co od rozwiniętego, zintegrowanego cyfrowego ekosystemu.

Cyfrowy kręgosłup NATO pełni kluczową rolę w procesach decyzyjnych oraz operacyjnych. Odporna, zabezpieczona i nowoczesna infrastruktura cyfrowa daje dowódcom NATO zdolność do szybkiego rozpoznawania sytuacji, oceny zagrożeń i podejmowania działań wyprzedzających, zanim adwersarze będą w stanie odpowiedzieć. Ta przewaga technologiczna jest nie tylko środkiem do zwiększenia efektywności operacyjnej, ale także demonstracją jedności, innowacyjności i siły politycznej Sojuszu. Na tym właśnie polega istota Wielodomenowych Operacji (ang. Multi-Domain Operations (MDO)) – harmonizacja zdolności i efektów we wszystkich domenach, aby utrzymać przewagę operacyjną.

Jednocześnie NATO podejmuje kroki, aby wzmocnić współpracę między państwami członkowskimi w zakresie badań i rozwoju. Inwestycja w nowoczesne technologie, takie jak sztuczna inteligencja (AI), analiza danych w dużych zbiorach (Big Data) czy narzędzia zwiększające cyberbezpieczeństwo, jest kluczowa dla budowy odpornej przyszłości. To podejście jest dowodem, że sojusznicy rozumieją, iż bezpieczeństwo poszczególnych państw członkowskich jest nierozerwalnie związane z bezpieczeństwem całego Sojuszu, a tylko wspólne działania mogą zagwarantować stabilność w coraz bardziej niestabilnym świecie.

Wielodomenowe Operacje NATO

Cyfrowy kręgosłup Wielodomenowych Operacji jest kluczowym elementem NATO, umożliwiającym sprawne funkcjonowanie Sojuszu w dynamicznych warunkach współczesnego pola walki. Codzienna działalność Agencji Łączności i Informatyki - NCIA (NATO Communications and Information Agency) koncentruje się na projektowaniu, dostarczaniu i ochronie zintegrowanych sieci komunikacyjnych oraz systemów, które pozwalają siłom NATO działać w sposób bezpieczny, płynny i efektywny. Od sieci misji w terenie po codzienne usługi

cyfrowe wspierające kwaterę główną NATO, eksperci NCIA inżynierowie, analitycy i specjaliści ds. cyberbezpieczeństwa dbają o przepływ zaufanych i bezpiecznych informacji będący podstawą odstraszania i obrony.

Działania NCIA integrują dowodzenie, kontrolę, komunikację, komputery, wywiad, nadzór i rozpoznanie (C4ISR) na każdym poziomie, skutecznie łącząc decydentów i operatorów. Dzięki temu NATO zyskuje zdolność do szybkiego reagowania na zagrożenia oraz koordynacji działań w ramach operacji wielodomenowych. Ćwiczenia NATO, takie jak Steadfast Defender, Steadfast Cobalt i CWIX, testują zdolności sieci w realistycznych warunkach, zapewniając niezawodne i gotowe komunikacje chronione warstwą zaawansowanego cyberbezpieczeństwa.

Cyberbezpieczeństwo jest fundamentem C4ISR. Na połączonym polu walki każda słabość w sieci czy systemach stwarza przeciwnikom możliwość ataku, co może prowadzić do natychmiastowych konsekwencji operacyjnych. Dlatego celem cyberbezpieczeństwa w NATO jest odporność budowana od podstaw, gwarantująca, że dowódcy i ich siły mogą polegać na zabezpieczonych sieciach, nawet w najbardziej wymagających sytuacjach.

Zespoły cybernetyczne NCIA działające w NCIA Cyber Security Centre (NCSC) zapewniają całodobowy monitoring i ochronę cyfrowej infrastruktury Sojuszu. Są odpowiedzialne za wykrywanie zagrożeń, reagowanie na incydenty oraz wzmacnianie obrony w sieciach oraz środowiskach operacyjnych. Bezpieczne środowisko operacyjne równa się gotowemu środowisku, dlatego NCSC gwarantuje gotowość sieci w całym Sojuszu, jednocześnie dostosowując się do wciąż ewoluujących zagrożeń.

Ponadto działania NCSC wspierają testy odporności NATO na cyberataki, przyczyniając się do budowy odpornych systemów, które odgrywają decydującą rolę w zachowaniu przewagi operacyjnej. Zintegrowana infrastruktura cyfrowa NATO jest nie tylko ważnym narzędziem w zabezpieczaniu zasobów przed wystąpieniem kryzysów na polu walki, ale też potwierdzeniem zdolności Sojuszu do zarządzania informacją w najbardziej skomplikowanych scenariuszach operacyjnych. To właśnie przepływ informacji chroniony zaawansowanym cyberbezpieczeństwem stanowi fundament Wielodomenowych Operacji i sukcesu NATO w globalnym środowisku bezpieczeństwa.

Transformacja cyfrowa NATO

Transformacja cyfrowa NATO jest jednym z filarów, które decydują o zdolności Sojuszu do skutecznego działania w obliczu współczesnych wyzwań. NCIA odgrywa kluczową rolę w napędzaniu tej transformacji, wykorzystując najnowocześniejsze technologie, aby wspierać operacyjność i bezpieczeństwo państw członkowskich NATO.

Rozwój takich obszarów, jak sztuczna inteligencja, przetwarzanie w chmurze, zarządzanie danymi na dużą skalę, automatyzacja kluczowych procesów oraz implementacja innych zaawansowanych rozwiązań technicznych, pozwala NCIA na przyspieszenie cyklu podejmowania decyzji przez NATO. W efekcie Sojusz zyskuje możliwość nie tylko szybkiego reagowania na nowe wyzwania, ale również poprawy świadomości sytuacyjnej poprzez dostarczanie dokładnych i wszechstronnych informacji w czasie rzeczywistym.

Oprócz usprawnienia procesu decyzyjnego, NCIA koncentruje się na inwestowaniu w systemy danych, które umożliwiają błyskawiczny i bezpieczny transfer informacji. Dzięki zaawansowanym narzędziom do analizy oraz przekształcania surowych danych w przydatne informacje, NATO jest w stanie skuteczniej przewidywać potencjalne zagrożenia i podejmować strategiczne działania w oparciu o precyzyjne analizy.

Integracja innowacji technologicznych w codzienne operacje Sojuszu ma kluczowe znaczenie dla utrzymania NATO w czołówce globalnych osiągnięć technologicznych. Stałe inwestycje w najnowsze rozwiązania pozwalają Sojuszowi dostosowywać się do szybko zmieniającego się środowiska bezpieczeństwa, jednocześnie umacniając zdolności współpracy międzynarodowej oraz ochrony interesów państw członkowskich.

Dzięki dynamicznemu rozwojowi infrastruktury cyfrowej, NCIA odgrywa istotną rolę w zapewnieniu, że Sojusz pozostaje przygotowany nie tylko na obecne, ale i przyszłe wyzwania, jednocześnie koncentrując się na budowaniu zaufania i stabilności w społeczności międzynarodowej. Cyfrowa transformacja NATO jest więc nie tylko wyrazem innowacyjności, ale również świadectwem strategicznej wizji przyszłości Sojuszu.

Transformacja oparta na partnerstwie

Ponieważ przemysł odgrywa kluczową rolę w tworzeniu innowacji kształtujących cyfrową przestrzeń informacyjną, skuteczna współpraca między NATO a sektorem prywatnym staje się nie tylko założeniem, ale koniecznością

w procesie modernizacji zdolności cyfrowych Sojuszu. Dynamicznie zmieniające się potrzeby operacyjne NATO wymagają rozwiązań, które bazują na najnowocześniejszych technologiach, umożliwiających zarówno skuteczne działanie w czasie rzeczywistym, jak i zabezpieczenie infrastruktury cyfrowej przed rosnącymi zagrożeniami cybernetycznymi. NCIA jako jedna z głównych jednostek odpowiedzialnych za rozwój i wdrażanie technologii w NATO, znacznie rozszerzyła swoje partnerstwa z podmiotami zewnętrznymi, aby w sposób skuteczny i szybki dostarczać nowoczesne rozwiązania dopasowane do potrzeb Sojuszu.

Zaangażowanie NCIA w współpracę z sektorem prywatnym obejmuje nie tylko realizację otwartych konkursów i zawieranie ramowych umów, ale również wczesne włączanie przemysłu w proces projektowania rozwiązań. Ten model współpracy pozwala na efektywne wprowadzanie komercyjnych innowacji do systemów NATO, przy jednoczesnym zachowaniu kluczowych warunków takich jak interoperacyjność, odporność i bezpieczeństwo. Rozwiązania te są projektowane z myślą o stabilnym, długoterminowym wsparciu infrastruktury cyfrowej NATO, aby sprostać różnorodnym wyzwaniom, z którymi Sojusz może się zetknąć na polu walki w przyszłości.

W ostatnich latach NCIA skoncentrowała się na licznych usprawnieniach mających na celu zwiększenie efektywności operacyjnej i gotowości całej organizacji. Kluczowymi działaniami w tym zakresie były: modernizacja procesów, implementacja innowacyjnych metod dostarczania zdolności technologicznych i usług, a także rozwój kompetencji personelu. Te działania sprawiają, że odpowiedzi na potrzeby klientów NATO, niezależnie od ich skali czy złożoności, są szybkie, dokładne i dostosowane do specyfiki danego wyzwania.

Priorytetem NCIA pozostaje także modernizacja procesów zakupowych, które odgrywają kluczową rolę w zapewnianiu NATO dostępu do najnowocześniejszych technologii i rozwiązań. Dzięki inwestycjom w narzędzia cyfrowe, możliwe jest zwiększenie przejrzystości i efektywności procesów logistycznych, co bezpośrednio przekłada się na poprawę organizacji i realizacji strategicznych działań. Dodatkowo, NCIA skupia się na budowaniu wspólnego zrozumienia i współpracy między członkami Sojuszu poprzez wprowadzanie dobrze udokumentowanych procedur gotowości. Taka strategia pozwala na lepszą koordynację działań, minimalizowanie ryzyka operacyjnego oraz osiąganie wysokiej skuteczności w reagowaniu na różnorodne kryzysy.

Poprzez integrację partnerstw, innowacyjnych rozwiązań przemysłowych i efektywne zarządzanie procesami operacyjnymi, NCIA zdecydowanie wzmacnia pozycję NATO jako lidera w kwestii technologicznych adaptacji w obszarze obrony i przygotowania na ewentualne wykorzystania technologii na teatrze działań. Wspólna praca w ramach platformy Sojuszu pozwala na realizację celu, jakim jest cyfrowa transformacja, która nie tylko buduje zdolność NATO do ochrony przed zagrożeniami, ale również zapewnia przewagę operacyjną w coraz bardziej złożonym środowisku bezpieczeństwa.

Wyzwania i gotowość do działania

Krajobraz C4ISR NATO jest złożoną mieszanką narodowych wkładów, przestarzałych platform oraz rozwijających się technologii. Luki w interoperacyjności nadal się utrzymują, szczególnie w miarę szybkiego rozwoju nowych domen, takich jak przestrzeń kosmicznai cyberprzestrzeń. Aby skutecznie rozwiązać te problemy, NCIA na potrzeby NATO musi rozwijać otwarte architektury i wspólne standardy poprzez kontynuowane inwestycje, zaangażowanie sojuszników oraz współpracę z sektorem prywatnym i przemysłem. NATO musi także traktować swoją cyfrową infrastrukturę jako strategiczny zasób, równorzędny z tradycyjnymi siłami zbrojnymi, aby osiągnąć jedność działania oraz skutecznie odstraszać przeciwników.

Przyszłe wyzwania wystawią zdolności adaptacyjne NATO na próbę. Rywalizacja strategiczna staje się coraz bardziej intensywna, ataki hybrydowe rozmywają granice między pokojem a konfliktem, a cyfrowe zależności znacząco wzrastają. Przeciwnicy NATO pozostają gotowi do wykorzystania przestrzeni informacyjnej, aby osłabić spójność Sojuszu i wpłynąć na jego zdolność do skutecznej obrony. W obliczu takich wyzwań NATO musi reagować szybciej, bardziej precyzyjnie i elastycznie. Kluczowym elementem skuteczności staje się równoczesne przewidywanie zagrożeń, podejmowanie decyzji i działanie zgodnie z dynamiczną sytuacją na arenie międzynarodowej.

W tym kontekście kluczową rolę odgrywa Koncepcja Gotowości i Reagowania (Readiness and Response Concept of Operations R2 CONOPS), która wspiera efektywność NCIA w reagowaniu na kryzysy i zagrożenia. R2 CONOPS nie tylko definiuje procesy ciągłości działania, ale także precyzuje role, umożliwia skuteczną koordynację liderów i dostarcza jasne procedury, które wspierają NATO w realizacji działań operacyjnych w pełnym zakresie misji So-

juszu. Jasno określone procesy i zwiększona świadomość sytuacyjna pozwalają NATO podejmować decyzje w odpowiednim czasie oraz synchronizować działania pomiędzy Kwaterą Główną NATO, Dowództwami Strategicznymi i agencjami partnerskimi.

Ćwiczenia symulacyjne organizowane przez NCIA, takie jak Table Top Exercise, są nieodzownym elementem sprawdzania gotowości Agencji. Te regularne szkolenia nie tylko potwierdziły efektywność systemu R2 CONOPS, ale również pozwoliły NCIA na identyfikowanie mocnych stron, eliminowanie luk w procesach, ograniczanie ryzyka i doskonalenie procedur. Dzięki takim działaniom NATO pozostaje przygotowane na każdą sytuację operacyjną, a NCIA dowodzi, że gotowość to proces ciągły, wymagający stałego doskonalenia, innowacji i współpracy na poziomie strategicznym.

Poprzez konsekwentną integrację współpracy z partnerami przemysłowymi, wykorzystanie zaawansowanych technologii oraz zaangażowanie innowacyjnych talentów, NCIA zapewnia, że przyszłe działania NATO sprostają wyzwaniom. Gwarantuje również zdolność Sojuszu do skutecznej obrony w każdej domenie operacyjnej: lądowej, morskiej, powietrznej, kosmicznej i cybernetycznej. Gotowość NATO nie jest już jedynie kwestią najlepszej postawy czy strategii, ale fundamentalnie opiera się na zdolności do efektywnego połączenia, dostosowania się i reagowania w dynamicznie zmieniającym się środowisku bezpieczeństwa.

gen. bryg. rez. Włodzimierz NOWAK

PRODUKCJA „DUAL USE" – CORAZ BARDZIEJ ISTOTNA W SYSTEMIE BEZPIECZEŃSTWA PAŃSTWA

Geopolityka napędza popyt na wiele produktów wykorzystywanych w produkcji zbrojeniowej szybciej, niż producenci są w stanie go obsłużyć. Dobrze to widać w tak dynamicznie rozwijającym się obszarze technologii jak drony. Przyjmijmy jako przykład Polskiego producenta dronów, który zatrudnia kilkanaście osób, rozpoczynającego rozmowy z MON, z pojawiającymi się pierwszymi zapytaniami z zagranicy.

Jak wygląda jego sytuacja od środka ? Z czym się taka firma mierzy nie mając wcześniejszych doświadczeń we współpracy z MON ? Czego brakuje, jakich kompetencji firma szuka na zewnątrz ?, gdzie ma luki których nie obsłuży samodzielnie? Okazuje się że kompetencje nie wystarczają , trzeba spełnić wiele warunków formalnych.

Wiele firm zachęconych kontraktami z wojskiem rozważa rozpoczęcie współpracy z MON, nie mając świadomości że wówczas firma przestanie już być „startupem od dronów", a zaczynie być mini-przemysłem obronnym. A wówczas pojawiają się problemy- technologia przestaje być wąskim gardłem, a wąskim gardłem staje się organizacja.

Firmy rozpoczynające współpracę w segmencie obronnym zazwyczaj są „za małe" na tworzenia własnych działów wsparcia: controlingu, HR, compliance, bezpieczeństwa itp., ale już „za duże" na improwizację. Potrzebują więc całego zaplecza usługowego, którego same nie zbudują.

I to jest chyba najważniejsza zmiana geopolityczna ostatnich lat. Powstaje ogromna warstwa pośrednia, między startupem technologicznym a klasycznym przemysłem zbrojeniowym, wspomagająca funkcjonowanie startupów technologicznych w obszarze obronności.

Ten nasz przykładowy Polski producent ma, dobry produkt, prototyp sprawdzony w testach, pierwsze rozmowy z Ministerstwo Obrony Narodowej, być może zainteresowanie z państw bałtyckich albo Skandynawii. Na papierze wygląda to jak sukces. Od środka – zaczyna się przeciążenie. Pierwsze wyzwanie jakie się pojawia to skala i tempo produkcji. Do tej pory firma budowała

5–10 platform miesięcznie, MON zaczyna mówić o setkach. Klient zagraniczny pyta o serwis, gwarancję, cyberbezpieczeństwo, zgodność z normami NATO, eksport komponentów dual-use. Nagle firma uświadamia sobie, że:

- nie ma działu compliance,
- nie ma controllingu projektowego,
- nie ma procedur jakościowych klasy przemysłowej,
- nie ma cyberbezpieczeństwa na poziomie wymaganym dla obronności,
- nie ma ludzi od kontraktów międzynarodowych,
- nie ma zdolności zakupowych i logistycznych.

Firma nie jest w stanie obsłużyć wszystkich wymagań formalnych, ma więc dwa wyjścia: rozbudować strukturę administracyjną lub poszukać wsparcia wśród firm wyspecjalizowanych w potrzebnych obszarach. I to jest moment, w którym firma musi zdać się na wsparcie firm wyspecjalizowanych, które stworzą cały ekosystem usług. Bardzo rzadko taka firma chce wszystko budować sama. Bo jej przewaga jest gdzie indziej: to algorytm, platforma, integracja, sensor czy software, a wszystko inne będzie outsourcowane albo współdzielone.

I tak np. usługi zewnętrzne (outsourcing) jakie pomogą wejść małej firmie na rynek zbrojeniowy to:

A. Profesjonalne finanse i księgowość (F&A)

Na początku całą księgowość startupu obsługiwało biuro rachunkowe. Teraz pojawiają się: kontrakty wieloletnie, zaliczki, finansowanie produkcji, granty, offset, rozliczenia eksportowe, kursy walut, kontrola marży na projektach, audyty, itp. I to już nie wystarczy, bardzo często właśnie tu następuje pierwszy kryzys- firma ma zamówienia, ale nie ma kapitału obrotowego, żeby je wykonać. Firma potrzebuje więc profesjonalnego: controllingu, modelowania cash flow, pozyskania finansowania pomostowego oraz przygotowania pod inwestora lub fundusz.

B. IT i cyberbezpieczeństwo

W sektorze obronnym bardzo szybko okazuje się, że „normalne IT" nie wystarcza. Pojawiają się dodatkowe wymagania takie jak:

- segmentacji sieci,
- ochrona dokumentacji technicznej,
- bezpieczna komunikacja,

- kontrola dostępu,
- klasyfikacja informacji,
- zgodności z wymaganiami NATO i UE,
- zapewnienie odporności na cyberatak i sabotaż.

Dla małej firmy to duże wyzwanie, bo dotąd wszystko działało „na Teamsach i Dropboxie". Firma zaczyna więc szukać: dostawcy SOC, bezpiecznych środowisk projektowych, doradztwa w zakresie NIS2 oraz wsparcia przy organizacji kancelarii tajnej i obiegu informacji niejawnych.

C. Human Resources (HR)

W praktyce okazuje się że największym deficytem nie są pieniądze, tylko ludzie.

Gwałtownie wzrasta zapotrzebowanie na specjalistów; embedded developerów, radiowców, ekspertów od AI/computer vision, operatorów BSP, inżynierów certyfikacji oraz ludzi z doświadczeniem wojskowym. Pozyskanie na rynku takich specjalistów nie jest proste i jest dość kosztowne.

D. Prawo i compliance

Tu pojawia się największy skok złożoności, bo firma zaczyna dotykać:

- eksportu dual-use,
- kontroli technologii,
- licencji,
- certyfikacji,
- wymogów offsetowych,
- kontraktów państwowych,
- odpowiedzialności za łańcuch dostaw.

Wyspecjalizowana firma z pewnością poradzi sobie z tymi problemami lepiej.

E. Produkcja i łańcuchy dostaw (supply chain)

To często najbardziej niedoceniany problem, bo drona można zaprojektować w garażu ale nie da się w garażu zapewnić powtarzalności i jakości w dużej skali produkcji. Później okazuje się, że jakiś komponent pochodzi z Chin, firmware ma ograniczenia eksportowe, kamera zawiera element objęty restrykcjami a na dostawę baterii trzeba czekać 40 tygodni (lead time). Wówczas firma zaczyna desperacko szukać alternatywnych dostawców, czy nowych partnerów produkcyjnych.

Wyobraźmy sobie firmę, która dostarcza komponenty do polskiego producenta dronów – elektronikę, optykę, podzespoły. Sama, drona, nie produkuje, ale to od niej zależy, czy producent dotrzyma swoich zobowiązań. Z jakimi certyfikacjami taka firma musi się zmierzyć? Dlaczego te procesy są w ogóle ważne, kto zazwyczaj certyfikuje i co konkretnie się sprawdza? To bardzo ciekawy moment rynku, bo dziś przewagę zdobywa nie tylko producent drona, ale cały jego łańcuch dostaw. I często okazuje się, że największym ryzykiem dla kontraktu nie jest sam BSP, tylko mały dostawca komponentów, który „nie dowozi" formalnie, jakościowo albo pod względem bezpieczeństwa. Bo poddostawca dostarczający: elektronikę, sensory, optykę, moduły radiowe, elementy AI/computer Visio itp., formalnie to tylko poddostawca ale w praktyce staje się on częścią infrastruktury bezpieczeństwa państwa. I właśnie dlatego zaczyna wpadać w świat certyfikacji, audytów i compliance, którego wcześniej często w ogóle firma nie znała.

Dlaczego te certyfikacje są tak ważne? Bo w sektorze obronnym klient nie kupuje wyłącznie produktu.

Kupuje: przewidywalność, odporność, bezpieczeństwo dostaw, możliwość audytu, zgodność z regulacjami czyli pewność, że komponent nie stanie się podatnością.

Dlatego MON czy integrator nie pyta już tylko o to „czy to działa?" Pyta: kto to wyprodukował, gdzie, z jakich komponentów, kto miał dostęp do dokumentacji, czy firmware jest bezpieczny, czy firma ma procedury jakości i czy można ją dopuścić do projektów wrażliwych. I właśnie temu służą certyfikacje.

Podstawowe wymagania z jakimi firma musi się zmierzyć to:

1. ISO 9001 – fundament wejścia do przemysłu zbrojeniowego

International Organization for Standardization

To zwykle pierwszy próg wejścia. Nie chodzi o „papier". Chodzi o udowodnienie, że firma ma odpowiednie procedury, kontrolę jakości, obieg dokumentacji, zarządzanie ryzykiem, nadzór nad dostawcami.

2. AQAP – język jakości NATO

Tu zaczyna się „prawdziwy defense”. AQAP (Allied Quality Assurance Publications) to standardy jakości NATO wymagane w wielu projektach wojskowych.

Dla małej firmy to duże wyzwanie, bo nagle okazuje się, że klient chce: pełnej identyfikowalności części, kontroli konfiguracji, formalnego zarządzania zmianą, procedur testowych, archiwizacji, prawa do audytu dostawcy. A to już nie jest zwykła produkcja przemysłowa.

3. Cyberbezpieczeństwo i NIS2

Tu nastąpiła największa zmiana ostatnich lat. Dostawca elektroniki może zostać uznany za element krytycznego łańcucha dostaw. To oznacza konieczność spełnienia wszystkich wymaganych regulacją procedur, standardów i zabezpieczeń. Klient defense coraz częściej pyta: gdzie są serwery, kto administruje środowiskiem, czy używany jest chiński hardware, jak chronione są repozytoria kodu.

4. ISO 27001 – bezpieczeństwo informacji

To często kluczowy certyfikat dla firm technologicznych. Pokazuje, że firma: chroni dane, zarządza dostępem do informacji, kontroluje ryzyka, ma procedury incydentowe i zabezpiecza własność intelektualną. W praktyce bez tego coraz trudniej wejść do projektów wojskowych i dual-use.

5. Export control / dual-use

Tu wiele firm wpada pierwszy raz w realną geopolitykę bo okazuje się, że kamera termowizyjna, moduł radiowy, sensor, kryptografia czy software sterowania, mogą podlegać ograniczeniom eksportowym. Wymaga to od firmy pełnej wiedzy o klasyfikacji towarów dual-use, embargach, sankcjach, licencjach eksportowych oraz kontroli końcowego użytkownika.

W kontekście ustawy o obrocie towarami strategicznymi i unijnego systemu kontroli produktów dual-use (podwójnego zastosowania), ograniczeniami mogą być objęte nie tylko fizyczne towary, ale również wartości niematerialne i prawne oraz wiedza techniczna. Dotyczy to zwłaszcza transferu technologii.

Do najważniejszych „niematerialnych” elementów objętych kontrolą dual-use należą:

- oprogramowanie,
- kod źródłowy,

- dokumentacja techniczna,
- know-how,
- technologie produkcji,
- instrukcje projektowe i konstrukcyjne,
- dane technologiczne,
- algorytmy kryptograficzne,
- modele symulacyjne,
- wyniki badań i prac rozwojowych,
- licencje technologiczne,
- patenty i nieopatentowana wiedza techniczna.

Szczególnie istotne jest to, że „eksportem" w rozumieniu przepisów dual-use może być również:

- wysłanie pliku e-mailem za granicę,
- udostępnienie repozytorium Git,
- przekazanie dokumentacji w chmurze,
- szkolenie techniczne cudzoziemca,
- zdalny dostęp do serwera,
- konsultacja inżynierska lub pomoc techniczna.

Takimi praktycznymi przykładami może tu być:

- oprogramowanie do kryptografii wojskowej,
- algorytmy sterowania dronami,
- modele AI do analizy obrazów satelitarnych,
- technologie radarowe,
- dokumentacja produkcji komponentów półprzewodnikowych,
- know-how dotyczący systemów naprowadzania lub cyberbezpieczeństwa.

W przepisach dual-use bardzo ważne jest pojęcie „technologii", które obejmuje informacje niezbędne do: rozwoju, produkcji, użytkowania, montażu, testowania, czy nawet konserwacji produktu. Jak widać ograniczenia nie dotyczą tylko technologii ale również jej składników niematerialnych.

Podstawą prawną w UE jest rozporządzenie UE 2021/821, a w Polsce ustawa o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym.

6. Świadectwo bezpieczeństwa przemysłowego

Zazwyczaj firma zaczyna mieć też kontakt z informacjami niejawnymi albo projektami wrażliwymi, czyli wchodzi w obszar, który wymaga posiadania kancelarii tajnej, pełnomocnika ochrony, PBO i fizycznej kontroli dostępu, więc przestaje być „zwykłym dostawcą elektroniki".

W praktyce bardzo często najtrudniejszy audyt robi nie państwo, ale główny wykonawca programu, bo to on bierze odpowiedzialność za cały łańcuch dostaw.

I tu jest przestrzeń dla firm doradczych, które mogą pomóc wejść na rynek zbrojeniowy dual use, muszą one jednak zrozumieć, że startupów nie należy traktować jak „zwykłego MŚP". To już nie jest zwykła produkcja. A startup kupuje od firmy doradczej nie prostą usługę a zdolność wejścia do większego kontraktu.

7. Logistyka i transport – drony, komponenty, części zamienne przemieszczane między producentem, klientem końcowym i partnerami zagranicznymi. Firma logistyczna sama nie produkuje, nie certyfikuje, ale jej operacje wpadają w reżim kontroli obrotu, sankcji i regulacji eksportowych dual-use. Weźmy firmę zajmującą się logistyką i transportem – dronów, komponentów i części zamiennych, przemieszczanych między producentem, klientem końcowym i partnerami zagranicznymi. Każdy ruch towaru wiąże się potencjalnie z kontrolą obrotu, sankcjami i regulacjami eksportowymi dotyczącymi produktów dual-use.

I tu pojawia się bardzo ciekawy paradoks rynku defense. Firma logistyczna często uważa, że jest „tylko transportem". Natomiast z perspektywy państwa i producenta staje się elementem systemu kontroli strategicznych technologii. Bo w sektorze dual-use problemem nie jest wyłącznie co produkujesz, ale również kto to przewozi, dokąd, przez jakie kraje, komu przekazuje, kto ma dostęp do ładunku, gdzie znajdują się dane transportowe i czy można śledzić cały łańcuch. Właśnie dlatego logistyka w defense zaczyna przypominać bardziej compliance niż klasyczny freight forwarding.

Dlaczego logistyka nagle staje się „wrażliwa"?

Wyobraźmy sobie:

- producent dronów z Polski,
- podzespoły z UE i Azji,
- integracja w Polsce,

- klient końcowy w państwie NATO,
- część serwisu realizowana lokalnie.

Teoretycznie zwykły łańcuch dostaw, ale praktycznie:

- kamera może być dual-use,
- moduł radiowy może podlegać kontroli eksportowej,
- software może zawierać kryptografię,
- bateria może być materiałem niebezpiecznym,
- odbiorca końcowy może wymagać weryfikacji sankcyjnej,
- tranzyt przez określone państwo może być zakazany.

I nagle firma logistyczna przestaje być przewoźnikiem, staje się uczestnikiem procesu zgodności eksportowej. Firma musi sprawdzać odbiorców, pośredników, kraje tranzytowe, armatorów, banki i operatorów końcowych.

W sektorze defense ogromne znaczenie ma pytanie „Czy można udowodnić, gdzie produkt znajdował się na każdym etapie?" To szczególnie ważne przy elektronice, optyce, kryptografii i sensorach.

8. Kolejny ważny element to proces wytwarzania oprogramowania. Weźmy jako przykład polski software house, który dostarcza oprogramowanie dla producentów dronów. Każda z firm – producent, dostawca komponentów, logistyk, software house jest potencjalnym celem ataku hackerskiego. Co wiec taka firma musi mieć poukładane u siebie w obszarze cyberbezpieczeństwa by w ogóle być wpuszczonym do tej współpracy? To jest dziś jeden z najważniejszych problemów całego rynku defense-tech. Bo kiedyś cyberbezpieczeństwo było „warstwą IT", dziś jest warunkiem wejścia do łańcucha dostaw. Z perspektywy klienta defense najważniejsze pytanie brzmi „Czy ta firma sama nie jest podatnością?" Bo jeśli atakujący wejdzie do repozytorium kodu, środowiska developerskiego, aktualizacji firmware czy kanału serwisowego, to może przejąć nie jedną firmę, ale cały łańcuch dostaw. I właśnie dlatego software house obsługujący drony zaczyna być traktowany niemal jak element infrastruktury krytycznej. To absolutny fundament. Klient defense nie pyta już tylko:„czy software działa?" Pyta: jak powstaje, kto ma dostęp do kodu, kto zatwierdza zmiany, czy pipeline jest bezpieczny, czy biblioteki są weryfikowane, czy można wykryć manipulację.

Bo dziś ogromnym zagrożeniem są ataki na łańcuchy dostaw (supply-chain).

W defense, bardzo szybko okazuje się, że największą podatnością nie jest firewall a jest nią człowiek. Dlatego klient oczekuje: wszędzie wieloetapowego logowania (MFA), kontroli kont uprzywilejowanych, separacji projektów i pełnego logowania dostępu. Pojawiają się istotne pytania co do organizacji procesu wytwarzania oprogramowania: kto miał dostęp do kodu, z jakiego kraju pracuje developer, czy używa prywatnego sprzętu, czy repozytorium jest izolowane oraz czy podwykonawca ma dostęp do produkcji ?. Tak więc, software house zaczyna przypominać środowisko o podwyższonym rygorze bezpieczeństwa.

Klient defense coraz częściej nie ufa już wyłącznie firmie głównej i pyta o łańcuchy dostaw. Pyta z jakich bibliotek korzystacie, kto hostuje repozytoria, gdzie jest cloud, kto administruje środowiskiem, kto robi outsourcing oraz czy dane trafiają poza UE/NATO. Tak więc software house musi umieć zarządzać nie tylko swoim ryzykiem, ale też ryzykiem swoich dostawców.

Do tego dochodzi monitoring i zdolność wykrywania incydentów. W sektorze defense zakłada się już nie „czy będzie atak", tylko „kiedy nastąpi". Dlatego ważna staje się zdolność: wykrywania, reagowania, izolowania, i odtwarzania środowiska. Co wynika z norm **ISO 27001 i NIS2,** a to coraz częściej jest minimum przystąpienia do rozmowy z MON.

Firmy chcące współpracować z MON, a nie mające doświadczenia w sektorze defense, muszą sobie zdawać sprawę z oczekiwań i warunków jakie należy spełnić. I nie chodzi tylko o technologię, chodzi też o zdolność do działania pod presją i współpracę w zakresie bezpieczeństwa państwa. Rozwój produktów dual use przez małe firmy technologiczne (startupy), przyczynia się również do rozwoju całego ekosystemu wsparcia ich produkcji i zapewnienia zgodności z wymaganiami w zakresie bezpieczeństwa produkcji.

Berta JURCZUK

CYBERZAGROŻENIA WE WSPÓŁCZESNYM ŚRODOWISKU WOJSKOWYM

Rozwój technologii informacyjno-komunikacyjnych w istotny sposób wpłynął na funkcjonowanie współczesnych państw oraz struktur odpowiedzialnych za zapewnienie bezpieczeństwa. Cyberprzestrzeń stała się obszarem intensywnej aktywności administracyjnej, gospodarczej oraz militarnej, co spowodowało konieczność uwzględnienia jej w systemie bezpieczeństwa narodowego[2]. Wraz z postępującą cyfryzacją procesów zarządzania oraz dowodzenia wzrosła również podatność na różnego rodzaju zagrożenia o charakterze cybernetycznym.

Zjawiska te sprawiają, że cyberbezpieczeństwo należy obecnie postrzegać jako jeden z kluczowych elementów współczesnego środowiska bezpieczeństwa[3]. Analiza zagrożeń oraz mechanizmów ochrony informacji stanowi istotny punkt wyjścia do dalszych rozważań dotyczących roli czynnika ludzkiego w systemie bezpieczeństwa.

W niniejszym artykule przedstawiono pojęcie cyberprzestrzeni, charakterystykę cyberzagrożeń oraz znaczenie cyberbezpieczeństwa w kontekście funkcjonowania państwa i struktur obronnych.

POJĘCIE I ZNACZENIE CYBERPRZESTRZENI W SYSTEMIE BEZPIECZEŃSTWA PAŃSTWA

Rozwój technologii informacyjno-komunikacyjnych w ostatnich dekadach doprowadził do powstania nowej przestrzeni funkcjonowania państwa, społeczeństwa oraz sił zbrojnych – cyberprzestrzeni. Stała się ona środowiskiem, w którym realizowane są procesy komunikacyjne, wymiana informacji, zarządzanie danymi oraz działania o charakterze administracyjnym, gospodarczym i militarnym.

W literaturze przedmiotu cyberprzestrzeń definiowana jest jako przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne oraz powiązania między nimi. Obejmuje ona zarówno infrastrukturę

[2] M. Marczyk, M. Stolarz, B. Terebiński, *Cyberbezpieczeństwo w teorii i praktyce. Wybrane aspekty*, Akademia Sztuki Wojennej, Warszawa 2022.
[3] J. Andress, *Podstawy bezpieczeństwa informacji. Praktyczne wprowadzenie*, Helion, Gliwice 2022.

techniczną, jak i użytkowników korzystających z sieci oraz urządzeń cyfrowych[4].

W ujęciu doktrynalnym cyberprzestrzeń postrzegana jest jako środowisko wielowarstwowe, obejmujące warstwę fizyczną, logiczną oraz tożsamości cyfrowej. Warstwa fizyczna odnosi się do infrastruktury technicznej, takiej jak urządzenia, sieci i systemy transmisyjne. Warstwa logiczna obejmuje dane, oprogramowanie oraz procesy przetwarzania informacji, natomiast warstwa tożsamości cyfrowej obejmuje funkcjonowanie podmiotów w cyberprzestrzeni poprzez ich wirtualne reprezentacje, takie jak loginy, adresy e-mail, profile czy inne identyfikatory cyfrowe. Warstwa tożsamości cyfrowej ma charakter abstrakcyjny i nie musi być bezpośrednio powiązana z rzeczywistą tożsamością osoby lub organizacji. W konsekwencji jeden podmiot może posiadać wiele tożsamości cyfrowych, a jedna tożsamość może być współdzielona przez różne podmioty[5].

Istotną konsekwencją przedstawionego modelu jest fakt, że w przeciwieństwie do warstwy fizycznej, której elementy posiadają określone położenie geograficzne, warstwa logiczna oraz warstwa tożsamości cyfrowej mają charakter transgraniczny. Oznacza to brak jednoznacznego przypisania do określonego terytorium państwowego, co istotnie wpływa na trudności w zakresie regulacji prawnych oraz zapewnienia bezpieczeństwa. Jednocześnie warstwy te pozostają ze sobą w ścisłej zależności – warstwa logiczna nie może funkcjonować bez warstwy fizycznej, natomiast warstwa tożsamości cyfrowej opiera się na zasobach warstwy logicznej[6].

Model warstwowy cyberprzestrzeni pozwala na lepsze zrozumienie jej złożonej struktury oraz identyfikację potencjalnych obszarów podatności na zagrożenia. Każda z warstw może stanowić odrębny cel oddziaływania, przy czym skutki działań podejmowanych w jednej z nich mogą wpływać na pozostałe. W szczególności naruszenia warstwy tożsamości cyfrowej może skutkować uzyskaniem nieuprawnionego dostępu do zasobów warstwy logicznej, a w konsekwencji oddziaływaniem na elementy warstwy fizycznej.

[4] P. W. Singer, A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, New York 2014.
[5] *Operacje w cyberprzestrzeni DD-3.20,* Centrum Doktryn i Szkolenia Sił Zbrojnych, Bydgoszcz 2020.
[6] Tamże.

Takie ujęcie wskazuje, że cyberprzestrzeń nie ogranicza się wyłącznie do aspektów technologicznych, lecz stanowi złożone środowisko funkcjonowania, w którym istotną rolę odgrywa zarówno infrastruktura, jak i czynnik ludzki oraz procesy informacyjne.

Wraz ze wzrostem uzależnienia instytucji publicznych i struktur wojskowych od systemów teleinformatycznych, cyberprzestrzeń zaczęła odgrywać istotną rolę w systemie bezpieczeństwa państwa. Zakłócenie jej funkcjonowania może prowadzić do ograniczenia zdolności operacyjnych, utraty poufności informacji oraz destabilizacji procesów decyzyjnych[7]. Z tego względu zagadnienia związane z ochroną cyberprzestrzeni stały się jednym z istotnych elementów współczesnej polityki bezpieczeństwa.

W dokumentach strategicznych wielu państw oraz organizacji międzynarodowych podkreśla się, że cyberprzestrzeń stanowi obecnie jeden z kluczowych obszarów oddziaływania zarówno w czasie pokoju, jak i w sytuacjach kryzysowych czy konfliktach zbrojnych[8]. Wskazuje się, że zagrożenia pojawiające się w tej domenie mogą mieć charakter transgraniczny, a ich skutki mogą oddziaływać równocześnie na strefę militarną, gospodarczą czy społeczną. Z tego względu ochrona cyberprzestrzeni została włączona do katalogu priorytetowych zadań państwa w zakresie zapewnienia bezpieczeństwa narodowego.

W polskich dokumentach strategicznych dotyczących bezpieczeństwa podkreśla się konieczność budowy i utrzymywania zdolności do zapobiegania, wykrywania oraz reagowania na incydenty w cyberprzestrzeni[9]. Zwraca się uwagę nie tylko na ochronę infrastruktury krytycznej i systemów administracji publicznej, ale również na zapewnienie ciągłości funkcjonowania struktur odpowiedzialnych za obronność. Oznacza to, że cyberbezpieczeństwo nie jest już traktowane jako zagadnienie wyłącznie techniczne, lecz jako element szerszej polityki bezpieczeństwa państwa.

---

[7] *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024*, Warszawa 2019.
M. Marczyk, M. Stolarz, B. Terebiński, *Cyberbezpieczeństwo w teorii i praktyce. Wybrane aspekty*, Akademia Sztuki Wojennej, Warszawa 2022.

[8] NATO, *Allied Joint Doctrine for Cyberspace Operations (AJP-3.20)*, Brussels 2020.
European Commission, *The EU Cybersecurity Strategy for the Digital Decade*, Brussels 2020.
The White House*, National Cyber Strategy of the United States of America*, Washington, D.C. 2018.

[9] *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024*, Warszawa 2019.
Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2020.

Istotnym krokiem w postrzeganiu cyberprzestrzeni jako obszaru o znaczeniu strategicznym było uznanie jej za domenę operacyjną. W praktyce oznacza to, że cyberprzestrzeń jest traktowana na równi z takimi domenami jak ląd, morze, powietrze czy przestrzeń kosmiczna[10]. Działania prowadzone w tym środowisku mogą wspierać operacje wojskowe, ale także mogą stanowić narzędzie oddziaływania przeciwnika, ukierunkowane na osłabienie zdolności obronnych państwa bez konieczności użycia klasycznych środków militarnych.

Wraz z rozwojem technologii oraz rosnącą cyfryzacją procesów dowodzenia i zarządzania, znaczenie cyberprzestrzeni w funkcjonowaniu sił zbrojnych systematycznie wzrasta. Systemy teleinformatyczne wspierają planowanie operacyjne, łączność, logistykę oraz obieg informacji. W konsekwencji ich zakłócenie może wpływać na sprawność podejmowania decyzji oraz skuteczność realizowanych zadań. Z tego powodu zapewnienie odpowiedniego poziomu bezpieczeństwa w cyberprzestrzeni stanowi obecnie jeden z warunków utrzymania zdolności obronnych państwa.

W kontekście funkcjonowania sił zbrojnych szczególnego znaczenia nabiera zapewnienie ciągłości wymiany informacji. System dowodzenia wymaga nieprzerwanego przepływu danych na potrzeby kierowania podległymi siłami i środkami, realizowanego w ramach sieci łączności gwarantującej dostępność, integralność oraz poufność przesyłanych informacji[11]. Zakłócenie tego procesu może prowadzić do ograniczenia zdolności dowodzenia oraz obniżenia efektywności realizowanych zadań.

W literaturze podkreśla się, że cyberbezpieczeństwo należy postrzegać nie tylko jako zbiór narzędzi technicznych, lecz jako proces obejmujący działania organizacyjne, prawne oraz edukacyjne. Zwraca się uwagę, że skuteczna ochrona systemów teleinformatycznych wymaga podejścia systemowego, uwzględniającego zarówno infrastrukturę, jak i użytkowników oraz obowiązujące regulacje[12].

[10] M. Marczyk, M. Stolarz, B. Terebiński, *Cyberbezpieczeństwo w teorii i praktyce. Wybrane aspekty*, Akademia Sztuki Wojennej, Warszawa 2022.
[11] M. Marczyk, B. Terebiński, *System łączności brygady obrony terytorialnej (BOT) w wojskowym systemie telekomunikacyjnym. Ujęcie teoretyczne*, „Kwartalnik Bellona", Military Publishing Institute, Warszawa 2021.
[12] M. Marczyk, M. Stolarz, B. Terebiński, *Cyberbezpieczeństwo w teorii i praktyce. Wybrane aspekty*, Akademia Sztuki Wojennej, Warszawa 2022.

Cyberbezpieczeństwo stanowi zatem element szerszego systemu zarządzania bezpieczeństwem państwa, w którym istotne znaczenie ma identyfikacja zagrożeń, ocena ryzyka oraz wdrażanie adekwatnych środków ochrony. Takie ujęcie wskazuje, że zapewnienie bezpieczeństwa w cyberprzestrzeni nie ogranicza się wyłącznie do aspektów technologicznych, lecz obejmuje również kształtowanie odpowiednich postaw i świadomości wśród osób korzystających z systemów informatycznych[13].

Wraz ze wzrostem znaczenia cyberprzestrzeni zwiększa się także skala oraz złożoność zagrożeń, które oddziałują zarówno na infrastrukturę techniczną jak i na użytkowników systemów teleinformatycznych.

RODZAJE I CHARAKTERYSTYKA CYBERZAGROŻEŃ

Współczesne cyberzagrożenia charakteryzują się dużą dynamiką oraz rosnącym stopniem złożoności. Rozwój technologii cyfrowych, powszechność urządzeń mobilnych oraz integracja systemów teleinformatycznych z procesami zarządzania i dowodzenia powodują, że potencjalne wektory ataku ulegają stałemu rozszerzaniu[14]. W literaturze przedmiotu wskazuje się, że zagrożenia w cyberprzestrzeni mogą mieć charakter zarówno techniczny, jak i społeczny, a ich skuteczność często wynika z połączenia obu tych elementów.

Do podstawowych rodzajów cyberzagrożeń zalicza się m.in. złośliwe oprogramowanie (malware), ataki typu phishing, ransomware, ataki typu Distributed Denial of Service (DDoS) oraz działania z zakresu inżynierii społecznej[15]. W przypadku środowiska wojskowego szczególne znaczenie mają zagrożenia ukierunkowane na zakłócenie łączności, pozyskanie informacji o charakterze operacyjnym oraz destabilizację procesu dowodzenia[16]. Jak podkreśla się w opracowaniach dotyczących bezpieczeństwa informacji, skuteczność ataku bardzo często nie wynika wyłącznie z zaawansowania technologicznego, lecz z wykorzystania podatności organizacyjnych i błędów użytkowników.

Powyższe wnioski znajdują potwierdzenie w aktualnych raportach dotyczących cyberbezpieczeństwa, w których podkreśla się, że jednym z dominujących trendów jest wzrost liczby ataków wykorzystujących techniki socjotechniczne oraz złośliwe oprogramowanie, w szczególności ransomware. Zwraca

[13] Tamże.
[14] Tamże.
[15] M. Marczyk, M. Stolarz, B. Terebiński, *Cyberbezpieczeństwo w teorii i praktyce. Wybrane aspekty*, Akademia Sztuki Wojennej, Warszawa 2022.
[16] B. Terebiński, *Teleinformatyka wojskowa,* Akademia Sztuki Wojennej, Warszawa 2021.

się również uwagę na rosnącą skalę incydentów wymierzonych w infrastrukturę krytyczną oraz systemy administracji publicznej, a także na coraz większe znaczenie operacji informacyjnych prowadzonych z wykorzystaniem cyberprzestrzeni. Analizy wskazują, że skuteczność wielu ataków wynika nie tyle z zaawansowania technologicznego, ile z wykorzystania podatności organizacyjnych oraz błędów użytkowników, co czyni czynnik ludzki jednym z kluczowych elementów systemu bezpieczeństwa[17].

W ostatnich latach zauważalny jest wzrost zagrożeń związanych z wykorzystaniem mediów społecznościowych oraz analizą dużych zbiorów danych (big data)[18]. Synergia tych obszarów umożliwia prowadzenie działań dezinformacyjnych, profilowanie użytkowników oraz budowanie przekazów oddziałujących na określone grupy odbiorców. Zjawisko to stało się szczególnie widoczne w kontekście konfliktu zbrojnego na Ukrainie, gdzie działania informacyjne i cybernetyczne stanowiły istotny element szerszej strategii oddziaływania[19]. Oprócz klasycznych ataków na infrastrukturę teleinformatyczną obserwowano intensywne kampanie dezinformacyjne, próby destabilizacji systemów komunikacyjnych oraz działania mające na celu wywołanie paniki wśród ludności cywilnej i żołnierzy.

Istotnym trendem jest również rosnąca liczba zagrożeń skierowanych przeciwko urządzeniom mobilnym[20]. Smartfony i tablety, wykorzystywane zarówno w życiu prywatnym, jak i służbowym, stanowią potencjalne źródło wycieku informacji. Aplikacje o niezweryfikowanym pochodzeniu, niezabezpieczone sieci Wi-Fi czy brak aktualizacji systemu operacyjnego zwiększają podatność użytkownika na ataki. W środowisku wojskowym problem ten nabiera szczególnego znaczenia, zwłaszcza w sytuacji korzystania z alternatywnych środków łączności poza infrastrukturą resortową.

Do nowszych form zagrożeń zalicza się również wykorzystanie sztucznej inteligencji do generowania treści dezinformacyjnych (deepfake), automatyzację ataków phishingowych oraz stosowanie narzędzi umożliwiających masowe skanowanie podatności systemów. Takie działania pozwalają na prowadzenie

[17] European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2023.
NASK – Państwowy Instytut Badawczy, Raport z działalności CERT Polska 2023, Warszawa 2024.
[18] J. Waszewski, *„Nie ukryjesz się". Konsekwencje synergii big data, mediów społecznościowych i neuronauki*, Akademia Sztuki Wojennej, Warszawa 2021.
[19] *Disinformation in the Russian invasion of Ukraine,* https://en.wikipedia.org/wiki/Disinformation_in_the_Russian_invasion_of_Ukraine.
[20] P. Verma, A. Dixit, *Bezpieczeństwo urządzeń mobilnych. Receptury,* Helion, Gliwice 2017.

operacji o charakterze hybrydowym, łączących oddziaływanie informacyjne, psychologiczne i cybernetyczne.

Na gruncie krajowym podkreśla się konieczność stałego monitorowania zagrożeń oraz podnoszenia poziomu świadomości użytkowników systemów teleinformatycznych. Doświadczenia ostatnich lat wskazują, że zagrożenia cybernetyczne nie ograniczają się do infrastruktury krytycznej, lecz mogą dotyczyć również pojedynczych użytkowników, których zachowania w cyberprzestrzeni mają wpływ na bezpieczeństwo całej organizacji[21]. W świetle struktur wojskowych szczególne znaczenie ma zatem właściwe przygotowanie personelu do rozpoznawania zagrożeń oraz przestrzegania zasad bezpieczeństwa informacji.

W kontekście terytorialnej służby wojskowej (tsw) specyfika pełnionej służby powoduje, że zagadnienie cyberzagrożeń nabiera dodatkowego znaczenia. Żołnierze Obrony Terytorialnej (OT) funkcjonują na styku środowiska cywilnego i wojskowego, łącząc aktywność zawodową z obowiązkami służbowymi. Taki model pełnienia służby sprzyja częstemu korzystaniu z powszechnie dostępnych narzędzi komunikacyjnych oraz urządzeń mobilnych, co może zwiększać ekspozycję na zagrożenia w cyberprzestrzeni.

W warunkach rozproszonej struktury organizacyjnej oraz rotacyjnego charakteru szkoleń istotne znaczenie ma poziom indywidualnej świadomości zagrożeń. Nawet pojedyncze nieostrożne działanie użytkownika, takie jak otwarcie podejrzanej wiadomości czy udostępnienie informacji w mediach społecznościowych, może prowadzić do naruszenia zasad bezpieczeństwa informacji. W tym kontekście cyberzagrożenia nie dotyczą wyłącznie infrastruktury technicznej, lecz również zachowań i nawyków użytkowników systemów teleinformatycznych.

Doświadczenia związane z konfliktem na Ukrainie pokazują, że działania informacyjne oraz cybernetyczne mogą być ukierunkowane także na żołnierzy oraz ich otoczenie. Analiza treści publikowanych w przestrzeni internetowej, próby profilowania czy kampanie dezinformacyjne mogą stanowić element szerszych operacji oddziaływania. Z tego względu podnoszenie poziomu świadomości cyberzagrożeń wśród żołnierzy OT stanowi istotny element budowania odporności informacyjnej.

[21] J. Andress, *Podstawy bezpieczeństwa informacji. Praktyczne wprowadzenie*, Helion, Gliwice 2022.

Przedstawione rodzaje cyberzagrożeń wskazują, że współczesne środowisko bezpieczeństwa charakteryzuje się wysokim poziomem niepewności oraz podatności na oddziaływanie zewnętrze. Skala i różnorodność zagrożeń powodują, że niezbędne staje się wdrażanie kompleksowych rozwiązań z zakresu cyberbezpieczeństwo, obejmujących zarówno środki techniczne, jak i działania organizacyjne oraz edukacyjne. Oznacza to konieczność przyjęcia systemowego podejścia do ochrony informacji, w którym istotną rolę odgrywa użytkownik.

CYBERBEZPIECZEŃSTWO JAKO ELEMENT ŚRODOWISKA BEZPIECZEŃSTWA – ROLA CZYNNIKA LUDZKIEGO

Skala i złożoność współczesnych cyberzagrożeń powodują, że cyberbezpieczeństwo należy postrzegać jako integralny element systemu bezpieczeństwa państwa. Nie ogranicza się ono wyłącznie do wdrażania rozwiązań technicznych, lecz obejmuje działania organizacyjne, prawne oraz edukacyjne, których celem jest minimalizowanie ryzyka naruszeń poufności, integralności i dostępności informacji[22]. Ochrona informacji wymaga zatem podejścia systemowego, uwzględniającego zarówno infrastrukturę techniczną, jak i użytkowników systemów teleinformatycznych.

W literaturze przedmiotu podkreśla się, że jednym z kluczowych czynników wpływających na poziom bezpieczeństwa jest człowiek[23]. Nawet najbardziej zaawansowane zabezpieczenia techniczne nie eliminują ryzyka wynikającego z błędów użytkownika, braku świadomości zagrożeń czy nieostrożnych zachowań w cyberprzestrzeni. W środowisku wojskowym, w którym obieg informacji stanowi podstawę systemu dowodzenia oraz realizacji zadań, znaczenie odpowiedzialnych postaw użytkowników nabiera szczególnego wymiaru[24].

Współcześnie komunikacja interpersonalna w znacznym stopniu przeniosła się do przestrzeni cyfrowej. Powszechność komunikatorów internetowych, mediów społecznościowych oraz aplikacji mobilnych powoduje, że użytkownicy tworzą grupy wymiany informacji. W warunkach wojskowych może to

[22] M. Marczyk, M. Stolarz, B. Terebiński, *Cyberbezpieczeństwo w teorii i praktyce. Wybrane aspekty*, Akademia Sztuki Wojennej, Warszawa 2022.
[23] Tamże.
[24] B. Terebiński, *Teleinformatyka wojskowa*, Akademia Sztuki Wojennej, Warszawa 2021.

generować określone ryzyka, związane między innymi z nieświadomym udostępnieniem informacji niejawnych osobom nieuprawnionym, błędną identyfikacją odbiorcy czy niedostateczną weryfikacją źródła komunikatu.

Szczególnego znaczenia nabiera także proces dezinformacji. Przekazy o charakterze sensacyjnym, odwołujące się do emocji odbiorców, mogą być wykorzystywane do destabilizacji środowiska informacyjnego oraz podważania zaufania do instytucji publicznych. W ramach jednej z kampanii Zespołu Działań Cyberprzestrzennych (ZDC) WOT skierowanych do żołnierzy i społeczeństwa zwrócono uwagę, że: „fake news nie musi być wiarygodny. Wystarczy, że jest sensacyjny”[25]. Mechanizm ten opiera się na szybkim rozpowszechnianiu treści wywołujących silne reakcje emocjonalne, co utrudnia ich racjonalną ocenę oraz weryfikację źródła.

Specyfika tsw, polegająca na łączeniu cywilnej aktywności zawodowej i prywatnej ze służbą wojskową, sprawia, że żołnierze funkcjonują równocześnie w dwóch środowiskach informacyjnych – cywilnym i wojskowym. Różnorodność wieku, doświadczenia zawodowego, wykształcenia oraz poziomu kompetencji cyfrowych może wpływać na zróżnicowany poziom świadomości zagrożeń. Część użytkowników może wykazywać mniejszą czujność wobec prób socjotechnicznych, manipulacji informacyjnej czy nieautoryzowanego dostępu do grup komunikacyjnych.

W tym kontekście cyberbezpieczeństwo należy postrzegać nie tylko jako zbiór procedur i zabezpieczeń technicznych, lecz jako element kultury organizacyjnej. Budowanie odporności informacyjnej wymaga systematycznych szkoleń, kształtowania właściwych nawyków oraz promowania odpowiedzialnych postaw w zakresie korzystania narzędzi komunikacyjnych. Poziom podnoszenia kompetencji w zakresie cyberbezpieczeństwa staje się zatem jednym z podstawowych warunków skutecznej ochrony informacji w strukturach wojskowych.

W obliczu przedstawionych zagrożeń oraz znaczenia czynnika ludzkiego dla poziomu bezpieczeństwa informacji zasadne staje się odniesienie powyższych rozważań do konkretnego środowiska organizacyjnego. Warto uwypuklić, że analiza sposobów komunikacji oraz wykorzystywanych narzędzi

[25] WOT, post opublikowany w serwisie Facebook dnia 19.02.2026 r. https://facebook.com/story.php?story_fbid=1240346458268522&id=100068795396576.

w strukturach wojskowych nabiera kluczowego znaczenia, ponieważ obieg informacji stanowi podstawę realizacji zadań.

Współczesna służba wojskowa obejmuje nie tylko działania kinetyczne, lecz również odpowiedzialność za ochronę bezpieczeństwa informacji oraz właściwe funkcjonowanie w cyberprzestrzeni, dlatego szczególnego znaczenia nabiera budowanie świadomości użytkowników w tym zakresie.

Rafał MAGOŃ
Mirosław FRIEDEK

TOPAZ + ASCA
SYSTEMY KIEROWANIA POLEM WALKI

Współczesne środowisko bezpieczeństwa ulega dynamicznym przemianom pod wpływem rozwoju technologii, nasilającej się rywalizacji geopolitycznej oraz wzrostu liczby zagrożeń hybrydowych, cybernetycznych i asymetrycznych. W konsekwencji zmienia się również charakter działań zbrojnych, w których kluczową rolę odgrywa zdolność do szybkiego pozyskiwania informacji, ich przetwarzania oraz natychmiastowego przekazywania do środków rażenia. W tych warunkach artyleria pozostaje jednym z podstawowych środków wsparcia wojsk lądowych, jednak jej skuteczność zależy obecnie nie tylko od parametrów uzbrojenia, lecz przede wszystkim od poziomu cyfryzacji systemów dowodzenia i kierowania ogniem oraz ich interoperacyjności.

Rozwój nowoczesnych systemów kierowania ogniem artylerii stanowi odpowiedź na rosnące wymagania dotyczące precyzji, szybkości reakcji oraz koordynacji działań prowadzonych w środowisku wielodomenowym. Współczesne rozwiązania integrują środki rozpoznania, stanowiska dowodzenia oraz efektory w jednolitą architekturę sieciocentryczną, umożliwiając znaczące skrócenie procesu **sensor-to-shooter**. Osiągnięcie tego efektu możliwe jest dzięki wykorzystaniu cyfrowych systemów dowodzenia, automatyzacji procesów obliczeniowych, zaawansowanych algorytmów przetwarzania danych oraz integracji z bezzałogowymi systemami rozpoznawczymi, radarami artyleryjskimi i precyzyjnymi środkami rażenia.

Systemy kierowania ogniem artylerii (Artillery Fire Control Systems – AFCS) stanowią obecnie jeden z najważniejszych elementów systemów

C4ISR. Ich zadaniem jest planowanie, koordynacja oraz realizacja zadań ogniowych z wykorzystaniem aktualnych danych o sytuacji operacyjnej. Cyfrowa automatyzacja procesu kierowania ogniem pozwala ograniczyć udział operatora w wykonywaniu obliczeń balistycznych, skrócić czas reakcji oraz zwiększyć dokładność prowadzonego ognia. Rozwiązania te wpływają jednocześnie na wzrost świadomości sytuacyjnej dowódców oraz efektywność wykorzystania dostępnych środków ogniowych.

Szczególnego znaczenia nabiera interoperacyjność narodowych systemów kierowania ogniem z rozwiązaniami stosowanymi przez państwa Sojuszu Północnoatlantyckiego. Po przystąpieniu Polski do NATO rozpoczęto proces dostosowywania krajowych systemów dowodzenia i kierowania ogniem do wymagań obowiązujących standardów sojuszniczych. Jednym z jego najważniejszych rezultatów było opracowanie oraz rozwój zautomatyzowanego systemu kierowania ogniem **TOPAZ**, który stał się podstawowym rozwiązaniem wykorzystywanym w Wojskach Rakietowych i Artylerii Sił Zbrojnych RP. Kolejnym etapem modernizacji była integracja systemu TOPAZ z programem **Artillery Systems Cooperation Activities (ASCA)**, umożliwiająca automatyczną wymianę danych o celach, zadaniach ogniowych oraz środkach wsparcia pomiędzy państwami NATO.



Przyrząd kierowania ogniem PUO-9M (ros. Прибор управления огнём ПУО-9М) – radziecki przyrząd artyleryjski przeznaczony do ręcznego wyznaczania nastaw i obliczania danych do strzelania. Źródło: [ww2-militaria-shop.de]

W badaniach zastosowano jakościową metodę analizy historyczno-porównawczej, ukierunkowaną na ocenę rozwoju systemów kierowania ogniem artylerii w Siłach Zbrojnych Rzeczypospolitej Polskiej oraz procesu osiągania interoperacyjności z systemami państw NATO. Analizie poddano ewolucję krajowych rozwiązań technicznych, ze szczególnym uwzględnieniem Zautomatyzowanego Zestawu Kierowania Ogniem TOPAZ oraz jego integracji z programem **Artillery Systems Cooperation Activities (ASCA)**.

W procesie badawczym wykorzystano analizę chronologiczną, umożliwiającą identyfikację kolejnych etapów rozwoju systemów kierowania ogniem – od rozwiązań manualnych, poprzez krajowe kalkulatory artyleryjskie UKART i SKART, aż do pełnej implementacji systemu TOPAZ oraz jego certyfikacji w ramach programu ASCA. Ocenie poddano również wpływ wdrożonych rozwiązań na skrócenie procesu **sensor-to-shooter**, zwiększenie świadomości sytuacyjnej oraz poprawę efektywności dowodzenia i wsparcia ogniowego podczas działań narodowych i koalicyjnych.

Ewolucja systemów kierowania ogniem w Siłach Zbrojnych Rzeczypospolitej Polskiej

Rozwój systemów kierowania ogniem artylerii w Siłach Zbrojnych RP odzwierciedla proces transformacji od klasycznych metod analogowych do nowoczesnych, cyfrowych systemów dowodzenia funkcjonujących w środowisku sieciocentrycznym. Głównym celem tej modernizacji było zwiększenie szybkości realizacji zadań ogniowych, poprawa ich precyzji oraz zapewnienie interoperacyjności z systemami państw Sojuszu Północnoatlantyckiego.

Do początku lat dziewięćdziesiątych proces kierowania ogniem opierał się na ręcznych obliczeniach balistycznych, mapach papierowych oraz przekazywaniu komend drogą głosową za pośrednictwem analogowych środków łączności. Obliczenia wykonywano z wykorzystaniem przyrządów mechanicznych i tabel balistycznych, natomiast dowodzenie pododdziałami artylerii realizowano w sposób scentralizowany. Takie rozwiązania charakteryzowały się dużą pracochłonnością oraz znacznym czasem niezbędnym do przygotowania danych do strzelania, co ograniczało skuteczność działania w dynamicznym środowisku operacyjnym.

Pierwszym etapem cyfryzacji polskiej artylerii było opracowanie na początku lat dziewięćdziesiątych krajowych kalkulatorów artyleryjskich **UKART**

i **SKART** przez Wojskową Akademię Techniczną. Urządzenia te umożliwiły automatyzację podstawowych obliczeń balistycznych, znacząco skracając czas przygotowania danych do prowadzenia ognia. Chociaż ich funkcjonalność była ograniczona w porównaniu ze współczesnymi systemami kierowania ogniem, stanowiły one przełom w procesie cyfryzacji Wojsk Rakietowych i Artylerii oraz stworzyły podstawy do dalszego rozwoju krajowych rozwiązań informatycznych.



Specjalizowany Kalkulator Artyleryjski SKART DANA – polski cyfrowy system kierowania ogniem, opracowany na początku lat 90. XX wieku dla 152 mm armatohaubicy samobieżnej DANA, stanowiący przełom w przejściu od stosowanych wcześniej radzieckich przyrządów ręcznego kierowania ogniem do zautomatyzowanego wykonywania obliczeń balistycznych. Źródło: [wml.wat.edu.pl]

Przełomowym wydarzeniem było rozpoczęcie w 1998 roku wdrażania Zautomatyzowanego Zestawu Kierowania Ogniem **TOPAZ**, opracowanego przez WB Electronics we współpracy z Siłami Zbrojnymi RP. System został początkowo zintegrowany z samobieżnymi haubicami 2S1 Goździk, a po zakończeniu badań kwalifikacyjnych wszedł do wyposażenia Wojska Polskiego w 2001 roku. W kolejnych latach jego funkcjonalność była systematycznie roz-

szerzana poprzez integrację z kolejnymi platformami artyleryjskimi, w tym haubicami DANA, KRAB, K9, moździerzami samobieżnymi RAK oraz wieloprowadnicowymi wyrzutniami rakiet HOMAR.

Chronologia rozwoju systemów kierowania ogniem Sił Zbrojnych RP przed przystąpieniem do programu ASCA.

Data	Opis	Uwagi
1980-1990	Ręczne wyznaczanie danych do strzelania, wykorzystanie kalkulatorów artyleryjskich, przekazywanie komend drogą głosową, sygnalizacja chorągiewkami oraz analogowe środki łączności.	
1992	Opracowanie kalkulatorów artyleryjskich UKART/SKART.	**Koncepcja:** rozpoczęcie cyfryzacji procesu kierowania ogniem oraz integracji systemu TOPAZ na poziomie batalionu.
1998	Wdrożenie systemu AFCS TOPAZ dla 122 mm haubicy samobieżnej 2S1 **GOŹDZIK**.	
2007	Integracja systemu AFCS TOPAZ z 152 mm armatohaubicą samobieżną **DANA**.	
2010	Integracja radaru rozpoznania artyleryjskiego **LIWIEC** z systemem AFCS TOPAZ.	**Koncepcja:** systematyczny rozwój funkcjonalności TOPAZ oraz integracja z nowoczesnymi systemami uzbrojenia i rozpoznania.
2011	Określenie wymagań dla systemu kierowania ogniem na szczeblu pułku i brygady artylerii.	
2011	Rozszerzenie możliwości systemu TOPAZ o integrację z bezzałogowymi statkami powietrznymi (UAV).	
2011	Rozszerzenie interoperacyjności z systemami wspomagania dowodzenia (C2), które w okresie opracowywania TOPAZ nie były jeszcze wdrożone do eksploatacji.	

2014	Integracja systemu AFCS TOPAZ z batalionowym modułem ogniowym **REGINA**.	
2016	Integracja systemu AFCS TOPAZ z kompanijnym modułem ogniowym **RAK**	
2016	Wprowadzenie wymagań dotyczących integracji oraz automatycznej wymiany danych pomiędzy batalionowymi modułami systemu TOPAZ.	
2018	Określenie wymagań interoperacyjności systemu AFCS TOPAZ z sojuszniczymi systemami kierowania ogniem za pośrednictwem interfejsu **ASCA**.	

Proces rozwoju TOPAZ obejmował również integrację z nowoczesnymi systemami rozpoznania. Szczególne znaczenie miało włączenie radaru rozpoznania artyleryjskiego **LIWIEC**, bezzałogowych statków powietrznych oraz cyfrowych systemów łączności, umożliwiających automatyczne pozyskiwanie i przekazywanie danych o celach. Dzięki temu możliwe stało się stworzenie jednolitego środowiska informacyjnego obejmującego sensory, stanowiska dowodzenia oraz środki ogniowe.

Kolejne etapy modernizacji koncentrowały się na rozszerzaniu funkcjonalności systemu z poziomu pojedynczego dywizjonu do poziomu pułku i brygady artylerii. Wprowadzono możliwość wymiany danych pomiędzy modułami TOPAZ, integrację z systemami wspomagania dowodzenia oraz automatyzację planowania i koordynacji wsparcia ogniowego. Rozwiązania te znacząco zwiększyły świadomość sytuacyjną dowódców, skróciły czas podejmowania decyzji oraz poprawiły skuteczność realizacji zadań ogniowych.



System kierowania ogniem artylerii TOPAZ – polska, sieciocentryczna architektura cyfrowego systemu kierowania ogniem.
Źródło: [2025Dryblak], s. 146.

Obecnie TOPAZ stanowi kompleksowy system C4ISR przeznaczony do planowania, dowodzenia i kierowania ogniem artylerii. Integruje środki rozpoznania, systemy bezzałogowe, radary, efektory oraz cyfrowe systemy łączności w jednolitą architekturę sieciocentryczną. Automatyzacja procesów obliczeniowych oraz wymiany danych umożliwia znaczące skrócenie czasu realizacji procesu **sensor-to-shooter**, zwiększenie precyzji rażenia oraz efektywne wykorzystanie dostępnych środków ogniowych podczas działań narodowych i koalicyjnych.

Program interoperacyjności Artillery Systems Cooperation Activities (ASCA)

Rosnące znaczenie operacji wielonarodowych oraz konieczność prowadzenia wspólnego wsparcia ogniowego doprowadziły do opracowania programu **Artillery Systems Cooperation Activities (ASCA)**, którego celem jest zapewnienie interoperacyjności narodowych systemów kierowania ogniem artylerii. Inicjatywa została zapoczątkowana na początku lat dziewięćdziesiątych przez Niemcy, Stany Zjednoczone oraz Wielką Brytanię, a jej głównym założeniem było opracowanie wspólnego interfejsu umożliwiającego automatyczną wymianę danych pomiędzy systemami różnych państw.

Podstawę funkcjonowania programu stanowią porozumienia standaryzacyjne NATO (STANAG), określające jednolite zasady wymiany informacji, planowania wsparcia ogniowego oraz współpracy systemów dowodzenia. Dzięki zastosowaniu wspólnego interfejsu ASCA możliwe jest automatyczne przekazywanie informacji dotyczących celów, realizowanych zadań ogniowych, dostępnych środków ogniowych, planów wsparcia oraz środków koordynacji przestrzeni walki.

Program ASCA zakłada stopniowy proces osiągania interoperacyjności przez państwa uczestniczące. Obejmuje on wdrożenie odpowiednich standardów technicznych, przeprowadzenie testów interoperacyjności oraz potwierdzenie zdolności do prowadzenia wielonarodowego wsparcia ogniowego. Państwa uczestniczące uzyskują możliwość współdziałania niezależnie od wykorzystywanych krajowych systemów kierowania ogniem, co pozwala dowódcom wykorzystywać najbardziej odpowiednie środki ogniowe bez względu na ich przynależność narodową.

Istotnym elementem programu jest również rozwój zdolności do prowadzenia operacji wielodomenowych. W kolejnych etapach planowane jest rozszerzenie wymiany danych o współpracę z lotnictwem, komponentem morskim oraz innymi systemami wsparcia ogniowego, tworząc jednolite środowisko dowodzenia i kierowania ogniem w ramach struktur NATO.

Przystąpienie Polski do programu ASCA oraz wdrożenie systemu AFCS TOPAZ

Proces integracji Polski z programem **Artillery Systems Cooperation Activities (ASCA)** stanowił jeden z najważniejszych etapów modernizacji krajowych systemów kierowania ogniem artylerii oraz dostosowania ich do wymagań interoperacyjności NATO. Formalne działania rozpoczęto w 2018 roku, kiedy Polska zgłosiła akces do programu, rozpoczynając jednocześnie proces dostosowania krajowych rozwiązań do obowiązujących standardów technicznych i proceduralnych.

Kluczowym elementem tego procesu było opracowanie interoperacyjności pomiędzy systemem **TOPAZ** oraz **International Field Artillery Tactical Data System – Poland (IFATDS-P)** a systemami kierowania ogniem wykorzystywanymi przez państwa członkowskie ASCA. W latach 2023–2024 przeprowadzono szereg testów interoperacyjności z wykorzystaniem amerykańskiego systemu **AFATDS**, podczas których potwierdzono możliwość automatycznej

wymiany informacji dotyczących celów, realizowanych zadań ogniowych oraz dostępnych środków wsparcia ogniowego.

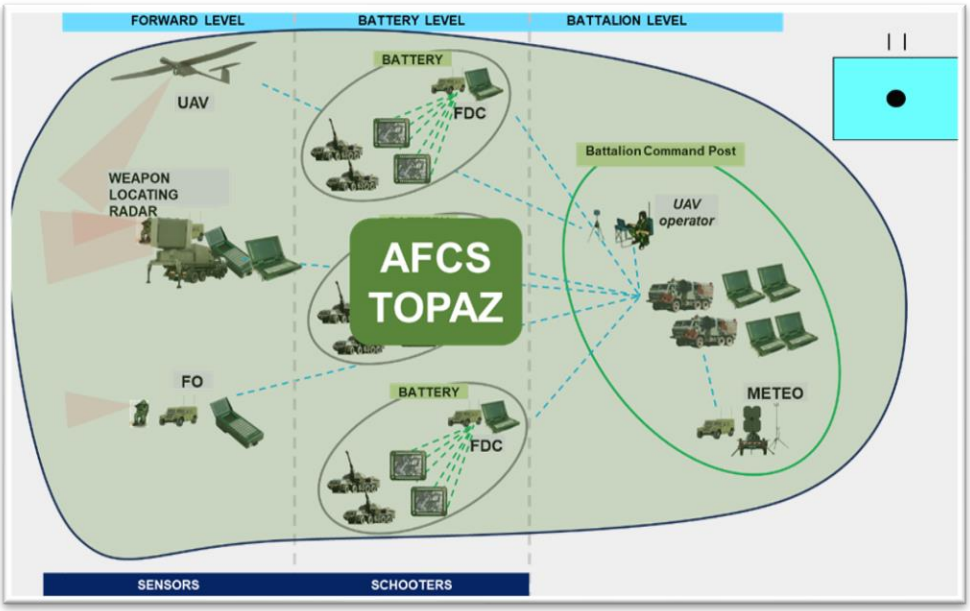
Po pozytywnym zakończeniu procesu certyfikacji Polska uzyskała w marcu 2024 roku status pełnoprawnego członka programu ASCA. Oznaczało to osiągnięcie pełnej interoperacyjności narodowego systemu kierowania ogniem z rozwiązaniami stosowanymi przez pozostałe państwa uczestniczące w programie oraz możliwość prowadzenia wielonarodowego wsparcia ogniowego w ramach struktur NATO.

Podstawowym elementem zapewniającym osiągnięcie tych zdolności jest **Automatyzowany Zestaw Kierowania Ogniem TOPAZ**, który stanowi obecnie podstawowy system dowodzenia i kierowania ogniem Wojsk Rakietowych i Artylerii Sił Zbrojnych RP. System umożliwia cyfrową wymianę danych pomiędzy stanowiskami dowodzenia, środkami rozpoznania oraz efektorami, zapewniając automatyzację procesu planowania, koordynacji i realizacji zadań ogniowych.

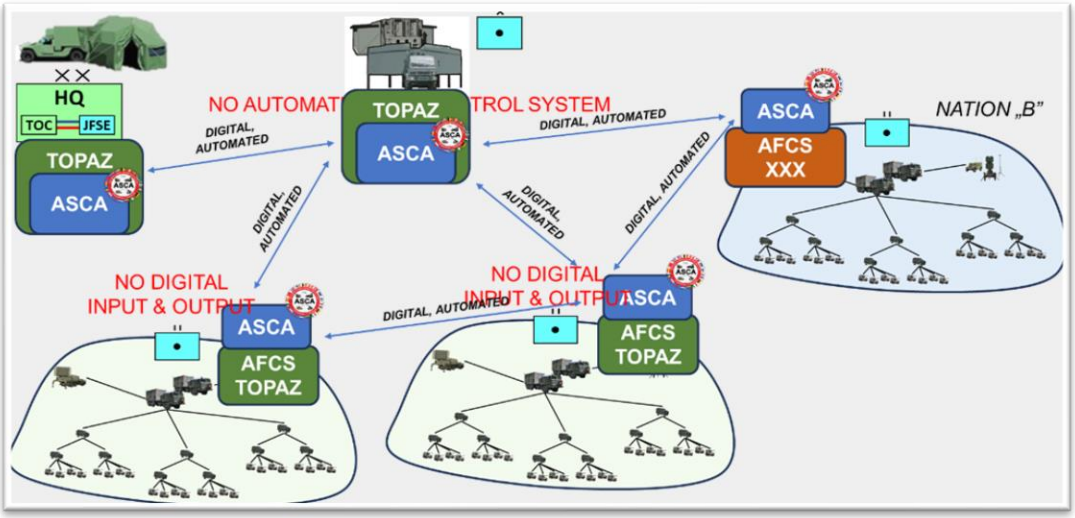
Architektura TOPAZ obejmuje wszystkie szczeble dowodzenia – od pojedynczych środków ogniowych po stanowiska dowodzenia batalionów i brygad artylerii. System integruje informacje pozyskiwane z radarów rozpoznania artyleryjskiego, bezzałogowych statków powietrznych, obserwatorów wysuniętych oraz innych źródeł rozpoznania, automatycznie wyznaczając optymalne środki rażenia i przekazując dane do wykonania zadania ogniowego.

Istotnym elementem funkcjonowania systemu jest możliwość bieżącej analizy sytuacji operacyjnej, monitorowania dostępności amunicji, koordynacji działań wielu pododdziałów oraz automatycznego prowadzenia obliczeń balistycznych. Dzięki temu czas realizacji procesu **sensor-to-shooter** został znacząco skrócony, a skuteczność wsparcia ogniowego uległa istotnemu zwiększeniu.

Integracja z programem ASCA rozszerzyła funkcjonalność TOPAZ poza środowisko krajowe, umożliwiając współpracę z systemami kierowania ogniem państw sojuszniczych. W praktyce oznacza to możliwość automatycznego przydzielania zadań ogniowych najefektywniejszym środkom rażenia, niezależnie od ich przynależności narodowej, co znacząco zwiększa efektywność prowadzenia operacji połączonych i wielonarodowych.



Zautomatyzowany System Kierowania Ogniem **TOPAZ** – *batalionowy moduł* kierowania ogniem



Implementacja interfejsu **ASCA** *w systemie* **AFCS TOPAZ**.

Przeprowadzona analiza potwierdza, że rozwój systemów kierowania ogniem artylerii w Siłach Zbrojnych RP stanowi przykład konsekwentnie realizowanego procesu transformacji technologicznej, prowadzącego od rozwiązań analogowych do w pełni cyfrowej architektury sieciocentrycznej. Osiągnięte zdolności znacząco zwiększyły skuteczność prowadzenia wsparcia ogniowego, poprawiając szybkość podejmowania decyzji, dokładność rażenia oraz poziom świadomości sytuacyjnej na wszystkich szczeblach dowodzenia.

Kluczowym osiągnięciem procesu modernizacji było opracowanie i wdrożenie systemu TOPAZ, który obecnie stanowi centralny element krajowego systemu kierowania ogniem artylerii. System ten zapewnia pełną integrację środków rozpoznania, stanowisk dowodzenia i efektorów, umożliwiając automatyczną realizację procesu planowania oraz kierowania ogniem zgodnie z wymaganiami współczesnego pola walki.

Uzyskanie przez Polskę pełnego członkostwa w programie ASCA stanowiło potwierdzenie osiągnięcia interoperacyjności z systemami kierowania ogniem państw NATO. Integracja ta umożliwia prowadzenie wspólnych działań ogniowych, automatyczną wymianę informacji oraz wykorzystanie narodowych systemów w ramach wielonarodowych struktur dowodzenia. Osiągnięcie interoperacyjności znacząco zwiększa elastyczność prowadzenia operacji połączonych oraz wzmacnia zdolności odstraszania i obrony kolektywnej Sojuszu. W perspektywie dalszego rozwoju systemów kierowania ogniem konieczne będzie rozszerzanie ich funkcjonalności o rozwiązania wykorzystujące sztuczną inteligencję, automatyczną analizę danych oraz zaawansowane algorytmy wspomagania decyzji. Istotnym kierunkiem pozostaje również dalsza integracja z bezzałogowymi systemami rozpoznawczymi i uderzeniowymi, sensorami wielodomenowymi oraz systemami wsparcia lotniczego i morskiego, zgodnie z koncepcją operacji wielodomenowych (Multi-Domain Operations).

Równocześnie rosnące znaczenie zagrożeń cybernetycznych oraz walki elektronicznej wymaga dalszego zwiększania odporności systemów dowodzenia i kierowania ogniem na zakłócenia oraz próby ingerencji w proces wymiany danych. Zachowanie wysokiego poziomu bezpieczeństwa teleinformatycznego będzie jednym z podstawowych warunków utrzymania skuteczności cyfrowych systemów wsparcia ogniowego w przyszłych konfliktach zbrojnych.

Przeprowadzone badania wskazują, że konsekwentna modernizacja krajowych systemów kierowania ogniem, oparta na krajowych kompetencjach technologicznych oraz zgodności ze standardami NATO, umożliwiła stworzenie nowoczesnego i interoperacyjnego środowiska wsparcia ogniowego. System TOPAZ, wspierany przez rozwiązania ASCA, stanowi obecnie jeden z kluczowych elementów budowy zdolności bojowych Sił Zbrojnych RP oraz ich efektywnego funkcjonowania w ramach operacji sojuszniczych.

Dominika CYBULSKA

BIAŁY WYWIAD (OSINT) JAKO NARZĘDZIE W CYBERPRZESTĘPCZOŚCI I CYBER-BEZPIECZEŃSTWIE

Rozwój technologii informacyjno-komunikacyjnych oraz postępująca cyfryzacja życia społecznego sprawiły, że informacje stały się jednym z najcenniejszych zasobów współczesnego świata. Każdego dnia użytkownicy Internetu publikują ogromne ilości danych dotyczących swojego życia prywatnego i zawodowego, często nie zdając sobie sprawy z konsekwencji wynikających z ich powszechnej dostępności. Dane te pochodzą nie tylko z mediów społecznościowych, lecz także z rejestrów publicznych, stron internetowych przedsiębiorstw, dokumentów udostępnianych online czy baz danych tworzonych przez instytucje państwowe i organizacje komercyjne. Powszechna dostępność informacji stworzyła nowe możliwości zarówno dla specjalistów zajmujących się cyberbezpieczeństwem, jak i dla cyberprzestępców. Jednym z najważniejszych narzędzi wykorzystywanych do pozyskiwania oraz analizy informacji z ogólnodostępnych źródeł jest Open Source Intelligence (OSINT), określany w języku polskim mianem białego wywiadu.

Znaczenie OSINT systematycznie wzrasta wraz z rozwojem Internetu oraz zwiększającą się ilością danych pozostawianych przez użytkowników w przestrzeni cyfrowej. Informacje, które pojedynczo wydają się nieistotne, po odpowiednim zestawieniu mogą stworzyć szczegółowy obraz osoby, przedsiębiorstwa lub instytucji. Z tego względu biały wywiad stanowi obecnie jedno z podstawowych narzędzi wykorzystywanych zarówno podczas analiz bezpieczeństwa, jak i przygotowywania cyberataków. Celem niniejszego artykułu jest przedstawienie istoty OSINT oraz omówienie jego znaczenia w kontekście współczesnej cyberprzestępczości i cyberbezpieczeństwa.

Istota białego wywiadu

Pojęcie Open Source Intelligence odnosi się do procesu systematycznego pozyskiwania, selekcjonowania, weryfikowania oraz analizowania informacji pochodzących z publicznie dostępnych źródeł. W odróżnieniu od działań polegających na nieuprawnionym dostępie do systemów teleinformatycznych OSINT opiera się wyłącznie na legalnie dostępnych danych, których pozyska-

nie nie wymaga przełamywania zabezpieczeń ani stosowania metod charakterystycznych dla cyberprzestępczości. O wartości białego wywiadu nie decyduje jednak samo odnalezienie informacji, lecz umiejętność ich odpowiedniego zestawienia i interpretacji. W praktyce nawet pozornie niepowiązane dane mogą po przeprowadzeniu analizy ujawnić informacje o strukturze organizacyjnej przedsiębiorstwa, wykorzystywanych technologiach, relacjach biznesowych czy codziennych aktywnościach określonych osób.

Źródła wykorzystywane podczas analiz OSINT są niezwykle zróżnicowane. Obejmują one między innymi media społecznościowe, strony internetowe przedsiębiorstw, publiczne rejestry państwowe, wyszukiwarki internetowe, fora dyskusyjne, dokumenty zawierające metadane, informacje o domenach internetowych, publicznie dostępne bazy wycieków danych oraz repozytoria kodu źródłowego. Rozwój technologii cyfrowych sprawił, że liczba dostępnych źródeł stale rośnie, co z jednej strony zwiększa możliwości analityczne, z drugiej natomiast znacząco utrudnia selekcję informacji oraz ocenę ich wiarygodności.

OSINT jako narzędzie cyberprzestępczości

We współczesnej cyberprzestępczości etap rozpoznania celu odgrywa kluczową rolę w przygotowaniu skutecznego ataku. Zanim cyberprzestępcy podejmą próbę przełamania zabezpieczeń technicznych, dążą do zgromadzenia możliwie największej ilości informacji dotyczących potencjalnej ofiary. W tym celu wykorzystują właśnie techniki OSINT, które pozwalają na poznanie struktury organizacyjnej przedsiębiorstwa, danych kontaktowych pracowników, wykorzystywanego oprogramowania, partnerów biznesowych czy informacji ujawnionych podczas wcześniejszych incydentów bezpieczeństwa.

Pozyskane informacje są następnie wykorzystywane do przygotowania ataków socjotechnicznych, których skuteczność zależy przede wszystkim od wiarygodności przekazu. Szczególnym zagrożeniem są ataki typu spear phishing, polegające na wysyłaniu starannie przygotowanych wiadomości elektronicznych do konkretnych osób. Przestępca, dysponując wiedzą na temat stanowiska pracownika, realizowanych projektów czy relacji służbowych, jest w stanie stworzyć wiadomość niemal nieodróżnialną od autentycznej korespondencji. W rezultacie ofiara znacznie częściej otwiera złośliwy załącznik lub korzysta z przesłanego odnośnika, co prowadzi do przejęcia danych uwierzytelniających lub zainfekowania systemu informatycznego.

Warto zauważyć, że skuteczność tego rodzaju działań wynika przede wszystkim z wykorzystania informacji dobrowolnie udostępnionych przez użytkowników. Publikowanie zdjęć z miejsca pracy, informacji o pełnionych funkcjach czy danych kontaktowych może wydawać się niegroźne, jednak w połączeniu z innymi publicznie dostępnymi informacjami tworzy wartościowy materiał analityczny dla osób planujących cyberatak.

Przykład wykorzystania OSINT w ataku typu spear phishing

Jednym z najbardziej charakterystycznych przykładów wykorzystania metod OSINT w cyberprzestępczości są ataki typu spear phishing, których skuteczność opiera się na wcześniejszym rozpoznaniu ofiary. Cyberprzestępcy często rozpoczynają działania od analizy publicznie dostępnych informacji zamieszczonych w serwisach społecznościowych oraz na stronach internetowych przedsiębiorstw. Na podstawie takich danych możliwe jest ustalenie struktury organizacyjnej firmy, zakresu obowiązków poszczególnych pracowników, wykorzystywanych technologii, a także relacji służbowych pomiędzy zatrudnionymi osobami.

Przykładowo, pracownik działu finansowego publikuje w serwisie LinkedIn informację o rozpoczęciu pracy w nowej organizacji oraz uczestnictwie w projekcie związanym z wdrożeniem nowego systemu finansowo-księgowego. Równocześnie na stronie internetowej przedsiębiorstwa pojawia się komunikat dotyczący współpracy z nowym dostawcą usług informatycznych. Dla osoby postronnej informacje te mogą wydawać się nieistotne, jednak po ich zestawieniu tworzą spójny obraz działalności organizacji.

Cyberprzestępca, wykorzystując zgromadzone dane, przygotowuje wiadomość elektroniczną podszywającą się pod przedstawiciela firmy wdrażającej nowe oprogramowanie. W treści wiadomości odwołuje się do rzeczywiście realizowanego projektu oraz używa nazwisk pracowników odpowiedzialnych za jego koordynację. Wiadomość zawiera odnośnik prowadzący do fałszywej strony logowania lub złośliwy załącznik. Ze względu na zgodność treści z aktualną sytuacją przedsiębiorstwa prawdopodobieństwo, że odbiorca uzna wiadomość za autentyczną, znacząco wzrasta.

Przedstawiony przykład pokazuje, że skuteczność ataku nie wynika z przełamania zabezpieczeń technicznych, lecz z umiejętnego wykorzystania informacji dobrowolnie udostępnionych przez użytkowników. Właśnie dlatego

ograniczenie ilości publicznie dostępnych danych oraz prowadzenie regularnych analiz OSINT stanowią istotny element strategii cyberbezpieczeństwa współczesnych organizacji.

Znaczenie OSINT w cyberbezpieczeństwie

Paradoksalnie te same metody wykorzystywane przez cyberprzestępców stanowią jedno z podstawowych narzędzi specjalistów odpowiedzialnych za bezpieczeństwo informacji. Organizacje coraz częściej prowadzą regularne analizy OSINT w celu identyfikacji własnych podatności wynikających z nadmiernego ujawniania informacji w Internecie. Pozwala to na wykrywanie wycieków danych, monitorowanie pojawiania się firmowych adresów poczty elektronicznej w publicznych bazach, identyfikowanie fałszywych stron internetowych podszywających się pod przedsiębiorstwo oraz ocenę poziomu ekspozycji organizacji na potencjalne zagrożenia.

Biały wywiad znajduje również zastosowanie podczas testów penetracyjnych oraz analiz Threat Intelligence, których celem jest identyfikacja nowych zagrożeń i monitorowanie aktywności grup cyberprzestępczych. Coraz częściej informacje pozyskane metodami OSINT integrowane są z nowoczesnymi systemami monitorowania bezpieczeństwa, umożliwiając szybsze wykrywanie incydentów oraz skuteczniejsze reagowanie na pojawiające się zagrożenia. Można zatem stwierdzić, że skuteczna ochrona organizacji wymaga obecnie spojrzenia na bezpieczeństwo z perspektywy potencjalnego napastnika i przewidywania sposobów wykorzystania publicznie dostępnych informacji.

Znaczenie białego wywiadu w obszarze cyberbezpieczeństwa systematycznie wzrasta wraz z rozwojem społeczeństwa informacyjnego. Powszechna dostępność danych sprawia, że informacje publikowane w Internecie stają się cennym zasobem wykorzystywanym zarówno do ochrony systemów teleinformatycznych, jak i do przygotowywania cyberataków. OSINT jest przykładem narzędzia, którego wartość zależy przede wszystkim od celu jego wykorzystania. Dla specjalistów ds. cyberbezpieczeństwa stanowi skuteczną metodę identyfikowania zagrożeń, monitorowania wycieków danych oraz wzmacniania odporności organizacji na ataki. Dla cyberprzestępców jest natomiast źródłem informacji umożliwiającym prowadzenie skutecznych działań socjotechnicznych i zwiększanie efektywności prowadzonych kampanii.

Współczesne bezpieczeństwo informacji nie może ograniczać się wyłącznie do stosowania zaawansowanych zabezpieczeń technicznych. Równie

istotne staje się świadome zarządzanie informacjami udostępnianymi w przestrzeni cyfrowej oraz budowanie świadomości użytkowników dotyczącej konsekwencji pozostawiania cyfrowych śladów. W świecie, w którym informacje są jednym z najcenniejszych zasobów, umiejętność prowadzenia analiz OSINT staje się nieodzownym elementem skutecznej ochrony przed zagrożeniami cyberprzestrzeni.

Daniel KONDYRA, Mateusz POŁONCZYK

BMS LEGION - POLSKI SYSTEM ZARZĄDZANIA POLEM WALKI NOWEJ GENERACJI



BMS LEGION to system wspomagania dowodzenia, którego zadaniem jest budowanie aktualnej świadomości sytuacyjnej oraz usprawnienie obiegu informacji na szczeblu batalionu i niższym. System rozwijany jest przez Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni, a jego nowoczesna architektura daje możliwość do dalszego rozwijania zgodnie z potrzebami Sił Zbrojnych RP.

Geneza systemu

BMS LEGION wywodzi się z wcześniejszego projektu funkcjonującego pod nazwą System Informatyczny Monitorowania Geograficznego Położenia Obiektów GPS (SI MGPO GPS). Prace nad rozwiązaniami służącymi do monitorowania położenia wojsk z wykorzystaniem środków łączności rozpoczęły się około 2010 roku. W kolejnych latach system intensywnie rozwijano w kierunku automatycznej transmisji danych o położeniu wojsk własnych w środowisku radiowym.

Lata 2017–2020 były okresem przygotowania rozwiązań prototypowych dla kluczowych platform bojowych, takich jak czołgi T-72 M1R oraz Kołowe

Transportery Opancerzone Rosomak wraz z przeprowadzeniem rygorystycznych testów bezpieczeństwa. W latach 2021–2022 przeprowadzono proces wprowadzenia systemu do Sił Zbrojnych RP. Jego interoperacyjność potwierdzono między innymi podczas międzynarodowych ćwiczeń NATO CWIX, realizując udaną integrację z systemem artyleryjskim TOPAZ, systemem poziomu operacyjnego HMS JAŚMIN oraz rozwiązaniami klasy DSS (Dismounted Soldier System) takimi jak TAK (Tactical Assault Kit) i WinTAK/ATAK.

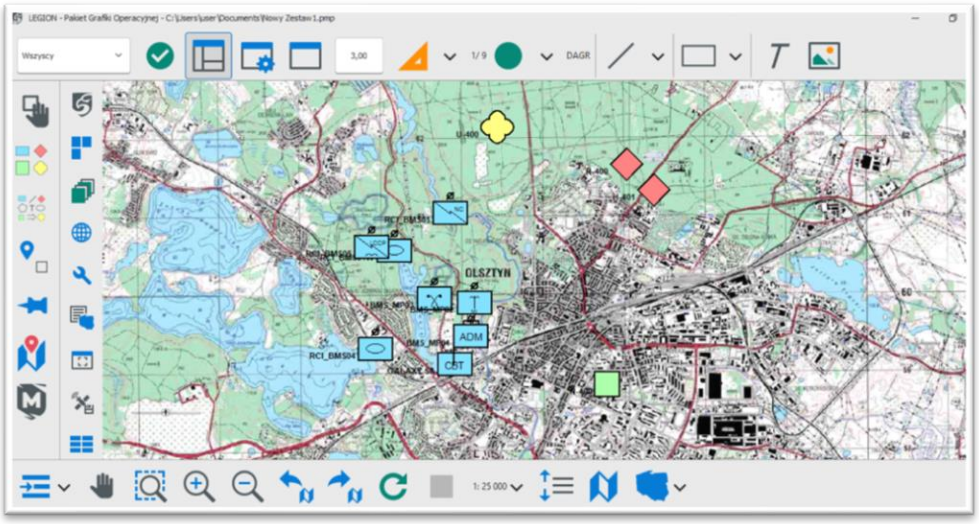
Przeznaczenie i zastosowanie

System został zaprojektowany jako narzędzie, które realnie zmienia sposób prowadzenia działań na poziomie batalionu i niższych szczebli dowodzenia. Jego podstawowym zadaniem nie jest jedynie wyświetlanie informacji na mapie, lecz stworzenie spójnego, cyfrowego środowiska zarządzania walką. W środowisku tym, dowódca otrzymuje możliwie pełny, aktualny i wiarygodny obraz sytuacji taktycznej. LEGION wspiera proces podejmowania decyzji w sposób ciągły: od fazy przygotowania działania, przez jego dynamiczne prowadzenie, aż po analizę skutków i odtwarzanie zdolności bojowej.

W praktyce oznacza to, że BMS LEGION pełni rolę cyfrowego pomostu między pojedynczym żołnierzem, pojazdem, stanowiskiem dowodzenia i wyższymi szczeblami kierowania. Dzięki pełnej automatyzacji obiegu informacji ekstremalnie zmniejsza się czas potrzebny na meldowanie, scalanie danych i ich interpretację, przy jednoczesnym zwiększeniu precyzji przekazu. System umożliwia precyzyjne śledzenie położenia wojsk własnych (BFT – *Blue Force Tracking*), obserwację obiektów istotnych operacyjnie oraz błyskawiczne przekazywanie meldunków, alarmów i danych o zagrożeniach, co bezpośrednio wzmacnia świadomość sytuacyjną całego pododdziału.

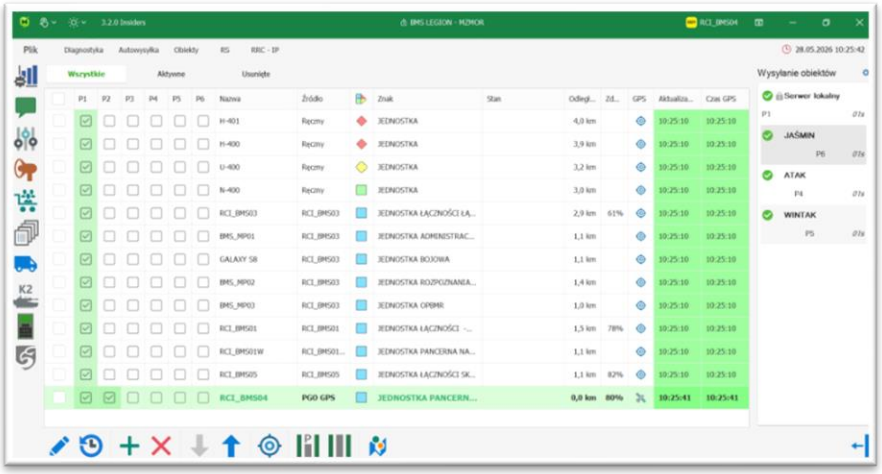
Możliwości systemu

Największą zaletą BMS LEGION jest to, że nie tylko gromadzi informacje, ale przede wszystkim nadaje im bezpośrednią wartość operacyjną. Dowódca nie otrzymuje już pojedynczych, rozproszonych meldunków, lecz uporządkowany obraz pola walki. Jest on analizowany w czasie rzeczywistym dzięki zaawansowanemu modułowi zobrazowania, (bazującym na Pakiecie Grafiki Operacyjnej) opartemu na pracy z mapą cyfrową.



Rysunek przedstawiający moduł zobrazowania BMS LEGION

Poza samym zobrazowaniem przestrzennym system daje możliwość stałego pozyskiwania i zarządzania informacjami o wojskach własnych, przeciwnika oraz o obiektach neutralnych, co realizowane jest za pośrednictwem dedykowanego modułu świadomości sytuacyjnej. W warunkach dynamicznych działań taktycznych taka przewaga oznacza większą szybkość reakcji, lepszą koordynację pododdziałów i bardziej świadome wykorzystywanie własnych zasobów.



Rysunek przedstawiający moduł, w którym zbierane są informacje o wszystkich obiektach odebranych przez system BMS Legion z sieci.

System oferuje również intuicyjny moduł komunikacji do bezpiecznej wymiany wiadomości tekstowych, plików i meldunków w ramach czatu taktycznego, a także alarmów i ostrzeżeń. Istotnym elementem architektury jest moduł logistyczny, który umożliwia precyzyjne zarządzanie zasobami materiałowymi i

stałe monitorowanie statusu podwładnych. Dowodzi to, że LEGION nie jest wyłącznie mapą taktyczną, lecz wszechstronnym narzędziem dowodzenia.

Dzięki wymienionym funkcjom BMS LEGION działa jak efektywny „wzmacniacz dowodzenia": zwiększa tempo obiegu informacji, minimalizuje ryzyko błędów wynikających z opóźnień lub niepełnych danych, a jednocześnie pozwala lepiej kontrolować sytuację na niższych szczeblach. To właśnie na poziomie batalionu i kompanii mają miejsce najbardziej intensywne interakcje taktyczne, dlatego obecność takiego narzędzia ma bezpośredni wpływ na skuteczność całej struktury bojowej.

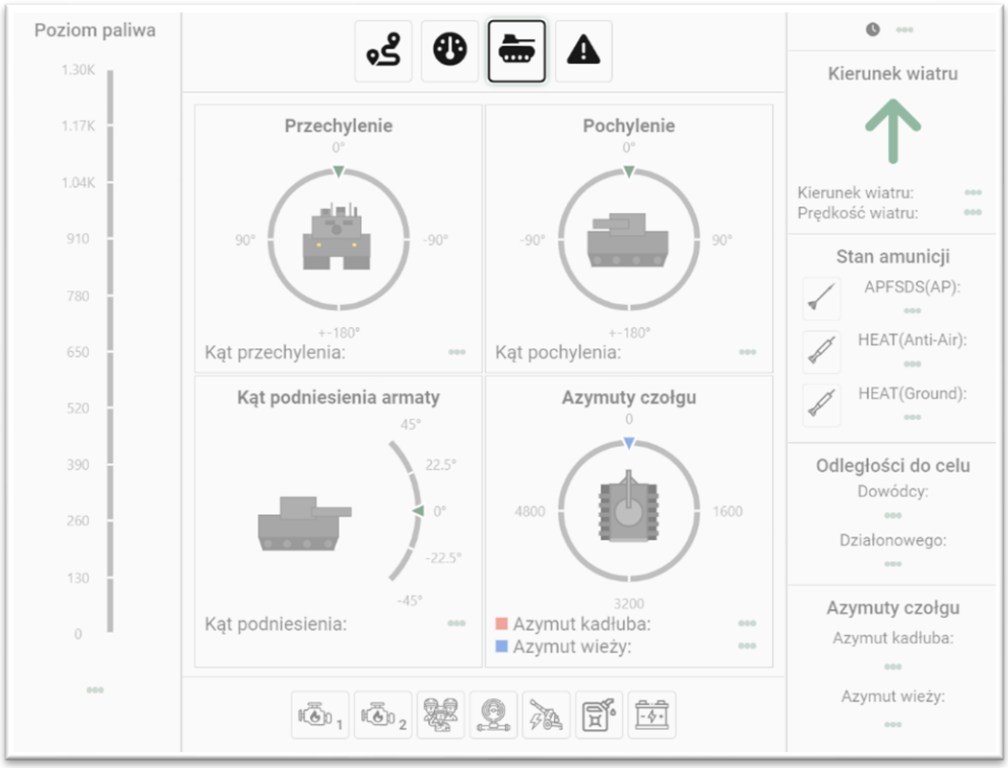
Interoperacyjność z innymi systemami

Jedną z najważniejszych cech BMS LEGION jest jego zdolność do współpracy z systemami zewnętrznymi. System jest w pełni zgodny ze standardami NATO, takimi jak STANAG 5527 NFFI, ADatP-3, NVG oraz *Cursor on Target* (CoT), co zwiększa możliwości wymiany danych i wspólnego działania w środowisku wielosystemowym oraz koalicyjnym.

Szczególnie ważna jest sprawdzona w praktyce integracja z systemami HMS JAŚMIN, TOPAZ, NCOP, IGeoSIT oraz z rozwiązaniami TAK (ATAK i WinTAK). Ma to kluczowe znaczenie, ponieważ system TAK jest środowiskiem aplikacji mapowych i współdzielenia informacji rozwijanym jako otwarta architektura z szerokimi możliwościami rozszerzeń, dostępnym na wielu platformach (Android, Windows, iOS). W tym kontekście połączenie BMS LEGION z rozwiązaniami klasy DSS stanowi milowy krok w stronę pełnej wymiany danych taktycznych i budowania wspólnej świadomości sytuacyjnej na różnych szczeblach działania.

Integracja z platformami i środkami łączności

BMS LEGION został wszechstronnie przygotowany do współpracy z wieloma typami radiostacji, w tym z zaawansowanymi urządzeniami firm L3Harris oraz Radmor. Co istotne, system umożliwia pełne sterowanie wymienionymi urządzeniami, co znacząco poprawia bezpieczeństwo obsługi i ułatwia działanie w wymagających warunkach bojowych.



Rysunek przedstawiający panel K2 w BMS Legion umożliwiający odczyt z szyny danych pojazdu K2 GF

Warto podkreślić również głęboką integrację BMS LEGION z nowoczesnymi platformami bojowymi, ze szczególnym uwzględnieniem czołgów K2 GF. W tym przypadku bezpośrednie wpięcie w szynę danych pojazdu pozwala na automatyczny odczyt kluczowych parametrów – informacji o celach, zagrożeniach, poziomach paliwa czy stanie amunicji. Przekłada się to na błyskawiczny przepływ danych w sieci oraz odciąża załogę od części dotychczasowych czynności raportowych.

Praktyczna implementacja tak zaawansowanych algorytmów integracji sygnałów z szyny danych pojazdu bojowego wymaga jednak stałego, eksperckiego nadzoru i wsparcia na poziomie operacyjnym. To właśnie konieczność płynnego przejścia od zaawansowanej technologii do jej efektywnego wykorzystania w linii dała impuls do zmian organizacyjnych w strukturach Sił Zbrojnych RP.



Osiągnięcia i kluczowe obszary działalności Sekcji Wsparcia BMS w Regionalnym Centrum Informatyki Olsztyn

Dynamiczny rozwój systemu BMS LEGION oraz sukcesywny wzrost liczby jego użytkowników naturalnie wygenerowały potrzebę powołania wyspecjalizowanego zespołu odpowiedzialnego za jego kompleksowe wsparcie. Odpowiedzią na to wyzwanie było utworzenie w **Regionalnym Centrum Informatyki Olsztyn Sekcji Wsparcia BMS** – pierwszej i obecnie jedynej takiej komórki w strukturach Sił Zbrojnych RP.



Zdj. przedstawiające salę laboratoryjną Sekcji Wsparcia BMS w RCI Olsztyn.

W skład sekcji wchodzą specjaliści, którzy wiedzę z zakresu instalacji, konfiguracji i obsługi systemu BMS LEGION łączą z szerokimi kompetencjami teleinformatycznymi oraz znajomością realiów systemów łączności Wojska Polskiego. Dotychczasowa, intensywna działalność sekcji koncentruje się wokół kilku kluczowych filarów, w których zespół osiągnął mierzalne sukcesy.

Działalność szkoleniowa i budowanie samodzielności jednostek

Zespół prowadzi intensywne warsztaty zarówno w nowoczesnym środowisku laboratoryjnym BMS w RCI Olsztyn, jak i bezpośrednio w jednostkach wojskowych na docelowym sprzęcie z zainstalowanym systemem na terenie całego kraju.

- **Skala działań:** W cyklu zajęć warsztatowych przeszkolono już grupy żołnierzy (administratorów, użytkowników) odpowiedzialnych za bezpośrednią obsługę systemu.
- **Zakres programowy:** Warsztaty obejmują pełen cykl życia systemu – od instalacji i konfiguracji, przez bieżącą eksploatację i zaawansowane diagnozowanie problemów (troubleshooting), aż po taktyczne wykorzystanie oprogramowania.
- **Efekt:** Dzięki praktycznej formule zajęć przeszkoleni administratorzy lokalni zyskali pełną autonomię w zakresie utrzymania systemu w swoich macierzystych jednostkach.

Synergia z twórcami systemu i rozwój oprogramowania

Sekcja Wsparcia BMS RCI Olsztyn wypracowała model bliskiej i efektywnej współpracy z zespołem programistów i deweloperów z DKWOC odpowiedzialnych za rozwój oprogramowania. Działając na pierwszej linii, administratorzy sekcji stali się kluczowym partnerem dla twórców systemu, tworząc z nimi zgrany ekosystem. Poprzez aktywny udział w testach nowych wersji, regularne przekazywanie zgłoszeń o błędach oraz rzetelne zbieranie wniosków i propozycji od użytkowników końcowych, sekcja dostarcza wartościowy wkład w rozwój systemu. Ten stały przepływ informacji zwrotnej pozwala twórcom na bieżąco optymalizować i doskonalić system BMS LEGION, dostosowując go do realnych wymogów współczesnego pola walki.

Zabezpieczenie wdrożeń i odbiorów technicznych sprzętu bojowego

Ważnym osiągnięciem sekcji jest jej stały, merytoryczny udział w pracach zdawczo-odbiorczych nowoczesnych platform bojowych wyposażonych w system LEGION, w tym czołgów K2 Black Panther. W tym obszarze spektrum działań objęło m.in.:

- Udział w komisjach odbiorczych czołgów K2 GF w 16 Dywizji Zmechanizowanej.
- Weryfikację poprawności konfiguracji urządzeń, stabilności integracji z systemami pokładowymi pojazdów oraz poprawnego współdziałania z radiostacjami wojskowymi.

Biorąc pod uwagę dynamikę kolejnych dostaw nowoczesnego sprzętu dla SZ RP, rola sekcji w tym procesie pozostaje kluczowa.



Zdj. przedstawiające udział członków Sekcji Wsparcia BMS w komisji odbiorczej K2 GF..

Wsparcie ćwiczeń poligonowych i testy interoperacyjności

Egzaminem z osiągniętych kompetencji zespołu było wsparcie w zabezpieczeniu teleinformatycznym kluczowych przedsięwzięć szkoleniowych i ćwiczeń taktycznych organizowanych przez Dowództwo Generalne RSZ oraz poszczególne dywizje. Administratorzy sekcji z sukcesem wspierali realizację

m.in. takich ćwiczeń jak: FEX-24, BLUSZCZ-24, CYFROW@ BRYGADA, CYFROWY LEGIONISTA oraz CYFROWY DZIK.

Podczas realizacji ćwiczeń wysiłki sekcji skupiały się wokół dwóch obszarów:

1. **Asysta techniczna (Helpdesk):** Zapewnienie ciągłości działania systemu w warunkach poligonowych, co pozwoliło szkolonym żołnierzom skupić się wyłącznie na zadaniach taktycznych.
2. **Rozwój interoperacyjności:** Udane testowanie innowacyjnych konfiguracji oraz integracja wymiany danych pomiędzy systemami **BMS LEGION, HMS JAŚMIN, TOPAZ i DSI TAK**, ze szczególnym uwzględnieniem współpracy z **bezzałogowymi systemami rozpoznawczymi (dronami)**. Jako media transmisyjne wykorzystano zarówno klasyczne polowe środki łączności, jak i nowoczesną łączność satelitarną, w tym systemy Starlink.

Promocja nowoczesnych technologii w SZ RP



Zdj. przedstawiające prezentację BMS Legion na Wojskowych Targach Służby i Pracy.

Sekcja aktywnie angażuje się w budowanie świadomości technologicznej w armii oraz poza nią. Potencjał i praktyczne możliwości systemu BMS LEGION były z powodzeniem prezentowane przez członków zespołu podczas prestiżowych wydarzeń, takich jak:

- Odprawy Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni (DKWOC),

- Międzynarodowe forum **CYBERSEC EXPO & FORUM**,
- Międzynarodowy Kongres Cyberbezpieczeństwa **INSECON**
- Wojskowe Targi Służby i Pracy oraz kluczowe wydarzenia wizerunkowo-promocyjne Sił Zbrojnych RP.

Podsumowanie i wnioski

Doświadczenia zebrane od momentu sformowania komórki jednoznacznie dowodzą, że skuteczne wdrażanie systemów klasy BMS wymaga silnego, scentralizowanego wsparcia eksperckiego. Powołanie Sekcji Wsparcia BMS w strukturach RCI Olsztyn okazało się kamieniem milowym na drodze do cyfryzacji współczesnego pola walki. Dotychczasowe sukcesy tej komórki – od wsparcia odbiorów czołgów K2 GF, przez zabezpieczenie kluczowych ćwiczeń, aż po budowanie samodzielności jednostek – jasno wskazują na pilną potrzebę i konieczność utworzenia kolejnych, analogicznych sekcji wsparcia w strukturach Wojska Polskiego w innych Regionalnych Centrach Informatyki.

Przykład Sekcji Wsparcia BMS RCI Olsztyn pokazuje, że za sukcesem nowoczesnych technologii stoi nierozerwalny łańcuch ludzkich kompetencji. To połączenie wysokich kompetencji twórców oprogramowania oraz unikalnej wiedzy, mobilności i ogromnego zaangażowania administratorów sekcji sprawia, że BMS LEGION przestał być jedynie zaawansowanym systemem informatycznym, a stał się realnym, niezawodnym i kluczowym narzędziem wspierania dowodzenia w Siłach Zbrojnych RP.

Suwerenność i bezpieczeństwo

Ważnym atutem BMS LEGION jest jego w pełni narodowy charakter. Oprogramowanie zostało wykonane w całości przez specjalistów z Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni, a kod źródłowy pozostaje wyłączną własnością Sił Zbrojnych RP. Skutecznie ogranicza to ryzyko krytycznego uzależnienia od zewnętrznych dostawców oraz zagranicznych licencji. Takie podejście drastycznie zwiększa kontrolę nad bezpieczeństwem rozwiązania, ale też nad tempem jego rozwoju i elastyczną możliwością dostosowania do konkretnych potrzeb operacyjnych. Na wysoką użyteczność systemu w warunkach bojowych ma również wpływ jego udowodniona zdolność do stabilnej pracy na starszym sprzęcie komputerowym i łączności taktycznej oraz w trudnych warunkach polowej łączności radiowej.

Kierunki rozwoju

BMS LEGION nie jest rozwiązaniem zamkniętym, lecz dynamiczną platformą rozwijaną wraz ze zmieniającymi się potrzebami nowoczesnego pola walki. Jednym z priorytetowych kierunków rozwoju są funkcjonalności oparte na algorytmach sztucznej inteligencji (AI), które mają wspierać zaawansowaną analizę danych taktycznych i maksymalnie przyspieszać proces podejmowania decyzji przez dowódców. Taki kierunek jest w pełni spójny z globalnymi trendami rozwoju systemów wspomagania dowodzenia i automatyzacji wymiany informacji. W praktyce oznacza to, że BMS LEGION będzie stawał się coraz ważniejszym elementem krajowego ekosystemu cyfrowego dowodzenia, łączącego w sobie suwerenność, bezpieczeństwo i pełną interoperacyjność.

Podsumowanie całego projektu

BMS LEGION to sztandarowy przykład nowoczesnego, krajowego systemu zarządzania polem walki, który w sposób spójny łączy funkcje świadomości sytuacyjnej, bezpiecznej komunikacji, cyfrowego zobrazowania oraz pełnej integracji z innymi systemami dowodzenia. Jego fundamentalne znaczenie wynika nie tylko z bieżących, wysokich możliwości operacyjnych, ale również z faktu, że stanowi rozwiązanie rozwijane w Polsce na potrzeby polskich sił zbrojnych, pozostając przy tym w pełni zdolnym do współdziałania w połączonym środowisku NATO. System ten idealnie wpisuje się w strategiczny kierunek rozwoju nowoczesnych sił zbrojnych, w których przewaga informacyjna staje się tak samo ważna, jak przewaga ogniowa. To dojrzałe rozwiązanie, które skutecznie porządkuje chaos współczesnego pola walki, przyspiesza procesy decyzyjne i pomaga dowódcom działać pewniej, szybciej i efektywniej.

G. K.

WOZY DOWODZENIA NA PODWOZIU KTO ROSOMAK ZAWILEC, KROTON I KROTON-2

Współczesne pole walki wymaga szybkiego przepływu informacji, wręcz natychmiastowej wymiany danych, wysokiej mobilności, skutecznego koordynowania działań wojsk operacyjnych oraz ich dowództw, jak również bezpieczeństwa systemów teleinformatycznych. Jednym z kluczowych elementów systemu dowodzenia Sił Zbrojnych RP są specjalistyczne wozy dowodzenia (WD) oparte na podwoziu Kołowego Transportera Opancerzonego (KTO) Rosomak. Konstrukcje te zapewniają mobilne stanowiska dowodzenia zdolne do działania zarówno podczas postoju, jak i w ruchu. Do najważniejszych polskich pojazdów tej klasy należą wozy dowodzenia o kryptonimie Zawilec, Kroton oraz Kroton-2 (Kroton bis). Wszystkie powyższe bazują na platformie Rosomak z napędem w systemie 8×8, lecz różnią się przeznaczeniem, wyposażeniem teleinformatycznym oraz zakresem współpracy z krajowymi i sojuszniczymi systemami dowodzenia. Jednocześnie zapewniają ciągłość dowodzenia jednostkami operacyjnymi w środowisku wielodomenowym.

Podstawą powyższych wariantów wozów dowodzenia omawianych pojazdów jest KTO Rosomak 8×8, będący polską odmianą fińskiego transportera Patria AMV. Platforma ta charakteryzuje się wysoką mobilnością, możliwością pokonywania trudnych warunków terenowych i bojowych oraz znaczną odpornością balistyczną, a jej unifikacja zdecydowanie ułatwia logistykę oraz szkolenie załóg. W przypadku wozów dowodzenia zastosowano podwyższony przedział roboczy umożliwiający instalację dodatkowych urządzeń teleinformatycznych, stanowisk operatorskich i systemów łączności.

Podstawowe dane taktyczno - techniczne

Parametr	Wartość
Układ jezdny	8×8
Długość	ok. 8,4 m
Szerokość	ok. 2,8 m
Wysokość	ok. 2,9 m

Masa bojowa	ok. 22–23 t
Prędkość maksymalna	do 100 km/h
Zasięg operacyjny	500–700 km
Załoga	5–7 osób (zależnie od wersji)

Wóz dowodzenia KROTON

Kroton jest pierwszym seryjnie produkowanym nowoczesnym wozem dowodzenia na podwoziu Rosomaka i stanowił przełom w procesie cyfryzacji stanowisk dowodzenia w SZ RP, a jego celem było zapewnienie mobilnych stanowisk dowodzenia dla jednostek współpracujących z siłami NATO. Program został rozpoczęty w 2018 roku.Jego pierwsze egzemplarze trafiły do jednostek wojskowych odpowiedzialnych za dowodzenie i wsparcie działań wielonarodowych, jak w przypadku Dowództwa Wielonarodowej Dywizji Północny - Wschód (MND-NE), a konkretnie podległego Pułku Wsparcia Dowodzenia (DWDPW).

Najważniejszym elementem WD Kroton jest rozbudowany system teleinformatyczny, który posiada takie możliwości jak:

- planowanie działań bojowych,
- wymiana danych taktycznych,
- prowadzenie wideokonferencji,
- współpraca z systemami NATO (do klauzuli NATO SECRET),
- zarządzanie sieciami łączności.

Pojazd posiada kilka stanowisk operatorskich wyposażonych w komputery wojskowe oraz zestawy środków łączności radiowej i satelitarnej. W jego wnętrzu znajduje się pięć stanowisk pracy dla oficerów sztabowych. Jego uzbrojenie obejmuje tylko broń osobistą załogi oraz wyrzutnię granatów dymnych, z uwagi na ich główną rolę jaką jest zabezpieczenie łączności i pracy sztabu, a nie bezpośrednia walka.



Wóz dowodzenia KROTON-2 (KROTON BIS)

Wóz Dowodzenia Kroton-2, znany również jako Kroton bis, stanowi rozwinięcie wcześniejszej wersji. Modernizacja była odpowiedzią na rosnące wymagania dotyczące bezpieczeństwa teleinformatycznego, interoperacyjności z wojskami sojuszniczymi oraz zwiększenia możliwości przetwarzania informacji. Wozy te zamówiono jako kolejną generację pojazdów przeznaczonych do współpracy w środowisku sojuszniczym NATO, dedykowane do wsparcia procesów dowódczo – sztabowych szczebla batalionu w pododdziałach 18 DZ w Siedlcach, wyposażonej w amerykańskie czołgi M1 Abrams.

W porównaniu z Krotonem zastosowano:

- nowocześniejsze systemy transmisji danych,
- rozbudowane środki kryptograficzne,
- ulepszone systemy łączności satelitarnej,
- większą liczbę interfejsów wymiany danych.

Kroton-2 umożliwia jednoczesne prowadzenie wielu kanałów łączności oraz obsługę informacji niejawnych zgodnie ze standardami NATO oraz zapewnia interoperacyjność z systemami zarządzania polem walki w czołgach Abrams.

Podobnie, jak w przypadku wcześniejszej wersji posiada:

- wyrzutnie granatów dymnych,
- system ostrzegania przed opromieniowaniem laserowym OBRA.



Wóz dowodzenia Zawilec

Zawilec jest najnowszą i najbardziej zaawansowaną odmianą wozu dowodzenia opracowaną dla potrzeb narodowego systemu dowodzenia Sił Zbrojnych RP. W odróżnieniu od Krotona zastosowano przede wszystkim krajowe rozwiązania teleinformatyczne opracowane przez Grupę WB Electronics.

Najważniejsze elementy wyposażenia obejmują:

- wielostanowiskowe systemy teleinformatyczne,
- krajowe systemy przetwarzania danych,
- zaawansowane środki łączności radiowej,
- możliwość integracji z narodowymi i sojuszniczymi systemami dowodzenia,
- nowoczesne serwery i urządzenia sieciowe,
- pełna mobilność stanowiska dowodzenia w warunkach dynamicznie zmieniającej się sytuacji taktycznej.

Pojazd definiowany jest jako „narodowy” wóz dowodzenia szczebla taktycznego przeznaczony do pracy dla organów dowodzenia brygad oraz dywizji Wojska Polskiego. Stanowi mobilny i autonomiczny węzeł teleinformatyczny, który integruje systemy wymiany danych w środowisku wielodome-

nowym, gdzie informacje pochodzą jednocześnie z wojsk lądowych, sił powietrznych, cyberprzestrzeni, systemów bezzałogowych oraz rozpoznania satelitarnego. Zastosowane rozwiązania czynią z Zawilca nowoczesne, mobilne centrum dowodzenia, zdolne do pracy bez konieczności rozwijania rozbudowanej infrastruktury stacjonarnej.

Systemy teleinformatyczne posiadają certyfikację do przetwarzania informacji niejawnych do szczebla TAJNE / NATO SECRET. Celem uzyskania bezpiecznego i elastycznego środowiska pracy operacyjnej w strukturach krajowych i sojuszniczych zapewniono jednoczesna pracę w dwóch odseparowanych domenach informacyjnych. Ich klauzule są definiowane w zależności od potrzeb operacyjnych.

W zakresie uzbrojenia Zawilec został wyposażony w zdalnie sterowane stanowisko uzbrojenia (ZSSU) na bazie karabinu maszynowego kal. 7,62 mm oraz zachował rozwiązania stosowane w rodzinie Rosomak:

- system OBRA,
- wyrzutnia granatów dymnych.

Pod koniec 2025 r. pierwsze Wozy Dowodzenia Zawilec trafiły na wyposażenie 5 Pułku Dowodzenia w podkrakowskiej Rząsce celem zapewnienia dowodzenia dla Dowództwa 2 Korpusu Polskiego stacjonującego w Krakowie.



Aktualnie wozy dowodzenia na platformie Rosomak 8x8 wykorzystywane są oprócz 5pdow również w innych JW jak w przypadku Wielonarodowej Dywizji Północny Wschód w Elblągu, 18 Dywizji Zmechanizowanej w Siedlcach czy 9 batalionie dowodzenia w Olsztynie.

Porównanie wozów dowodzenia

Cecha	Kroton	Kroton-2 (Kroton bis)	Zawilec
Podwozie	Rosomak 8×8	Rosomak 8×8	Rosomak 8×8
System teleinformatyczny	WB Electronics	Harris, Radmor zgodny z NATO	Krajowy system Grupy WB
Szczebel działania	Batalion/Brygada	Batalion/Brygada/NATO	Brygada/Dywizja
Ochrona balistyczna	Rosomak	Rosomak	Rosomak
System OBRA	Tak	Tak	Tak

Wozy dowodzenia Kroton, Kroton-2 i Zawilec stanowią kluczowy element modernizacji systemu dowodzenia SZ RP. Wszystkie powyższe wykorzystują sprawdzoną platformę bojową Rosomak, zapewniając wysoką mobilność i ochronę załogi. Kroton był pierwszym krokiem do stworzenia nowoczesnych mobilnych stanowisk dowodzenia zgodnych ze standardami NATO. Kroton-2 rozwinął te możliwości, zwiększając interoperacyjność i bezpieczeństwo wymiany informacji. Najnowszy Zawilec reprezentuje kierunek budowy narodowego systemu dowodzenia opartego na polskich rozwiązaniach teleinformatycznych, przystosowanego do prowadzenia działań w środowisku wielodomenowym. Dzięki temu Wojsko Polskie zyskuje nowoczesne narzędzia pozwalające skutecznie kierować działaniami bojowymi zarówno samodzielnie, jak i w ramach struktur sojuszniczych NATO.

FIRMY TELEKOMUNIKACYJNE

Grupa WB

PERAD I COMP@N – UKŁAD NERWOWY NOWOCZESNEGO POLA WALKI

Grupa WB

SYSTEM RADIOSTACJI COMP@N-Z DLA SIŁ ZBROJNYCH RP

– System COMP@N-Z

System COMP@N-Z umożliwia wymianę informacji fonicznych (głosowych) oraz transmisję danych cyfrowych klasyfikowanych do klauzuli ZASTRZEŻONE, NATO RESTRICTED, RESTREINT UE/EU RESTRICTED. System zawiera komponenty służące do planowania sieci radiowych (SPSR) oraz generacji/zarządzania/dystrybucji dokumentów kryptograficznymi w całym cyklu życia tych dokumentów (SZGDK). System zawiera wszystkie, kompletne elementy, niezbędne do zapewnienia jego działania w trybie jawnym i niejawnym, spełniające niezbędne wymogi bezpieczeństwa.

W skład systemu COMP@N-Z wchodzi:

a. Rodzina radiostacji:
   - Radiostacja doręczna H09-Z/1;
   - Zestaw przewoźny radiostacji H09-Z/1 (H39-Z/1);
   - Radiostacja plecakowa M09-Z/1;
   - Radiostacja pokładowa V09-Z/1;

b. Elementy planowania, generacji i dystrybucji:
   - System Planowania Sieci Radiowych (SPSR);
   - System Zarządzania i Generacji Dokumentów Kryptograficznych (SZGDK);

– Radiostacja doręczna H09-Z/1

H09-Z/1 to szerokozakresowa, wąskopasmowa radiostacja doręczna wykonana w technologii SDR (Software Defined Radio), a tym samym jest ona w pełni programowalna (jej funkcjonalność jest definiowana przez zaimplementowane w niej oprogramowanie). Radiostacja może być więc udoskonalana i wzbogacana, np. na życzenie klienta/użytkownika o kolejne funkcjonalności, poprzez aktualizację jej oprogramowania, co w połączeniu z bar-

dzo szerokim zakresem częstotliwości pracy daje ogromne możliwości stosowania różnych standardów łączności, ich aktualizacji w zgodzie najnowszą rewizją i przełączania między nimi „w locie” (w trakcie pracy radiostacji).

H09-Z/1 umożliwia przetwarzanie informacji niejawnych klasyfikowanych do klauzuli **ZASTRZEŻONE, NATO Restricted, Restreint UE/EU Restricted**.



Rysunek 1 Radiostacja doręczna H09-Z/1.

1.1.1. Specyfikacja

Ogólna specyfikacja radiostacji:

- pasmo pracy: 30÷520 MHz;
- moc maksymalna 5W, wraz z adapterem i wzmacniaczem tworzy zestaw przewoźny o mocy 50W;
- wbudowany odbiornik GPS;
- wymiary radiostacji doręcznej (bez anteny): 220 x 87 x 48 mm;
- bardzo wysoka czułość odbiornika (zapewnia ponadprzeciętne zasięgi).

Spełnione normy obronne:

- NO-06-A103:2021 dla grupy N.11/N.12 (H39-Z/1, V09-Z/1) i N.14 (H09-Z/1, M09-Z/1)
- NO-06-A200:2012

- NO-58-A213:2015

Podstawowe ukompletowanie zestawu Radiostacji H09-Z/1:

- radiostacja H09-Z/1;
- trzy zasilacze akumulatorowe 3579/3;
- futerał;
- anteny: 4702/1, 4702/2 i 4702/3;
- manipulator 0604/1;
- zestaw nagłowny 01322/1;
- zestawy nagłowne z ochronnikami słuchu innych producentów (opcja);
- urządzenie ładujące jednostanowiskowe 02765/1;
- zasilacz sieciowy 4504/1;
- opakowanie transportowe.

1.1.2. Waveformy

Waveform (WF) – oprogramowanie radiostacji służące takiemu przekształceniu informacji - od jej wejścia do radia po wyjście (w formie sygnału z anteny) – aby, jak najlepiej informację zabezpieczyć i jak najefektywniej przesłać ją w eterze.

Zaletą takiego rozwiązania, jest możliwość opracowania i zastosowania WF-ów dopasowanych do wymaganych przekształceń informacji w zależności od jej rodzaju, zakresu częstotliwości, czy też wymaganej odporności. Możliwe jest więc stosowanie kilku standardów łączności oraz swobodne przełączanie między nimi w zależności od potrzeb misji.

Obecnie radiostacje z rodziny COMP@N-Z obsługują głównie trzy waveformy:

- AM/FM;
- BMS IP;
- W2FH.

1.1.2.1. Waveform AM/FM – stała częstotliwość

Pracujący na stałej częstotliwości Waveform AM/FM jest interoperacyjny z urządzeniami wspierającymi STANAG 4203/4204/4205. Przykładem innych urządzeń pracujących w oparciu o waveform AM/FM są:

- Rodzina radiostacji COMP@N oraz COMP@N-Z produkcji Radmor S.A.;

- Radiostacja 3501 produkcji Radmor S.A. pracująca w trybie A;
- Radiostacja RRC9200 pracująca w trybie FF - HLG i HLC;
- Radiostacja RRC9500 pracująca w trybie FF - HLG i HLC;
- Rodzina radiostacji F@stnet: RRC9210, RRC9310, RRC9211 i RRC9311 pracujących w trybie FF - HLG i HLC;
- Radiostacje lotnicze wspierające STANAG 4204/4205, jak np. Leonardo SDR SRT-800.

Podstawowe cechy waveformu:

- waveform wąskopasmowy;
- modulacja AM lub FM;
- praca na jednej częstotliwości;
- praca w zakresie częstotliwości od 30MHz do 520MHz;
- odstęp międzykanałowy:
  - FM: 25 kHz;
  - AM: 8.33 lub 25 kHz;
- blokada szumów (ton: FM, szum: AM i FM);
- możliwość zaprogramowania do 100 kanałów pracy;
- praca na trzech poziomach mocy;
- praca wyłącznie w trybie jawnym;
- konfiguracja kanałów możliwa zarówno za pomocą aplikacji SPSR jak i lokalnego interfejsu radiostacji.

1.1.2.2. Waveform W2FH

W2FH jest całkowicie opracowanym przez RADMOR, wąskopasmowym waveformem klasy EPM (Electronic Protective Measures) umożliwiającym realizację silnie zabezpieczonej transmisji mowy i danych (chronionych przez zakłóceniem i przejęciem), pracującym w trybie hoppingowym. Umożliwia pracę w trybie jawnym i niejawnym.

Główne cechy:

- waveform wąskopasmowy dla pasma VHF/UHF typu LPI/LPD;
- dedykowany do pracy w zakresie częstotliwości 30MHz – 87,975MHz (możliwość uruchomienia waveformu w pełnym zakresie pracy radiostacji);
- synchronizacja bez potrzeby dostępu do zewnętrznych referencji czasu (np. GNSS),

- pracujący w trybach jawnym albo zastrzeżonym (COMSEC zapewnia moduł kryptograficzny radiostacji);
- wbudowane mechanizmy bezpieczeństwa transmisji - TRANSEC;
- dostęp do medium radiowego w trybie CSMA (Carrier Sense Multiply Access) – waveform nie wymaga rozsyłania danych kontrolnych;
- przy braku potrzeby transmisji danych użytkowych sieć może pozostawać w całkowitej „ciszy radiowej” nawet przez wiele miesięcy zachowując zdolność do synchronizacji;
- odstęp międzykanałowy: 25 kHz;
- konfiguracja parametrów pracy za pomocą aplikacji SPSR;
- rozpraszanie widma - FH (Frequency Hopping).

1.1.2.3. Waveform BMS IP

BMS IP to całkowicie opracowany przez RADMOR, wąskopasmowy waveform typu MANET (Mobile Ad-Hoc Network), czyli samoorganizującej się sieci, umożliwiający jednoczesną transmisję cyfrowej mowy, danych IP lub szeregowych, świadomości sytuacyjnej, pozycji GPS i innych informacji wymaganych w systemach BMS (Battlefield Management System). Waveform pozwala na pracę w trybie jawnym oraz niejawnym.

Podstawowe cechy waveformu:

- waveform wąskopasmowy pracujący w paśmie VHF/UHF;
- do pracy w zakresie częstotliwości 30-87,975 MHz (możliwość uruchomienia waveformu w pełnym zakresie pracy radiostacji);
- praca na jednej częstotliwości lub w trybie hoppingowym;
- odstęp międzykanałowy 50 kHz;
- MANET;
- waveform tworzący sieć zamkniętą, do której dostęp maję jedynie uprzednio zaplanowane radiostacje;
- pracujący w trybach jawnym albo zastrzeżonym (COMSEC zapewnia moduł kryptograficzny radiostacji);
- wbudowane mechanizmy bezpieczeństwa transmisji - TRANSEC;
- wbudowane mechanizmy bezpieczeństwa sieci - NETSEC;
- korespondencja głosowa w trybie rozgłoszeniowym (P2MP) oraz selektywnym (P2P);
- możliwa równoczesna transmisja głosowa P2P, P2MP oraz danych;
- zasięg usługi transmisji mowy do dwóch skoków radiowych;
- zasięg usługi transmisji danych IP do pięciu skoków radiowych;

- wsparcie transmisji danych IP typu unicast i multicast;
- wsparcie dla sieci zewnętrznych IP;
- mechanizmy QoS zwiększające prawdopodobieństwo dostarczania danych IP zoptymalizowane dla wielohopowych transmisji w sieci radiowej (ARQ);
- wiadomości Situation Awareness z towarzyszącą pozycją wprowadzaną automatycznie (GPS) lub manualnie;
- rozgłaszanie informacji wiadomości o Kasowaniu Awaryjnym;
- wymiana wiadomości SMS;
- rozsyłanie wiadomości alarmowych ALERT;
- transmisja danych szeregowych w trybie kolizyjnym lub bezkolizyjnym;
- typ dostępu do medium – TDMA;
- synchronizacja bez dostępu do zewnętrznej referencji czasu (domyślnie) lub z możliwością wykorzystania GPS;
- konfiguracja parametrów pracy za pomocą aplikacji SPSR;

– Zestaw przewoźny radiostacji H09-Z/1 (H39-Z/1)

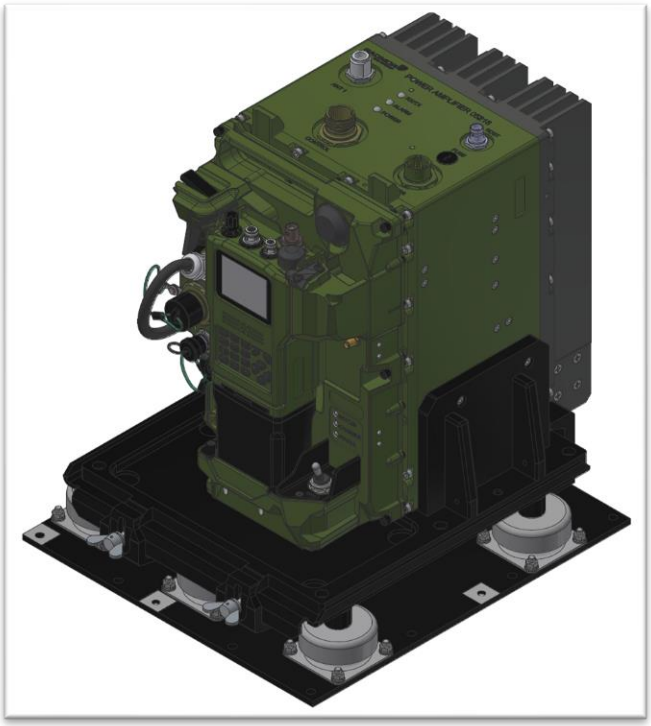
Charakteryzuje się identycznymi parametrami i funkcjonalnościami jak radiostacja doręczna za wyjątkiem zasięgów, które zostały znacząco zwiększone dzięki zastosowaniu dodatkowego stopnia wzmacniacza zewnętrznego oraz anten pojazdowych. Zestaw przeznaczony jest do instalowania w lekkich czołgach, bojowych wozach piechoty, kołowych transporterach opancerzonych i obiektach zbudowanych na ich bazie (zgodnie z NO-06-A103:2021 dla grupy N.11).

Na zestaw przewoźny H09-Z/1 składa się:

- radiostacja H09-Z/1;
- adapter 05211/2;
- wzmacniacz 05218/1/1;
- głośnik aktywny 0529/4;

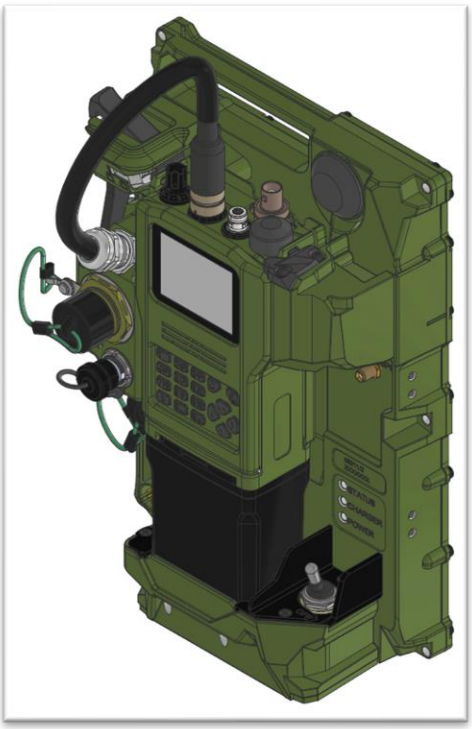
Zestaw przewoźny radiostacji występuje w trzech konfiguracjach:

Konfiguracja A - Wzmacniacz 05218/1 oraz Adapter 05211/2 z zamontowaną radiostacją H09-Z/1, umiejscowione na jednej podstawie montażowej. Praca z mocą do 50 W.



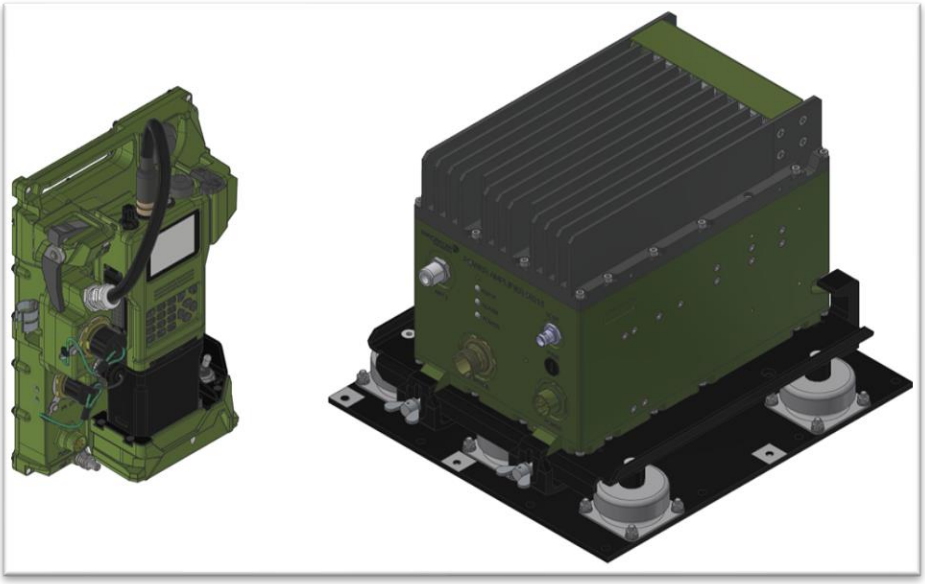
Rysunek 2 Radiostacja H09-Z/1 w konfiguracji A z adapterem i wzmacniaczem.

Konfiguracja B - Adapter 05211/2 z zamontowaną radiostacją H09-Z/1. Praca z mocą do 5 W.



Rysunek 3 Radiostacja H09-Z/1 w konfiguracji B z adapterem.

Konfiguracja C - Adapter 05211/2 z zamontowaną radiostacją H09-Z/1 oraz wzmacniacz zamontowany na osobnej podstawie montażowej w odległości do 10 metrów od radiostacji. Praca z mocą do 50 W.



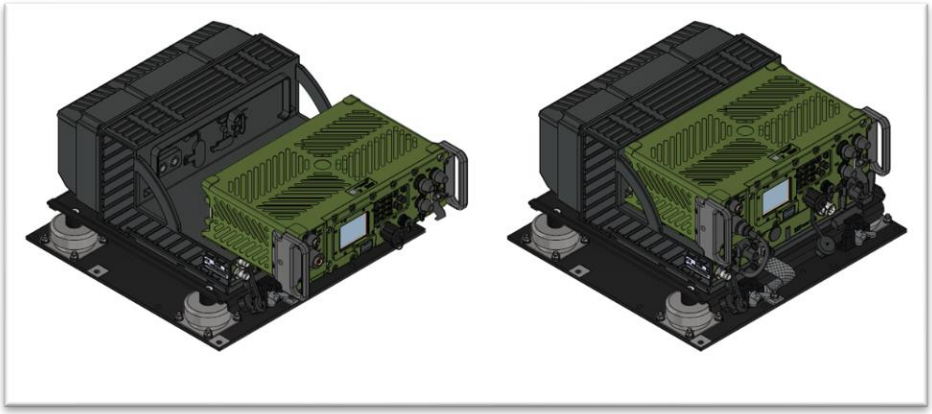
Rysunek 4 Radiostacja H09-Z/1 w konfiguracji C z adapterem i wzmacniaczem.

– Radiostacja pokładowa V09-Z/1

Radiostacja pokładowa V09-Z/1 charakteryzuje się:

- kompatybilnością wsteczną z waveformami radiostacji H09-Z/1;
- rozbudowanymi funkcjonalnościami waveformów (dane szeregowe, wiadomości SMS, wiadomości ALARM, zwiększone przepływności W2FH, inne);
- możliwością wykorzystania wzmacniacza i anten radiostacji pokładowej RRC 9310 (pracując w zakresie częstotliwości 30-88 MHz z mocą do 50 W;
- pełną kompatybilnością z akcesoriami radiostacji COMP@N-Z;
- rozbudowanymi funkcjonalnościami pozwalającymi na wykorzystanie radiostacji jako samodzielnego szyfratora w oparciu o ustandaryzowane algorytmy NINE/STACIS;
- pracą z wykorzystaniem tych samych systemów SPSR i SZGDK co przy pracy z radiostacją H09-Z/1 (możliwość tworzenia misji składających się z radiostacji różnego typu).

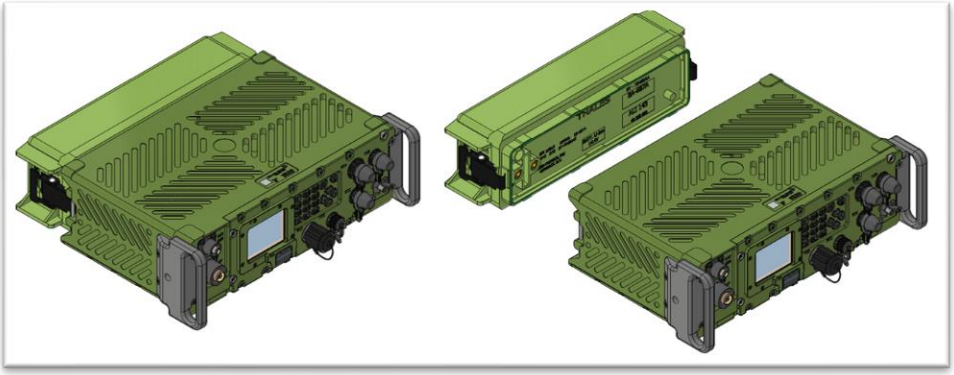
Zestaw przeznaczony jest do instalowania w lekkich czołgach, bojowych wozach piechoty, kołowych transporterach opancerzonych, haubicach, moździerzach i obiektach zbudowanych na bazie pojazdów zarówno kołowych jak i gąsienicowych (zgodnie z NO-06-A103:2021 dla grupy N.11 i N.12).



Rysunek 5 Radiostacja pokładowa V09-Z/1.

– Radiostacja plecakowa M09-Z/1

Radiostacja plecakowa M09-Z/1 bazująca na urządzeniu nadawczo-odbiorczym zastosowanym w wersji pokładowej (moc do 5W) jest dopełnieniem rodziny radiostacji COMP@N-Z i charakteryzuje się tymi samymi funkcjonalnościami co radiostacja pokładowa.



Rysunek 6 Radiostacja plecakowa M09-Z/1.

– System Planowania Sieci Radiowych (SPSR)

System Planowania Sieci Radiowych (SPSR) stanowi dedykowane oprogramowanie, którego zadaniem jest planowanie sieci radiowych oraz generacja:

- Danych Radiowych (niezbędnych do poprawnego skonfigurowania radiostacji);

- zamówień na Dokumenty Kryptograficzne przesyłane do SZGDK (System Zarzadzania Generacją Danych Kryptograficznych);
- zamówień na PIN użytkowników (zarządzanie PIN odbywa się w SZGDK).

Ideą opracowania Systemu Planowania Sieci Radiowych było stworzenie programowego narzędzia do planowania łączności dla wszystkich radiostacji z rodziny COMP@N-Z oraz w kolejnym wydaniu, dla radiostacji osobistych (RO) systemu TYTAN. Założenie takie wynika z zidentyfikowanej potrzeby wytworzenia jednolitych planów łączności dla tych systemów, generowanych w oparciu o takie samo narzędzie, co zdecydowanie ułatwia proces szkolenia odpowiedzialnych w SZ RP za przygotowanie obu wspomnianych systemów do pracy.

Należy podkreślić, że jednym z założeń przyjętych w tworzeniu SPSR jest wykorzystanie modułowej architektury programowej, co pozwoli w przyszłości na rozbudowę systemu i możliwość generowania danych radiowych, planów łączności oraz tabel z danymi radiowymi także dla innych radiowych środków łączności. Po uzyskaniu akceptacji właściwych instytucji, SPSR będzie mógł pracować w środowisku systemu MILNET-Z.

Funkcjonalności:

- planowanie struktury dowodzenia;
- przypisanie osób funkcyjnych (korespondentów) do poszczególnych elementów struktury;
- tworzenie i aktualizowanie bazy dostępnych środków łączności radiowej;
- wprowadzenie listy nominałów częstotliwości;
- wprowadzenie adresów IP zewnętrznych interfejsów środków łączności;
- przydzielenie środków łączności do osób funkcyjnych;
- planowanie sieci radiowych;
- przygotowywanie danych eksploatacyjnych dla radiostacji;
- przygotowanie zapotrzebowania na dokumenty kryptograficzne.

– System Zarządzania i Generowania Dokumentów Kryptograficznych (SZGDK)

SZGDK stanowi platformę sprzętowo-programową pozwalającą na generację danych kryptograficznych służących do konfiguracji algorytmów

kryptograficznych implementowanych w radiostacjach COMP@N-Z oraz w kolejnym wydaniu również dla RO TYTAN. Ponadto, SZGDK personalizuje radiostacje przed pierwszym użyciem, zarządza dystrybucją materiałów dostarczanych do radiostacji, zapewnia rozliczalność cyklu życia materiałów kryptograficznych oraz umożliwia zbieranie i analizę logów z urządzeń radiowych.

Wymagana liczba terminali niezbędnych do zapewnienia sprawnej generacji i dystrybucji danych kryptograficznych zależna jest od struktury organizacyjnej związku taktycznego. Producent nie ogranicza liczby sieci i urządzeń radiowych mogących zapewnić materiały i ich rozliczalność. Planując system łączności na poziomie taktycznym należy zaplanować również gdzie i na jakim poziomie (brygada, batalion) zostaną rozmieszczone terminale SZGDK.

Opracowany system podlega badaniu i ocenie bezpieczeństwa w ramach procesu certyfikacji prowadzonej przez SKW (w trybie art. 50 ust. 2 i 6 Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych – tekst jednolity Dz. U. 2023 poz. 756 t.j.). Szczegółowe funkcjonalności oraz opis systemu stanowią dane niejawne i nie mogą być publikowane w niniejszym dokumencie.

Funkcjonalności:

- import Danych Radiowych (DR) oraz Zapotrzebowania na Dane Kryptograficzne (ZDK) z SPSR;
- generacja dokumentów kryptograficznych;
- przygotowanie i zabezpieczenie Danych Eksploatacyjnych (DE = DR + ZDK) dla poszczególnych radiostacji;
- dystrybucja Danych Eksploatacyjnych do poszczególnych radiostacji;
- dystrybucja i analiza logów z radiostacji;
- dystrybucja paczek aktualizacyjnych radiostacji;

– System Szkoleniowy

Na podstawie doświadczeń z wielu szkoleń wykonywanych na potrzeby wdrożeń oraz warsztatów wykonywanych z personelem SZ RP i kooperantami, opracowano szereg programów szkoleniowych na poziomach zapoznawczym, operatorskim oraz instruktorskim.

Nowym elementem systemu jest również Zintegrowana Interaktywna Platforma Szkoleniowa - system wspierający proces nauczania, łączący funkcje

platformy e-learningowej z zaawansowanymi symulatorami. Integralną częścią systemu są symulator oraz trenażer pozwalające na praktyczny sposób szkolenia personelu wojskowego. System oferuje dostęp do materiałów dydaktycznych, testów, prezentacji oraz umożliwia monitorowanie postępów i ocenę uczestników. Symulator radiostacji H09-Z/1 wiernie odwzorowuje działanie rzeczywistego urządzenia i ponadto:

- umożliwia prowadzenie komunikacji głosowej między stanowiskami, zależnej od ustawień i warunków (np. zasięgu czy pozycji na mapie);
- umożliwia podłączanie akcesoriów;
- wizualizuje położenie radiostacji w terenie;
- umożliwia instruktorowi, w czasie rzeczywistym, wprowadzanie zakłóceń do pracy sieci radiowej oraz symulowanie niesprawności sprzętu poszczególnych korespondentów;
- umożliwia instruktorowi dostęp do panelu zarządzania, pozwalającego na monitorowanie stanowisk, kontrolę komunikacji, wprowadzanie uszkodzeń oraz prowadzenie egzaminów;
- daje możliwość nauczania i prowadzenia treningów, w ramach cyklu szkolenia, wprowadzających do faktycznego użycia sprzętu;
- jest podatny na rozbudowę o kolejne typy radiostacji w miarę jak zostają wdrażane do SZ RP.

Zastosowanie symulatora obniża koszty szkolenia, eliminuje zużycie sprzętu oraz umożliwia realizację scenariuszy niedostępnych w warunkach rzeczywistych.



Rysunek 7 Zintegrowana Interaktywna Platforma Szkoleniowa

– Możliwości integracji

Radiostacja ma interfejs SNMP do wygodnego zarządzania zdalnego oraz interfejsy audio i danych (IP/szeregowe) umożliwiające integrację z systemami pokładowymi oraz systemami typu BMS. Radiostacja M09-Z/1 wyposażona jest w tzw. czarny interfejs oraz oprogramowanie umożliwiające wykorzystanie radiostacji w roli samodzielnego szyfratora (praca przewodowa).

– STaCIS / NINE

Radiostacja ma wbudowane mechanizmy bezpieczeństwa STaCIS (zgodne z normą STANAG 5068) i NINE (Information Infrastructure Internet Protocol Network Encryption) zgodne ze STANAG 4787.

– TOPAZ

Radiostacja COMP@N-Z może być częścią systemu TOPAZ-ICMS (Integrated Combat Management System) – Zintegrowanego Systemu Zarządzania Walką. Jest to modułowy zestaw aplikacji klasy C4I/BMS, zaprojektowany by zapewnić dowódcom na każdym szczeblu dowodzenia pełną kontrolę nad sytuacją na polu walki. System obejmuje m.in. moduły TOPAZ Fires – kierowania różnorodnymi środkami artylerii lufowej i rakietowej, czy TOPAZ Strike – kierowania bezzałogowymi środkami uderzenia (UCV, np. WARMATE). Gwarantuje użytkownikowi utrzymanie stałej przewagi informacyjnej nad przeciwnikiem.

– DSI TAK

DSI TAK to aplikacja na smartfony z wykorzystywana do tworzenia świadomości sytuacyjnej pola walki. Umożliwia użytkownikom nawigację z wykorzystaniem GPS i wizualizację danych świadomości sytuacyjnej w czasie rzeczywistym.. Radiostacja COMP@N-Z pozwala na integrację z aplikacją DSI TAK w celu prezentacji danych na podkładzie mapowym w czasie rzeczywistym (demonstracja podczas warsztatów „Bystry Bluszcz-25”). W trakcie opracowania jest również aplikacja umożliwiająca sterowanie wybranymi parametrami radiostacji (np. zmiana kanału, głośność) przy pomocy smartfonu.

– HMS C3IS JAŚMIN

JAŚMIN to opracowany i produkowany przez TELDAT, stacjonarny wielodomenowy, zautomatyzowany system zarządzania walką, na poziomie operacyjno–taktycznym. W ramach Programu WISŁA system Comp@n-Z bazujący na radiostacji H09-Z/1 został zintegrowany z HMS JAŚMIN.

– BMS LEGION

LEGION to zintegrowane oprogramowanie i sprzęt mające za zadanie wsparcie planowania, dowodzenia, kierowania i łączności w siłach zbrojnych. W ramach warsztatów BB-25 system Comp@n-Z bazujący na radiostacji H09-Z/1 został zintegrowany z BMS Legion.


PRZYSZŁOŚĆ
WOJSKOWEJ
KOMUNIKACJI
POLSKIE
RADIOSTACJE
PROGRAMOWALNE
JEDYNE RADIOSTACJE
W SIŁACH ZBROJNYCH
RP Z CERTYFIKATEM
OCHRONY
KRYPTOGRAFICZNEJ
SKW
OSOBISTE,
DORĘCZNE
I POJAZDOWE
COMP@N-Z wielozakresowa
Szerokopasmowa PERAD
OSOBISTA IP
www.wbgroup.com
GRUPA WB

Siltec

SILTEC Sp. z o.o.

SILTEC – BEZPIECZNA KOMUNIKACJA. NIEZAWODNA INFRASTRUKTURA

TEMPEST – bezpieczeństwo zaczyna się od sprzętu



W ochronie informacji niejawnych nie ma miejsca na kompromisy. Każde urządzenie, każdy komponent i każdy etap wdrożenia musi spełniać wymagania środowisk, w których bezpieczeństwo danych ma znaczenie strategiczne.

SILTEC od lat rozwija rozwiązania TEMPEST projektowane z myślą o bezpiecznym przetwarzaniu informacji o szczególnym znaczeniu. Od komputerów i laptopów, przez urządzenia sieciowe i systemy transmisji danych, aż po specjalistyczną infrastrukturę IT. Portfolio spółki odpowiada na potrzeby organizacji, dla których ochrona informacji jest codzienną odpowiedzialnością, a nie dodatkiem do technologii.



Za każdym z tych rozwiązań stoi kompleksowy proces realizacji: projektowanie, integracja, produkcja, badania laboratoryjne i wsparcie serwisowe. Własne zaplecze techniczne oraz doświadczony zespół inżynierów pozwalają SILTEC tworzyć systemy dopasowane do realnych potrzeb użytkowników – dziś i w przyszłości.

Komunikacja bez ograniczeń



W świecie, w którym decyzje często zapadają w czasie rzeczywistym, bezpieczne środowisko współpracy nie może być przywiązane do jednego miejsca. Raz odbywa się w sali konferencyjnej, innym razem w terenie, blisko działań operacyjnych. Z tego względu SILTEC rozwija systemy wideokonferencyjne, które pozwalają zachować łączność niezależnie od warunków i lokalizacji.

Gdy miejscem działania staje się sala konferencyjna, SILTEC dostarcza rozwiązania VTC łączące wysoką jakość komunikacji z wygodą codziennego użytkowania. Kamera, mikrofony i głośniki zamknięte w jednym urządzeniu zapewniają wysoką jakość obrazu i dźwięku, a zestaw z ekranem i stojakiem pozwala szybko stworzyć wygodne środowisko do spotkań na różnych platformach wideokonferencyjnych.

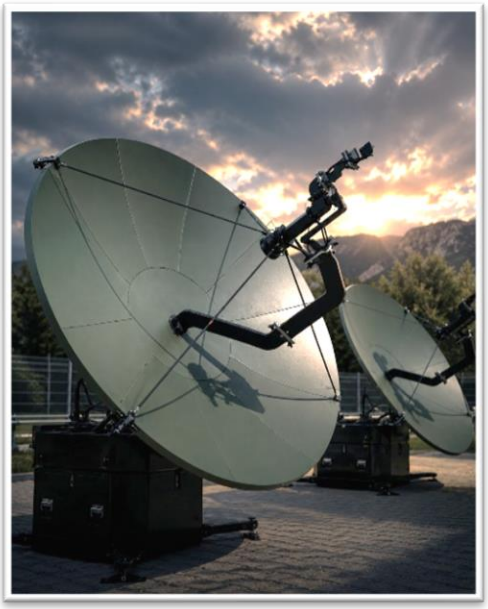


W przypadku gdy komunikacja musi wyjść poza budynek, odpowiedzią jest MVTC – mobilny system wideokonferencyjny zaprojektowany i wykonany przez SILTEC w dedykowanej zabudowie walizkowej. To rozwiązanie gotowe do pracy w terenie, odporne na trudne warunki atmosferyczne i dostępne zarówno w wariancie komercyjnym, jak i TEMPEST. W jednej wytrzymałej konstrukcji zintegrowano monitor LCD, nagłośnienie, kamerę, router, kodek Cisco Webex Room Bar oraz panel sterowania, tworząc kompletne stanowisko telekonferencyjne tam, gdzie warunki wymagają pełnej niezawodności.

Łączność bez granic

Są miejsca, w których tradycyjna infrastruktura telekomunikacyjna po prostu nie istnieje. Są też sytuacje, w których niezawodna komunikacja staje się

kluczowym elementem powodzenia całej operacji. Właśnie z myślą o takich wyzwaniach powstał Średni Terminal Satelitarny STS.



To rozwiązanie zapewnia bezpieczną i stabilną łączność satelitarną wszędzie tam, gdzie liczy się mobilność, szybkość działania i niezależność od lokalnej infrastruktury. Zaprojektowany z myślą o pracy w wymagających warunkach terenowych, pozwala na sprawne uruchomienie komunikacji i utrzymanie ciągłości wymiany danych nawet w najbardziej wymagających środowiskach operacyjnych.

Całość uzupełniają dedykowane rozwiązania transportowe opracowane przez SILTEC, dzięki którym system pozostaje gotowy do działania zarówno podczas przemieszczania, jak i po dotarciu do miejsca realizacji zadania.

Bezpieczna infrastruktura IT w kompaktowej formie

Wrażliwy sprzęt teleinformatyczny coraz częściej musi pracować poza stałą infrastrukturą – być przewożony, szybko uruchamiany i wykorzystywany w miejscach, gdzie warunki dalekie są od środowiska typowego dla serwerowni. W takich sytuacjach liczy się nie tylko sama funkcjonalność urządzeń, ale także ich ochrona przed wstrząsami, zakłóceniami elektromagnetycznymi i nieautoryzowanym dostępem.



W odpowiedzi na te potrzeby SILTEC stworzył Mobilną Platformę IT – rozwiązanie łączące bezpieczny transport sprzętu teleinformatycznego z ochroną elektromagnetyczną i odpornością na trudne warunki eksploatacji. Kompaktowa konstrukcja pozwala integrować i przewozić urządzenia w standardzie 19” RACK, zapewniając im ochronę zarówno w drodze, jaki podczas pracy operacyjnej.

Wysoka odporność mechaniczna, skuteczne ekranowanie elektromagnetyczne oraz możliwość dostosowania konfiguracji do indywidualnych potrzeb użytkownika sprawiają, że platforma znajduje zastosowanie wszędzie tam, gdzie bezpieczeństwo informacji musi iść w parze z mobilnością.

Mobilność, modularność, niezależność – infrastruktura gotowa wszędzie

Nie każda lokalizacja dysponuje serwerownią. Nie każda operacja może czekać na budowę zaplecza IT. Dlatego SILTEC rozwija Mobilne Data Center – kontenerowe centrum danych stworzone z myślą o środowiskach wymagających pełnej niezależności i gotowości do działania.

Mobilne Data Center to znacznie więcej niż mobilna serwerownia. To kompletna, samowystarczalna infrastruktura IT, którą można uruchomić praktycznie w dowolnym miejscu – od obiektów infrastruktury krytycznej po działania realizowane w terenie. Modułowa konstrukcja pozwala szybko dopasować rozwiązanie do potrzeb konkretnego projektu, a następnie rozwijać je wraz ze wzrostem wymagań użytkownika.



Rozwiązanie wspiera zarówno sektor obronny, jak i organizacje odpowiedzialne za realizację procesów o znaczeniu strategicznym. Zapewnia ciągłość działania, bezpieczne przetwarzanie danych oraz pełną gotowość operacyjną nawet w najbardziej wymagających warunkach środowiskowych.

Dostępne są zarówno warianty komercyjne, jak i wersje o zwiększonej ochronie elektromagnetycznej, przeznaczone do zastosowań wymagających najwyższego poziomu bezpieczeństwa informacji. Dzięki wysokiej elastyczności, autonomiczności i zgodności z rygorystycznymi wymaganiami rozwiązanie stanowi niezawodny fundament nowoczesnej infrastruktury krytycznej.

Standardy, które budują zaufanie

SILTEC posiada szeroki zakres uprawnień, certyfikatów i akredytacji potwierdzających spełnianie najwyższych standardów jakości i bezpieczeństwa w realizacji projektów dla sektora obronnego, administracji publicznej oraz infrastruktury krytycznej.

SILTEC Sp. z o.o.
ul. Parzniewska 12, 05-800 Pruszków
+48 22 572 18 00 | biuro@siltec.pl
www.siltec.pl


Siltec
Łączymy
doświadczenie
z nowoczesnymi technologiami
Projektujemy, produkujemy i wdrażamy zaawansowane rozwiązania dla telekomunikacji, infrastruktury krytycznej i obronności – od rozwiązań dedykowanych dla łączności po niezawodne systemy zasilania gwarantowanego.
Nowoczesne technologie
Sprawdzone rozwiązania
Niezawodność w działaniu
Bezpieczeństwo danych
SYSTEMY ŁĄCZNOŚCI
ZABUDOWY KONTENEROWE
TEMPEST IT
SYSTEMY ZASILANIA
ROZWIĄZANIA SPECJALNE
biuro@siltec.pl

Transbit Sp. z o.o.

TRANSBIT – INTEGRATOR SYSTEMÓW ŁĄCZNOŚCI DLA WOJSK OBRONY PRZECIWLOTNICZEJ



Wojska Obrony Przeciwlotniczej należą do najbardziej wymagających użytkowników systemów łączności. Spełnienie ich wymagań operacyjnych wymaga zapewnienia wysokiej niezawodności systemu, precyzyjnej synchronizacji czasu pomiędzy węzłami sieci oraz minimalnych opóźnień transmisji danych — w tym ograniczenia zmienności opóźnień pakietów IP, określanej jako jitter.

Jako integrator systemów łączności Transbit odpowiada za kompleksową infrastrukturę telekomunikacyjną — przewodową i radiową — w programach obrony powietrznej Sił Zbrojnych RP: WISŁA średniego zasięgu, NAREW krótkiego zasięgu, PILICA bardzo krótkiego zasięgu oraz SAN przeznaczonym do zwalczania zagrożeń bezzałogowych.

Transbit opracował kompleksowy podsystem łączności zapewniający bezpieczną transmisję danych, wysoką przepustowość oraz precyzyjne zarządzanie czasem w rozproszonej architekturze obrony powietrznej.

Radion OPL – sieć łączności dla obrony powietrznej

Kluczowym elementem rozwiązania jest system Radion OPL, przeznaczony do zarządzania pracą sieci oraz przepływem informacji pomiędzy najważniejszymi elementami systemu obrony przeciwlotniczej, w tym radarami, wyrzutniami rakietowymi, stanowiskami dowodzenia i węzłami łączności.

W architekturze Radion OPL Transbit wdrożył również Dedykowane Łącze Komunikacyjne DCL, zapewniające bezpieczną łączność głosową oraz niezawodną transmisję danych.

Radiolinia R-460AM

Radiolinia R-460AM, pracująca w paśmie NATO IV, zapewnia wysokoprzepustową i bezpieczną transmisję pakietową na odległościach do około 40 km — przy zastosowaniu odpowiedniej konfiguracji masztowej.

System umożliwia transmisję danych z przepływnością ponad 600 Mb/s w obu kierunkach. Praca w paśmie IV pozwala na wykorzystanie szerszych kanałów radiowych, zwiększając ilość transmitowanych danych. Zastosowanie anten dual-polarized oraz trybu MIMO umożliwia osiąganie wysokiej przepustowości przy efektywnym wykorzystaniu dostępnego widma.

Radiolinia została wyposażona w mechanizmy synchronizacji czasu, które — po integracji z serwerem czasu — zapewniają wysoką precyzję niezbędną m.in. dla systemów pasywnej lokacji.

Istotną funkcją R-460AM jest możliwość pracy wielokanałowej z wykorzystaniem systemu anten Switched Beam (SB). Rozwiązanie umożliwia jednoczesne utrzymywanie łączności z wielu kierunków z radioliniami wyposażonymi w anteny kierunkowe lub pracę w sieci radioliniowej typu MESH, złożonej z wielu węzłów wyposażonych w anteny SB.

Taka konfiguracja może być wykorzystywana do budowy zintegrowanej sieć kierowania ogniem w architekturze systemu IBCS — Integrated Battle Command System, wykorzystywanego w polskim wojsku z wyrzutniami PATRIOT. Radiolinia R-460AM jest zintegrowana z systemem IBCS i stanowi podstawową warstwę transmisji danych pomiędzy jego węzłami sieciowymi.

Mobilne Węzły Łączności MCC

Polska sieć łączności realizowana w ramach programu WISŁA opiera się na węzłach łączności Mobile Communication Center (MCC).

Węzły MCC wyposażone są w systemy radioliniowe R-460AM-2 Transbit oraz inne elementy infrastruktury łączności, w tym radiostacje szerokopasmowe R-450C, serwery czasu, routery, serwery i switche. Transbit odpowiada za dostawę oraz integrację kompletnego systemu w ramach węzłów MCC.



Radiostacja szerokopasmowa R-450C

Radiostacja R-450C wykorzystuje autorski waveform opracowany i zoptymalizowany pod kątem wymagań operacyjnych Wojsk OPL.

Zapewnia łączność szerokopasmową i wymianę danych w taktycznym środowisku operacyjnym.

Serwer czasu TS-01

Serwer czasu TS-01 zapewnia synchronizację czasu we wszystkich elementach systemu, niezależnie od dostępności sygnału GPS.

Urządzenie zostało zaprojektowane do pracy w warunkach celowych zakłóceń i zagłuszania sygnałów satelitarnych.

Routery RP-510-01 i RP-301-01

Routery RP-510-01 oraz RP-301-01 spełniają wymagania bezpieczeństwa dla zastosowań wojskowych i zapewniają stabilną, niezawodną transmisję danych w środowisku taktycznym.



Router pokładowy RP-510-01



Router pokładowy RP-301-01

Aplikacja SMiKO

Aplikacja SMiKO stanowi narzędzie do konfiguracji, diagnostyki i zarządzania wojskowymi sieciami łączności. System wspiera również planowanie rozmieszczenia oraz pozycjonowania węzłów komunikacyjnych w terenie.

Radiolinia R-460W

Radiolinia R-460W została opracowana z myślą o budowie łączy o niskim prawdopodobieństwie przechwycenia — Low Probability of Intercept (LPI).

Rozwiązanie przeznaczone jest do działań wymagających wysokiego poziomu dyskrecji oraz ograniczenia ryzyka wykrycia transmisji. Urządzenie

pracuje w paśmie częstotliwości 36–37 GHz i umożliwia transmisję danych na odległościach około 10 km.



Radiolinia łącza trudno wykrywalnego R-460W, zintegrowana z rotorem

SanComms – zintegrowany system łączności dla programu antydronowego SAN

W ramach programu antydronowego SAN, realizowanego na potrzeby Sił Zbrojnych RP, Transbit odpowiada za zaprojektowanie i integrację kompleksowego systemu łączności SanComms.

SanComms stanowi kręgosłup komunikacyjny systemu SAN, zapewniający bezpieczną i niezawodną wymianę informacji pomiędzy wszystkimi

elementami ugrupowania bojowego. Obejmuje łączność pomiędzy stanowiskami dowodzenia szczebla plutonu i baterii, sensorami, radarami, systemami optoelektronicznymi w warunkach mobilnych i stacjonarnych.

System został zaprojektowany dla środowiska operacyjnego, w którym kluczowe znaczenie mają mobilność, szybka reakcja oraz zdolność do działania w warunkach dużego nasycenia przestrzeni powietrznej zagrożeniami bezzałogowymi. W przypadku zwalczania dronów, szczególnie w scenariuszu ataku rojowego, skuteczność działania zależy od bardzo szybkiego wykrycia zagrożenia, przekazania danych do systemu dowodzenia, identyfikacji celu oraz skierowania efektora.

SanComms umożliwia przekazywanie danych, obrazu, głosu w czasie rzeczywistym. System wspiera szybkie odświeżanie wspólnego obrazu sytuacji powietrznej — Recognized Air Picture (RAP) — co ma istotne znaczenie dla procesu dowodzenia i kierowania ogniem.

Łączność dla mobilnego ugrupowania bojowego

System SAN integruje wiele elementów rozmieszczonych w terenie i zdolnych do szybkiej zmiany pozycji. Oznacza to konieczność budowy elastycznej infrastruktury komunikacyjnej, zdolnej do utrzymania wymiany danych pomiędzy rozproszonymi platformami, nawet przy ograniczonej dostępności infrastruktury stałej.

SanComms łączy warstwę radiową i przewodową, tworząc odporną architekturę transmisji danych dla mobilnych elementów systemu. Rozwiązanie uwzględnia wymagania dotyczące bezpieczeństwa transmisji, odporności na zakłócenia oraz podziału środowiska przetwarzania danych na domeny o różnym poziomie ochrony informacji.

R-450C – serce radiowej wymiany danych



Podstawowym środkiem łączności radiowej w systemie SanComms jest radiostacja szerokopasmowa R-450C.

Radiostacja została zaprojektowana do pracy w rzeczywistych warunkach pola walki, gdzie priorytetem są niezawodność, odporność operacyjna oraz minimalne opóźnienia transmisji. R-450C umożliwia szybką wymianę danych pomiędzy elementami ugrupowania, wspierając przekazywanie informacji niezbędnych do skutecznego wykrywania, śledzenia i zwalczania zagrożeń.

Zastosowanie radiostacji R-450C jako głównego elementu warstwy radiowej pozwala zapewnić sprawną transmisję danych pomiędzy stanowiskami dowodzenia, sensorami i efektorami, także w dynamicznie zmieniającym się środowisku operacyjnym.

Integracja wielu elementów systemu SanComms nie jest jedynie siecią łączności. To zintegrowane środowisko teleinformatyczne, umożliwiające współpracę wielu komponentów systemu antydronowego.

Architektura obejmuje urządzenia radiowe, elementy infrastruktury IP, serwery, routery, switche oraz interfejsy do integracji z systemami dowodzenia i kierowania ogniem. System będzie współpracować z rozwiązaniami C2 (Command and Control) systemami dowodzenia i kierowania.



Serwer usług sieciowych SUS-24-01



Terminale łączności VoIP AC-30IP

Kluczowym wyzwaniem jest integracja wielu źródeł danych oraz zapewnienie ich szybkiego i bezpiecznego przekazywania pomiędzy wszystkimi uczestnikami ugrupowania bojowego. Dotyczy to zarówno danych z sensorów, jak i informacji wykorzystywanych przez stanowiska dowodzenia oraz efektory.

Zarządzanie siecią i diagnostyka

System SanComms wykorzystuje aplikację SMiKO — System Monitorowania i Konfigurowania Obiektu. SMiKO umożliwia graficzne zarządzanie siecią, konfigurację urządzeń, monitorowanie stanu infrastruktury oraz diagnostykę połączeń i interfejsów. Narzędzie wspiera operatorów w szybkim wykrywaniu nieprawidłowości, lokalizacji usterek oraz utrzymaniu gotowości systemu.

Otwarta architektura aplikacji pozwala na integrację urządzeń i systemów różnych dostawców, co ma szczególne znaczenie w złożonych systemach obrony powietrznej i przeciwdziałania zagrożeniom bezzałogowym.

Doświadczenie Transbit w integracji systemów obrony powietrznej

Projekt SanComms wykorzystuje doświadczenie Transbit zdobyte w programach obrony przeciwlotniczej, w tym w systemach PILICA i PILICA+, a także w innych rozwiązaniach przeznaczonych dla Sił Obrony Powietrznej.

Kompetencje Transbit obejmują projektowanie, dostawę i integrację rozbudowanych systemów łączności dla wieloelementowych architektur wojskowych. Firma posiada doświadczenie w łączeniu stanowisk dowodzenia, radarów, sensorów, efektorów oraz mobilnych węzłów transmisji danych w jedną spójną, odporną i skalowalną architekturę.

SanComms jest przykładem zdolności Transbit do realizacji złożonych projektów integracyjnych, w których niezawodna wymiana informacji, minimalne opóźnienia oraz interoperacyjność wszystkich elementów mają bezpośredni wpływ na skuteczność działania systemu bojowego.

Rozwiązania Transbit stanowią fundament nowoczesnej, sieciocentrycznej architektury łączności wojskowej. Wspierają skuteczne dowodzenie i kierowanie, budowę świadomości sytuacyjnej oraz bezpieczeństwo operacyjne na współczesnym polu walki.

WZŁ-1 S.A.

ROLA SERWISU TECHNICZNEGO WOJSKOWYCH ZAKŁADÓW ŁĄCZNOŚCI NR 1 S.A. W ZAPEWNIENIU ŁĄCZNOŚCI W POLSCE I W POLSKICH KONTYNGENTACH WOJSKOWYCH (PKW)

Serwis techniczny WZŁ-1 S.A. odgrywa niebagatelną rolę w zapewnieniu łączności dla Sił Zbrojnych RP zarówno stacjonujących w kraju jak i poza jego granicami. Dotyczy to zarówno łączności przewodowej, jak i bezprzewodowej realizowanej za pośrednictwem urządzeń radiowych, radiolinio-wych i satelitarnych. Przedmiot łączności należ rozpatrywać w kilku aspektach, które dopiero połączone w całość gwarantują sprawną, skuteczną i przede wszystkim bezawaryjną łączność na polu walki.



Pierwszym z nich jest zaplanowanie i zabezpieczenie odpowiednich urządzeń i rozwiązań telekomunikacyjnych w zależności od szeregu rozmaitych czynników, takich jak rejon działania, liczebność i mobilność zgrupowania wojsk, wymagane parametry transmisyjne i niezawodnościowe, redundancja oraz szybkość zarówno rozwinięcia (uruchomienia), jak i zwinięcia systemu łączności. Inne będą bowiem wymagania i wykorzystane rozwiązania w przypadku zabezpieczenia łączności dla plutonu czy kompanii, a inne dla brygady czy dywizji.

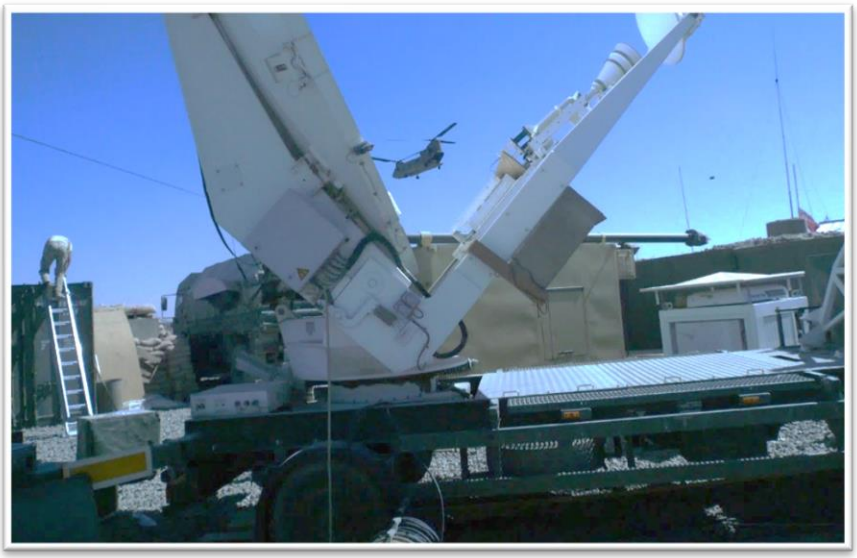


Jednak zaplanowanie i uruchomienie odpowiednich rozwiązań telekomunikacyjnych to nie wszystko. Równie ważne, o ile nie istotniejsze, jest zapewnienie bezawaryjnej pracy wykorzystywanych rozwiązań realizowane poprzez odpowiednią eksploatację, regularną konserwację i serwis sprzętu łączności. Na tym polu Serwis Wojskowych Zakładów Łączności Nr 1 S.A. dysponuje ogromną wiedzą i doświadczeniem a także wykwalifikowaną i wielokrotnie sprawdzoną w boju kadrą gotową podjęcia się kolejnych wyzwań.

Nasze rozwiązania techniczne i wsparcie serwisowe towarzyszą Siłom Zbrojnym RP od bardzo wielu lat zarówno w kraju, jak i w odległych zakątkach świata. Nasi przedstawiciele byli obecni – zarówno w formie wyjazdów serwisowych, jak i ciągłego wsparcia w rejonach PKW – między innymi w Bośni i Hercegowinie, Iraku, Afganistanie, Libanie, Kosowie, krajach Bałtyckich, Turcji, Rumunii i we Włoszech.









W tym miejscu należy zaznaczyć, iż działania serwisu technicznego nie ograniczają się wyłącznie do naprawy lub wymiany uszkodzonego sprzętu, ale także do bieżącej kontroli parametrów pracy i stanu urządzeń. Takie podejście do utrzymania sprzętu sprawia, iż potencjalne uszkodzenia pojawiają się znacznie rzadziej, a żywotność całego sprzętu ulega wydłużeniu. Dodatkową zaletą regularnych interwałów serwisowych jest możliwość wcześniejszego przewidzenia przyszłych uszkodzeń, co pozwala odpowiednio wcześniej przygotować niezbędne części zamienne i przeprowadzić naprawę urządzenia zanim przestanie ono funkcjonować.



Utrzymanie sprzętu łączności w dobrym stanie pozwala na minimalizację kosztów obsługi, gdyż naprawa eksploatowanego sprzętu jest zwykle wielokrotnie tańsza niż wymiana go na nowy. Ponadto, często zakup nowego rozwiązania związany jest z bardzo długim czasem oczekiwania na realizację zamówienia.



Równie ważne jak regularne serwisowanie sprzętu jest jego codzienna należyta obsługa przeprowadzana przez etatowych użytkowników. Jednak nie pozostają oni zdani sami na siebie, gdyż każdorazowe przekazanie sprzętu łączności do Sił Zbrojnych jest nierozerwalnie połączone z przeszkoleniem jego przyszłych użytkowników.





Dodatkowo, dzięki dużemu zapleczu intelektualnemu i sprzętowemu, Wojskowe Zakłady Łączności Nr 1 S.A. zapewniają bieżące i profesjonalne wsparcie dla każdego swojego wyrobu na cały okres jego użytkowania oraz prowadzenia szkoleń kolejnych załóg w zakresie podstawowym, zaawansowanym oraz serwisowym (szkolenie pozwalające na samodzielną diagnostykę i naprawę wybranych uszkodzeń).



SPIS TREŚCI

OD REDAKCJI **3**

Z DZIAŁALNOŚCI ZWIĄZKU **5**

INFORMACJA ZARZĄDU GŁÓWNEGO - *Mieczysław Hucał* 5

Z DZIAŁALNOŚCI OODZIAŁU SIERADZ w latach 2024-2025 – *Jerzy Sokołowski* 24

Z DZIAŁALNOŚCI ODDZIAŁU ŚREM – *Andrzej Korneluk* *50*

Z DZIAŁALNOŚCI ODDZIAŁU WARSZAWA - Ryszard *Floryński, Witold Fornalski, Urbańska* *80*

Z DZIAŁALNOŚCI ODDZIAŁU ZEGRZE - *Mieczysław Hucał* *98*

DZIEŃ ŁĄCZNOŚCIOWCA W SEROCKU – *Mieczysław Hucał* *115*

WSPÓŁPRACA MIASTA I GMINY SEROCK ZE ŚWIATOWYM ZWIĄZKIEM POLSKICH ŻOŁNIERZY ŁĄCZNOŚCI – *Artur Borkowski* *133*

Z ŻAŁOBNEJ KARTY **138**

JEDNOSTKI WOJSK ŁĄCZNOŚCI **141**

31. PUŁK STRZELCÓW KANIOWSKICH - ŁĄCZNOŚĆ - *Jan Kowalski* 141

ŁĄCZNOŚCIOWE TRADYCJE I TELEINFORMATYCZNY PULS ARMII – *Jarosław Sosiński* 149

BRYGADA WSPARCIA DOWODZENIA WIELONARODOWEGO KORPUSU PÓŁNOCNY-WSCHÓD – Adam *Dzielecki* *158*

60 – LECIE INFORMATYKI WOJSKOWEJ W REGIONIE BYDGOSZCZ – *Janusz Miraszewski* *183*

WSPOMNIENIA ŁĄCZNOŚCIOWCÓW **199**

PATRON REGIONALNEGO CENTRUM INFORMATYKI WARSZAWA – *Kamila Ochwat* *199*

PRZYWRÓCIĆ PAMIĘĆ MJR INŻ. ANDRZEJ GARBOŚ
- ŻOŁNIERZ ŁĄCZNOŚCI I WSPÓŁWYNALAZCA MIN
– Krzysztof Krząstek 204

Z OBERLANGEN DO MACZKOWA – Małgorzata Kaczyńska *211*

PUŁKOWNIK BERNARD MIEŃKOWSKI – PATRON PODODDZIAŁU WARSZAWA ŚZPŻŁ – Marian *Turek* *219*

Z ŻYCIA ŻOŁNIERZA – OD SZEREGOWEGO DO OFICERA STARSZEGO, CZ. IV – *Rafał Magoń* *224*

NA SZLAKU PODRÓŻY Z ŁĄCZNOŚCIĄ W TLE – LUBUSKIE MUZEUM WOJSKOWE W ZIELONEJ GÓRZE Z/S W DRZONOWIE *- Błażej Mościpan* *231*

RWIE DIĘ DO SŁOŃCA – *Marek Ruszczak, Roman Soroczyński* *239*

SPRZĘT ŁĄCZNOŚCI I INFORMATYKI 241

ENABLING MULTIDOMAIN OPERATION THROUGH DIGITAL RESILIENCE – *Krzysztof Kociuba* 241

PRODUKCJA „DUAL USE” – CORAZ BARDZIEJ ISTOTNA W SYSTEMIE BEZPIECZEŃSTWA PAŃSTWA
– *Włodzimierz Nowak* 249

CYBERZAGROŻENIA WE WSPÓŁCZESNYM ŚRODOWISKU WOJSKOWYM – *Berta Jurczuk* 258

TOPAZ + ASCA SYSTEMY KIEROWANIA POLEM WALKI
– Rafał *Magoń, Mirosław Friedek* 268

BIAŁY WYWIAD (OSINT) JAKO NARZĘDZIE W CYBERPRZESTĘPCZOŚCI I CYBERBEZPIECZEŃSTWIE – Cybulska 279

BMS LEGION – POLSKI SYSTEM ZARZĄDZANIA POLEM WALKI NOWEJ GENERACJI – Daniel *Kondyra,Mateusz Polonczyk* *284*

WOZY DOWODZENIA NA PODWOZIU KTO ROSOMAK ZAWILEC, KROTON I KROTON 2 – *G.K* *295*

FIRMY TELEKOMUNIKACYJNE 301

SYSTEM RADIOSTACJI COMPAN@N-Z DLA SIŁ ZBROJNYCH RP – *Grupa WB.* 301

GRUPA *WB - Reklama* 315

SILTEC – BEZPIECZNA KOMUNIKACJA NIEZAWODNA – INFRASTRUKTURA - Siltec 317
SILTEC – *Reklama* 321
TRANSBIT – INTEGRATOR SYSTEMÓW ŁĄCZNOŚCI DLA WOJSK OBRONY PRZECIWLOTNICZEJ – *TRANSBIT* 322
ROLA SERWISU TECHNICZNEGO WOJSKOWYCH ZAKŁADÓW ŁĄCZNOŚCI NR 1 S,A, W ZAPEWNIENIU ŁĄCZNOŚCI W POLSCE I W POLSKICH KONTYGMENTACH WOJSKOWYCH (PKW) – *WZŁ 1* 331