

KAMILA MATELA*

Politechnika Warszawska, Warszawa, Polska

WYBRANE ASPEKTY SYSTEMÓW WYWIADU, OBSERWACJI I ROZPOZNANIA (ISR)

CHOSEN ASPECTS OF INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE (ISR) SYSTEMS



ABSTRAKT: Niniejsza praca jest próbą syntetycznego przedstawienia współczesnego rozumienia i zastosowania jednego z kluczowych dla każdej armii na świecie obszarów – wywiadu, obserwacji i rozpoznania (ISR). W artykule dokonano podsumowania najważniejszych aspektów ISR i implementacji tego zagadnienia w siłach zbrojnych Polski i NATO oraz wyzwań z nimi związanych. Z uwagi na znaczący postęp technologiczny zaprezentowano również aspekty techniczne jednego z najszybciej rozwijających się rodzajów rozpoznania i wywiadu – analizy obrazu. Każdy rozdział zawiera odniesienie do polskich sił zbrojnych.

SŁOWA KLUCZOWE: ISR, wywiad, obserwacja, rozpoznanie, analiza obrazu, ISTAR.

ABSTRACT: This paper is an attempt to synthetically present the contemporary understanding and application of one of the key areas for any army in the world - intelligence, surveillance and reconnaissance (ISR). The article summarizes the most important aspects of ISR and its implementation in the Polish and NATO armed forces, as well as the challenges associated with them. Due to significant technological progress, technical aspects of one of the fastest growing types of reconnaissance and intelligence - image analysis - are also presented. Each chapter contains a reference to the Polish Armed Forces.

KEYWORDS: ISR, intelligence, surveillance, reconnaissance, image intelligence, ISTAR.

* Kamila Matela, Warsaw University of Technology, Warsaw, Poland

 <https://orcid.org/0000-0002-8728-1604>  [email: 01147225@pw.edu.pl](mailto:01147225@pw.edu.pl)

WPROWADZENIE

Artykuł 5 Organizacji Traktatu Północnoatlantyckiego (NATO) stanowi, że atak na jednego członka NATO jest atakiem na wszystkich jego uczestników. NATO wykorzystało ten zapis tylko raz w swojej historii – organizując operację w Afganistanie w odpowiedzi na ataki terrorystyczne z 11 września 2001 roku. Oprócz misji w Afganistanie, NATO interweniowało w Kosowie oraz w ramach misji pokojowej „Zabezpieczanie Morza Śródziemnego i Wsparcia Unii Afrykańskiej”. Misja w Afganistanie wykazała, że siły NATO mają poważny problem z szybką i ujednoczoną komunikacją – ze względu na udział w operacjach licznych sił różnych krajów, dysponujących dziesiątkami systemów. Z tego względu współpraca pomiędzy nimi jest dużym wyzwaniem.

Aby zarządzać operacjami NATO (niezależnie od ich charakteru: wsparcie pokoju, tradycyjne operacje wojskowe, misje stabilizacyjne lub zarządzania kryzysowego), siły Sojuszu muszą być wyposażone w natychmiastowe, zintegrowane i wydajne systemy multidyscyplinarne, wśród których są wywiad, obserwacja i rozpoznanie (ISR).

Celem artykułu jest przedstawienie bieżącego zakresu ISR i funkcjonowania tego obszaru w polskich siłach zbrojnych na tle systemów wdrażanych w NATO, a także jego zastosowania w operacjach wojskowych. Z uwagi na prowadzone przez autorkę tekstu eksperymenty w obszarze analizy obrazu, (ang. *Image Intelligence*) przedstawiono najbardziej aktualne informacje i aspekty techniczne związane z tą dziedziną wywiadu.

ZNACZENIE ISR

Literatura dotycząca systemów rozpoznania pola walki jest obszerna. Ich definicja zależy od wielu czynników, w tym: kontekstu, w jakim są prezentowane; celu, jakiemu służą; rodzaju sił zbrojnych czy instytucji, która kieruje jego rozwojem. Jednym z istotnych wyznaczników organizacji systemu rozpoznania jest rodzaj zagrożenia - również w tym zakresie obszar definicyjny będzie zróżnicowany.

Przez stulecia termin rozpoznanie, używany w dziedzinie wojskowości, rozpatrywany był głównie w kontekście działalności człowieka. Pierwsze opisy działań zwiadowczych znajdujemy w księgach Starego Przymierza. Służby wywiadowcze były integralną częścią sił zbrojnych od starożytności. Monarchie absolutne XVII i XVIII wieku przywiązywały wagę do terminowego rozpoznania zamiarów potencjalnych przeciwników¹, jednak pierwsze, formalne komórki powstały w XIX wieku, niemal równocześnie w Niemczech i Francji.

¹ Roger Faligot, Remy Kauffer, *Służby specjalne. Historia wywiadu i kontrwywiadu na świecie*, Wyd. ISKRY, Warszawa 2006, s. 8

Wagę i znaczenie systemów rozpoznawczych dla XX wieku w sposób uniwersalny zaprezentował oficer Cesarskiej Armii Rosyjskiej - Aleksander Iwanowicz Kuk – który w 1921 roku stwierdził, że zwycięstwo danego państwa zależy przede wszystkim od:

a. "znajomości planu wojennego prawdopodobnego przeciwnika (przeciwników) przez dane państwo oraz stopnia faktycznej skuteczności jego realizacji;

b. utrzymania w tajemnicy wszystkiego, co dane państwo wymyśliło i zrealizowało w swoim planie wojennym"².

Przełom w rozwoju obszaru rozpoznania przyszedł wraz z pierwszym konfliktem zbrojnym o zasięgu globalnym. Pojawiły się nowe techniki: łączność radiowa i telefoniczna; nowe możliwości dla praktyk rozpoznawczych: fotografia lotnicza, wojska desantowe. Wraz z rozwojem technologii, wojskowe systemy rozpoznawcze były doskonalsze, a ich poszczególne elementy coraz bardziej wyspecjalizowane. Jednym z najważniejszych wynalazków związanych z dziedziną wywiadu były maszyny do szyfrowania informacji – w tym najbardziej znana Enigma. Złamanie systemu jej funkcjonowania przez polskich matematyków i przekazanie tej wiedzy aliantom miało znaczący wpływ na losy II wojny światowej.

Współczesny, dynamiczny rozwój technologiczny wymaga szczegółowego spojrzenia na zakres systemów rozpoznania. Ponieważ NATO nie posiada autonomicznych sił i środków ISR, dlatego podczas prowadzenia operacji wykorzystuje się zarówno wydzielone, jak i narodowe zdolności ISR. Logika ISR została przedstawiona w Sojuszniczej Wspólnej Doktrynie Wywiadu, Kontrwywiadu i Bezpieczeństwa (*Allied Joint Doctrine for Intelligence, Counterintelligence and Security*), gdzie:

1. Wywiad definiuje się jako "(...) działania wynikające z bezpośredniego zbierania i przetwarzania informacji (...) "³;

Wyróżnia się kilkanaście rodzajów wywiadu wojskowego, a wśród nich:

Tabela 1. Lista rodzajów wywiadu.

HUMINT	Ang. <i>Human Intelligence</i> W tej dziedzinie, mimo dominacji technologicznej we współczesnym świecie, niezwykle istotna jest rola człowieka. „Konflikty zbrojne w Iraku i Afganistanie w znaczący sposób zmieniły podejście do prowadzenia rozpoznania operacyjnego. Tam najważniejszym elementem rozpoznania był człowiek i jego środowisko" ⁴ .
--------	--

² Aleksander Iwanowicz Kuk, *Kanwa wywiadu agenturalnego. Podstawy wywiadu osobowego*, Akademia Sztuki Wojennej, Warszawa 2020, s. 18

³ AJP-2.7 *Allied Joint Doctrine for Intelligence, Counterintelligence and Security*, Published by NATO, 2016, s.2-4

⁴ K. Danielewicz, *Komórka sztabowa 2X w operacji typu COIN* – wybrane zagadnienia, Przegląd ABW, s.1-3

OSINT ⁵	Ang. <i>Open Source Intelligence</i> , tzw. biały wywiad. Informacje są pozyskiwane z publicznie dostępnych źródeł: serwisów społecznościowych, specjalizowanych (serwisy mapowe) i dedykowanych (serwisy udostępniające narzędzia szpiegowskie za opłatą), zdjęcia, video itp. Prowadzenie działań wywiadowczych w tym zakresie nazywane jest też rozpoznaniem pasywnym.
SIGINT	Ang. <i>Signal Intelligence</i> – wywiad sygnałowy. Opiera się na analizie fal elektromagnetycznych oraz sygnałów pochodzących z systemów komunikacji (Ang. <i>Communication Intelligence</i>), radarowych lub innych. W ramach SIGINT rozróżnia się dwie podkategorie COMINT i ELINT.
COMINT	Ang. <i>Communication Intelligence</i> – analiza różnych kanałów komunikacji: radiowych, telefonicznych, satelitarnych, smsowych, w ramach której badaniu podlegają m.in. częstotliwości, nadajniki, czas trwania sygnału.
ELINT	Ang. <i>Electronic Signals Intelligence</i> – obejmuje analizę sygnału elektronicznego, który nie jest rozmową lub tekstem (zarezerwowane dla COMINT). Ma szczególne zastosowanie w zakresie Walki Radio-Elektronicznej (WRE), kiedy to koncentruje się na lokalizowaniu konkretnych celów ELINT. Uwzględnia w dużej części analizę telemetryczną polegającą na przechwytywaniu, przetwarzaniu i raportowaniu obcych telemetrii.
GEOINT	Ang. <i>Geospatial Intelligence</i> ⁶ - wywiad geoprzestrzenny. Polega na wykorzystaniu oraz analizie obrazu i informacji geoprzestrzennej do opisu, oceny i wizualizacji cech fizycznych, a także lokalizacji różnego rodzaju działalności na Ziemi (np. elektrowni jądrowych czy baz terrorystów). Wynikiem działań ISR i fuzji danych jest stworzenie wielowarstwowej informacji geoprzestrzennej.
IMINT	Ang. <i>Image Intelligence</i> - analiza obrazu. Zgodnie z najnowszymi ustaleniami literaturowymi, stanowi integralną część GEOINT ⁷ . Uwzględnia badania m.in. obrazów elektrooptycznych, podczerwonych, radarowych i wideo.
MASINT ⁸	Ang. <i>Measurement and Signature Intelligence</i> Wywiad pomiarowo - badawczy. Obejmuje analizę wielu rodzajów danych w różnych typach środowisk. Zgodnie, z poniższym:
ACINT	Ang. <i>Acoustical Intelligence</i> – skupia się przede wszystkim na badaniu sygnałów podmorskich pochodzących zarówno z łodzi podwodnych, jak i innych obiektów ulokowanych pod wodą.
RADINT	Ang. <i>Radar Intelligence</i> – rozpoznanie radiolokacyjne, radiotechniczne.
RINT	Ang. <i>Unintentional Radiation Intelligence</i> Polega na badaniu informacji o niezamierzonej radiacji pochodzącej z różnego rodzaju elektronicznych i elektrycznych obiektów.

⁵ Vide: Benes, Libor. *OSINT, New Technologies, Education: Expanding Opportunities and Threats. A New Paradigm*. Journal of Strategic Security 6, no. 3 Suppl. (2013): 22-37.

⁶ Vide: *Joint Publication 2-01, Joint and National Intelligence Support to Military Operation*, 5 July 2017, s.III-41

⁷ Vide: *Intelligence Sources in the Process of Collection of Information by the U.S. Intelligence Community*, Mariusz Kamiński, Security Dimensions, NO. 32; 2019 (82–105), s. 90-93, DOI:10.5604/01.3001.0014.0988

⁸ *Federation of American Scientists*: <https://fas.org/irp/program/masint.htm>

CBNINT	Ang. <i>Chemical and Biological Intelligence</i> Obejmuje prowadzenie zarówno tradycyjnych analiz chemicznych, jak i materiałów biologicznych, w tym przeprowadzanie zaawansowanych badań w laboratoriach mikrobiologicznych.	
DEWINT	Ang. <i>Directed Energy Weapons Intelligence</i> Wywiad skierowany na badanie broni wiązkowej, różnych aspektów energii kierowanej.	
NUCINT	Ang. <i>Nuclear Intelligence</i> Polega m.in. na monitorowaniu testów jądrowych oraz analizie emisji radioaktywnych próbek.	
EMPINT	Ang. <i>Electromagnetic Pulse Intelligence</i> Badanie impulsu elektromagnetycznego. Oprócz piorunów i wyładowań statycznych, impulsy mogą być generowane przez radar lub broń, stworzoną do niszczenia sprzętu elektronicznego.	
ELECTRO- -OPTINT	Ang. <i>Electro-optical Intelligence</i> – polega na optycznej analizie spektrum elektromagnetycznego od ultrafioletu (0,01 mikrometra) do dalekiej podczerwieni (1000 mikrometrów).	
	LASINT	Ang. <i>Laser Intelligence</i> Podkategoria wywiadu opto-elektronicznego, w ramach której podejmowane są działania na rzecz zbadania sygnałów pochodzących z systemów laserowych.
MATE- RIALS INTELLIG ENCE	Polega na badaniu różnorodnych materiałów: tradycyjnych lub innowacyjnych. W przypadku tych ostatnich coraz powszechniej używa się dedykowanego oprogramowania, które pozwala na zdefiniowanie materiału, a także jego/ich łączenie. Analizie podlega kształt materiału, surowce, z których jest wykonany lub miejsce produkcji.	
IRINT	Ang. <i>Infrared Intelligence</i> Obejmuje gromadzenie i analizowanie danych pochodzących z zakresu podczerwieni.	

Źródło: Opracowanie własne na podstawie strony *Federation of American Scientists (FAS)*.

Wywiad odgrywa kluczową rolę we wspieraniu dowódców w podejmowaniu decyzji w całym zakresie operacji wojskowych. Skuteczność działań wywiadowczych polegających na pozyskiwaniu informacji o zasobach i ruchach przeciwnika zależy od czasu i wiarygodności danych⁹. W trakcie konfliktu zbrojnego szczególnie istotne jest, by informacje wywiadowcze były przekazywane w czasie rzeczywistym. Dowódcy wykorzystują dane wywiadowcze do przewidywania, wizualizacji i zrozumienia sytuacji operacyjnej. Bezpieczeństwo, pojemność i precyzja danych jest niezbędna dla funkcjonowania procesu prowadzenia operacji wojskowych i zarządzania systemem walki.

⁹Sposoby zdobywania informacji [w:] *System rozpoznania Sił Zbrojnych RP. Doświadczenia i wnioski z funkcjonowania ISTAR. Część I. ISTAR jako element systemu walki*, red. naukowa Szymon Markiewicz, Warszawa 2016, red., s. 246-247

W zależności od poziomu działań wojennych, wsparcie wywiadowcze powinno być ukierunkowane na poziom strategiczny, operacyjny lub taktyczny. Aby zapewnić dowódcom pełne zrozumienie sytuacji, oprócz rozpoznania i obserwacji nowych celów lub pojawiających się wysoce prawdopodobnych zagrożeń, analitycy wywiadu muszą również brać pod uwagę i łączyć inne istotne aspekty sytuacji operacyjnej, takie jak czynniki socjokulturowe.

2. Obserwacja jest definiowana jako "(...) systematyczna obserwacja przestrzeni powietrznej, powierzchni lub obszaru pod powierzchnią, miejsc, osób lub rzeczy za pomocą środków wizualnych, podsłuchowych, elektronicznych, fotograficznych lub innych"¹⁰.

Obserwację (nadzór lub śledzenie) można opisać kilkoma przymiotnikami: stabilna, stała, systematyczna. Wszystkie one pozostają aktualne, niezależnie od tego, czy obserwacja dotyczy celu odległego i jest prowadzona z wykorzystaniem wywiadu optoelektronicznego, czy też celu bliskiego, gdzie wykorzystywany jest wywiad sygnałowy. Obserwacja może być również prowadzona przez człowieka, który przez określony czas i we właściwie dobrany sposób śledzi cel.

3. Rozpoznanie definiuje się jako "(...) misję podjętą w celu uzyskania informacji o działaniach lub zasobach przeciwnika (...) lub zabezpieczenia danych dotyczących meteorologicznych, hydrograficznych lub geograficznych cech danego obszaru"¹¹.

Rozpoznanie należy rozumieć, jako konkretną misję skoncentrowaną na zwiadzie terenowym (z wykorzystaniem np. GEOINT, IMINT) lub/i rozpoznaniu siłowym (z wykorzystaniem wszystkich rodzajów wywiadu, które pozwalają na zidentyfikowanie sprzętu, technologii, infrastruktury i innych zasobów wykorzystywanych przez przeciwnika). Rola systemu rozpoznania rośnie, ponieważ poziom technologiczny narzędzi wykorzystywanych do analizy zasobów militarnych i taktyki przeciwnika jest coraz bardziej wymagający.

Istnieją jeszcze dwa pojęcia integrujące wywiad, obserwację i rozpoznanie, które wykraczają poza przytoczone wyżej definicje:

4. ISTAR¹² (Intelligence, Surveillance, Target Acquisition and Reconnaissance), które oprócz zakresu ISR uwzględnia techniki odnajdywania i operowania celami wyznaczonymi do zniszczenia, obejmuje procesy kompleksowej analizy danych. Ma szczególne zastosowanie w wykorzystaniu platform bezzałogowych.

¹⁰ AJP-2.7 *Allied Joint Doctrine for Intelligence, Counterintelligence and Security*, Published by NATO, 2016, s. 2-4

¹¹ Ibidem.

¹² Vide: *Science & Technology Trends 2020-2040*, NATO Science & Technology Organization, Brussels, March 2020, s. 23-78

W odniesieniu do polskiego wdrożenia oczekuje się, że w ramach ISTAR zostanie stworzony system informatyczny do zbierania informacji z różnych źródeł - rozpoznanie patrolowe, dalekiego zasięgu, elektroniczne, obrazowe i osobowe. Informacje te będą następnie analizowane i dystrybuowane na właściwych szczeblach dowodzenia operacyjnego i taktycznego. System ISTAR jest jednym z elementów dowodzenia pozycjami polowymi na szczeblu pułku, brygady i dywizji. Taka konfiguracja przynosi korzyści na poziomie dowodzenia, ponieważ rozpoznaje cel niezależnie od rodzaju wojsk i potwierdza szybko pozyskane dane z różnych źródeł.

5. Pojęcie JISR (Joint Intelligence, Surveillance and Reconnaissance) powstało w odpowiedzi na zwiększające się potrzeby ściślejszej integracji systemów ISR, która została zidentyfikowana zarówno po kampanii na Bałkanach, jak i Afganistanie oraz misji w Libii¹³. Koncentruje się na planowaniu, przetwarzaniu, wykorzystywaniu i rozpowszechnianiu informacji ISR członków NATO i powinna być postrzegana jako zintegrowana działalność łącząca produkty wywiadu, z ciągłą obserwacją (śledzenie) i operacjami zbierania informacji (rozpoznanie).

Analizując podstawowe pojęcia dla obszaru ISR warto również wskazać Plan Synchronizacji ISR, który - dla dowódcy prowadzącego operację - jest najważniejszym elementem integrującym informacje z różnych źródeł. Działania prowadzone przez sztab w trakcie analizy zadania/misji (np. Informacyjne przygotowanie Pola walki (IPB), opracowanie wstępnych danych szacunkowych, wstępny *targeting*) tworzą już na początku wymagania informacyjne/wywiadowcze. Synchronizacja napływających danych z systemów ISR jest kluczowym elementem integracji informacyjnej, która wspiera dowódcę i sztab. Pozwala również m.in. poprawnie ustalać priorytety, monitorować działania przeciwnika, wykorzystać zalety terenu i pogody, określać wpływ ludności cywilnej na prowadzoną operację. W wyniku właściwego opracowania Planu Synchronizacji ISR podwładni w określonym czasie składają meldunki, tworzą i rozpowszechniają do podwładnych informację oraz przekazują przełożonemu w danym czasie informacje wspierające proces dowodzenia. Proces synchronizacji m.in.:

- a. Identyfikuje wymagania informacyjne i wywiadowcze
- b. Identyfikuje luki informacyjne między systemami w zmieniającym się czasie
- c. Dokonuje oceny dostępnych zasobów własnych i przydzielonych dowódcy do operacji
- d. Zapewnia terminowe wykorzystanie zasobów

¹³ NATO/ Multinational Joint Intelligence, Surveillance and Reconnaissance Unit, A feasibility Study, Joint Air Power Competence Centre, Germany, October 2015, s. 1-15

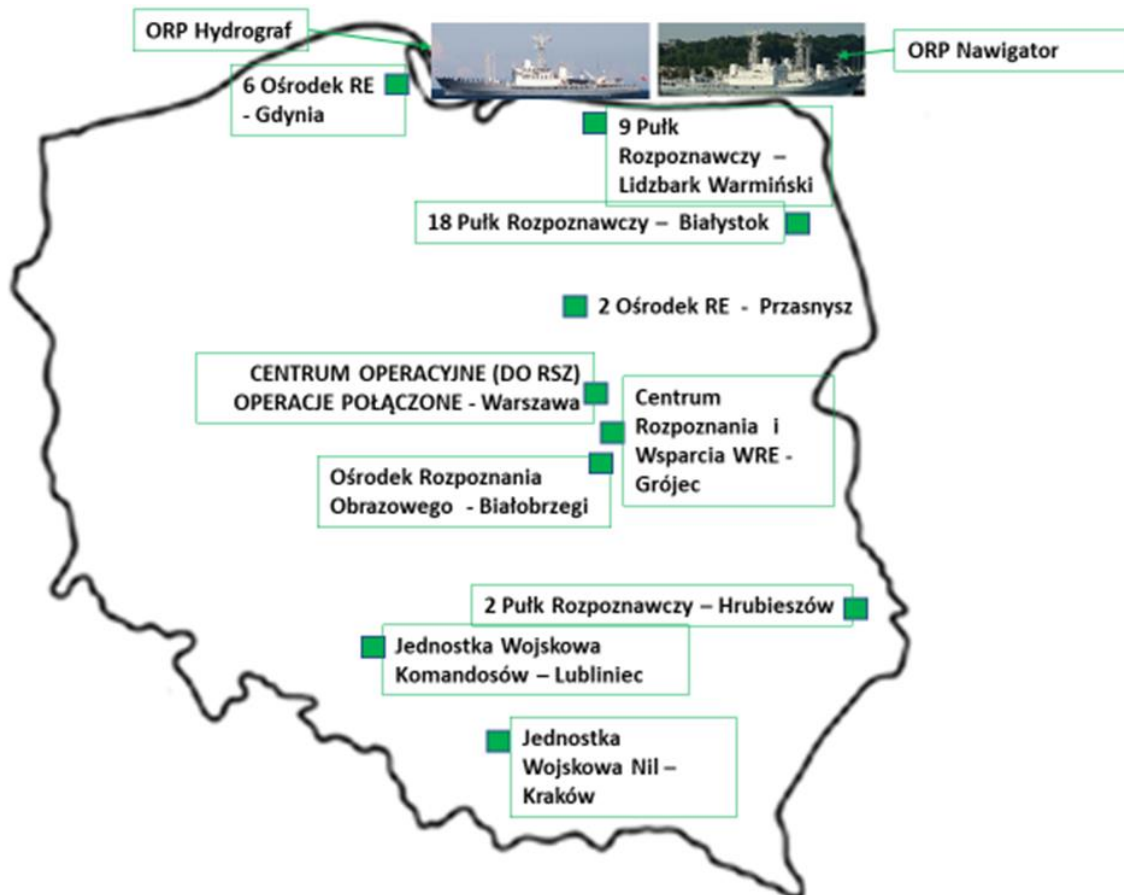
- e. Umożliwia podejmowanie decyzji o tym czy wykorzystywać zasoby własne czy wnioskować do przełożonego o informację z jego zasobów

Wyniki synchronizacji ISR przeprowadzonej podczas analizy zadania/misji prowadzą do wstępnego planu synchronizacji ISR niezbędnego w każdej operacji.

SYSTEMY ISR W POLSKICH SIŁACH ZBROJNYCH

W Polsce, jednostki rozpoznawcze ulokowane zostały w większości we wschodniej części kraju.

Rys. 1. Jednostki rozpoznawcze – stan aktualny.



Źródło: Opracowanie własne. Grafika ORP Navigator: https://pl.wikipedia.org/wiki/ORP_Navigator Grafika ORP Hydrograf: https://pl.wikipedia.org/wiki/ORP_Hydrograf

Podczas operacji stabilizacyjnej w Iraku Polski kontyngent był wspierany „(...)” przez kontyngenty wojskowe z innych państw koalicji. W zakresie prowadzonej operacji ujawniły się braki polskiej armii, szczególnie w zakresie rozpoznania osobowego, a także niedocenianego rozpoznania patrolowego. Potencjał rozpoznawczy dywizji ulegał ciągłemu zmniejszeniu podczas kolejnych zmian polskiego kontyngentu wojskowego. Spowodowane to było głównie wycofywaniem się kolejnych kontyngentów wojskowych państw uczestniczących w wsparciu i zastępowaniem jednostek

rozpoznawczych jednostkami bojowymi. Można stwierdzić, że posiadany potencjał rozpoznawczy był zdecydowanie za mały w stosunku do ilości zadań stawianych przed systemem rozpoznania"¹⁴.

Inaczej wyglądała sytuacja w trakcie misji w Afganistanie. Polski kontyngent brał udział w działaniach stabilizacyjnych, wśród których najważniejsze było rozpoznanie i patrolowanie. Większe wykorzystanie bezzałogowych statków powietrznych na poziomie dowodzenia taktycznego i operacyjnego wymagało nowych możliwości pozwalających na sprawne i dokładne pozyskiwanie oraz przetwarzanie danych obrazowych. Dzięki temu wzrosło zrozumienie konieczności wykorzystania w misjach wojskowych obszaru ISR.

Obecnie w procesie planowania i prowadzenia operacji istotną kwestią jest spełnienie wymagań stawianych Dowództwu Operacyjnemu Sił Zbrojnych oraz Dowództwom innych komponentów - jednostek zależnych. Informacje pozyskiwane m.in. z ISR lub instytucji współdziałających są niezbędne do planowania na poziomie operacyjno-strategicznym oraz podczas realizacji operacji. Biorąc to pod uwagę, najważniejsze dla procesu decyzyjnego są czas i dostęp do właściwych informacji.

Nadmiar danych i faktów generowanych z wielu źródeł, w tym przez instytucje i agendy współdziałające z wojskiem, może utrudniać ich terminowe przetwarzanie. Z tego powodu kluczowe znaczenie ma możliwość znalezienia i dostarczenia ważnych informacji w pożądanym czasie¹⁵. W tym celu budowany jest zintegrowany system gromadzenia, przetwarzania i wymiany danych/informacji. Jego opracowanie jest jednak bardzo trudne ze względu na specyfikę systemów rozpoznania (rozpoznanie na poziomie patroli, pododdziałów, artylerii, sił powietrznych, rozpoznanie bliskie i dalekie itp.) oraz rozproszoną architekturę systemów.

Znaczenie i konieczność wdrożeń ISR w Siłach Zbrojnych RP znalazło swoje odzwierciedlenie w Planie Modernizacji Technicznej, w którym przewidziano następujące systemy i przedsięwzięcia:

- a. System informatyczny do gromadzenia, analizy i dystrybucji informacji ze wszystkich elementów ISTAR (rozpoznania patrolowego, dalekiego zasięgu, elektronicznego, obrazowego i osobowego) – kryptonim SOWA. Jego zadaniem będzie przyjmowanie i dystrybucja wszystkich wiadomości rozpoznawczych mogących mieć istotne znaczenie dla prowadzonych działań oraz wsparcie informacyjne dowództw w zakresie zapewnienia

¹⁴ Zbigniew Modrzejewski, Piotr Balon, *System rozpoznania w operacjach poza granicami kraju*, Akademia Sztuki Wojennej, Warszawa 2017, s. 124-125

¹⁵ *Sposoby zdobywania informacji [w:] System rozpoznania Sił Zbrojnych RP. Doświadczenia i wnioski z funkcjonowania ISTAR. Część I. ISTAR jako element systemu walki*, red. naukowa Szymon Markiewicz, Akademia Sztuki Wojennej. - Warszawa : Wydawnictwo Akademii Sztuki Wojennej, 2016., s.246-247

zdolności bojowej i bezpieczeństwa wojsk z wykorzystaniem zautomatyzowanych systemów dowodzenia,

- b. Zautomatyzowany system zbierania, przetwarzania i dystrybucji wiadomości rozpoznawczych otrzymywanych z elementów rozpoznania dalekiego zasięgu – kryptonim PAJĄK,
- c. Lekkie opancerzone pojazdy rozpoznawcze – kryptonim KLESZCZ,
- d. Pojazdy rozpoznawcze dla jednostek rozpoznania dalekiego zasięgu – kryptonim ŻMIJA,
- e. Mobilne bezzałogowe pojazdy rozpoznawcze (MBPR) – kryptonim TARANTULA.

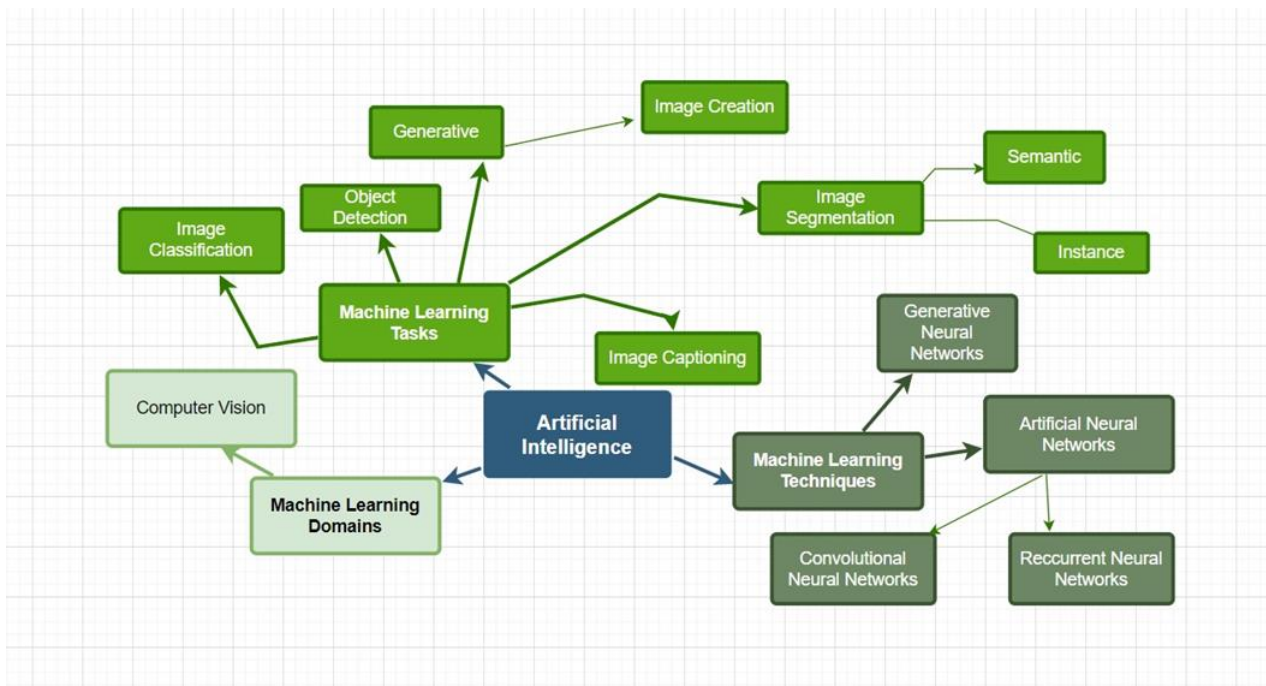
ANALIZA OBRAZU

Kolejnym zagadnieniem, które warto poruszyć w kontekście systemów ISR jest postęp technologiczny i komercyjny środków i narzędzi, które mają wpływ na skuteczność i efektywność ISR. Należy mieć świadomość ich dynamicznego rozwoju na rynku cywilnym. Coraz większa dostępność tego typu rozwiązań może stanowić zagrożenie dla bezpieczeństwa systemów wojskowych. Oznacza to potrzebę zwiększenia ochrony tych rozwiązań.

Przykładem szybkiej i problematycznej ewolucji jest analiza obrazu, która wymaga ciągle bardziej wyrafinowanych instrumentów.

Historia analizy obrazu i jej automatyzacji ma już kilkadziesiąt lat, jednak największa rewolucja nastąpiła w ciągu ostatnich dziesięciu lat dzięki *computer vision* i sztucznym sieciom neuronowym (*Artificial Neural Networks* - ANN), wśród których najbardziej efektywne w znajdowaniu wzorców na obrazie są sieci konwolucyjne (*Convolutional Neural Networks* - CNN).

Rys. 2. Umieszczenie analizy obrazu w dziedzinach, technikach i zadaniach sztucznej inteligencji (ang. *Artificial Intelligence* – AI)



Źródło: Opracowanie własne, częściowo na podstawie Aurelien Geron, *Hands-On Machine Learning with Scikit-Learn, Keras and Tensorflow: Concepts, Tools and Techniques to Build Intelligent Systems, 2nd Edition*, Helion S.A. 2020

Konwolucja, będąc złożonym aparatem matematycznym, pozwala na sprawne wydobycie cech z obrazów. Najbardziej znane architektury konwolucyjnych sieci neuronowych to (chronologicznie): LeNet (zaproponowana przez Yanna LeCuna i in. w 1989 roku), AlexNet (zaproponowana w 2012 roku, w pracy badawczej o nazwie „*Imagenet Classification with Deep Convolution Neural Network*” przez Alexa Krizhevsky'ego, Ilyę Sutskevera i Geoffreya E. Hinton), GoogLeNet (zaproponowana przez Google we współpracy różnych uniwersytetów w 2014 roku w pracy badawczej o nazwie „*Going Deeper with Convolutions*”), VGGNet (architektura sieci VGG została wprowadzona przez Simonyana i Zisserman w pracy z 2014 roku „*Very Deep Convolutional Networks for Large Scale Image Recognition*”), ResNet (stworzona przez He i in., która wygrała konkurs ImageNet w 2015 roku).

Analiza obrazu najczęściej jest prowadzona przez grupy analityczne, które dokonują klasyfikacji, lokalizacji lub detekcji obiektów. W zależności od celu pracy analitycznej stosuje się różne algorytmy i różne sieci neuronowe. Najpopularniejszymi algorytmami detekcji, stosowanymi obecnie są:

1. Algorytm *Faster R-CNN*, który dziedziczy po całej rodzinie algorytmów (*RCNN* i *Fast RCNN*) najlepsze parametry i uwzględnia dalsze ulepszenia. Oparty jest na ROI (*Region of Interest Pooling*).

2. Rodzina YOLO ("*You Only Look Once*") - algorytm rozpoznawania obiektów w czasie rzeczywistym pozwalający na szybką detekcję i umożliwiający przeprowadzanie obliczeń na niskim poziomie z zadowalającą dokładnością. Wykorzystuje on tylko jedną propagację przez sieć.
3. SSD (*Single Shot MultiBox Detector*) - klasyfikuje obiekty, które wcześniej zostały wykryte i zlokalizowane.

Problematyka sztucznej inteligencji i jej sieci neuronowych jest coraz szerzej i częściej opisywana naukowo. Obecnie największym wyzwaniem dla analizy obrazu nie jest zdefiniowanie obserwowanego obiektu, ale właściwe sklasyfikowanie zdarzenia, które pozwoli na kompleksową ocenę sytuacji. Z jednej strony, bardziej zaawansowana analiza powinna ujawnić przykładowo czy grupa ludzi wokół obiektu to osoby cywilne czy wojskowi i czy obiekt zmienił położenie czy też należy do krajobrazu na stałe. W tym celu wykorzystywana jest „inteligencja rozszerzona (ang. *augmented intelligence*)” stanowiąca połączenie AI i analizy prowadzonej przez człowieka. Pozwala to skupić się na istotnych zdarzeniach i pogłębić analizę o nowe, nieopisane jeszcze w systemach dane (jak warunki atmosferyczne lub stan obiektów).

Z drugiej strony, warto podkreślić, że mimo iż algorytmy detekcji są dziś podstawowym elementem prowadzenia rozpoznania obrazowego (w przypadku dużej ilości danych) to nadal muszą być objęte oceną człowieka. Może to wpływać na interpretację sytuacji i jej klasyfikację. Zmniejszenie stroniczości w mechanizmach AI jest trudne i opiera się na wielokrotnej weryfikacji modeli, ich ciągłej aktualizacji i zwiększaniu dokładności.

Mając powyższe na względzie i oceniając postęp technologiczny w obszarze analizy obrazu należy mieć na uwadze fakt, że pole walki i przegrupowania sił mogą zmieniać się na tyle dynamicznie, że ograniczenia AI (opisane powyżej, jak brak bieżącego kontekstu i wiedzy o najnowszych wydarzeniach) nie pozwolą na właściwą analizę i interpretację wyników. Dodatkowo, dostęp i pozyskanie wysokiej jakości zdjęć i filmów jest dziś możliwe z poziomu tanich urządzeń kompaktowych, takich jak telefony komórkowe. Zwiększyła się również liczba ogólnodostępnych i darmowych narzędzi, które pozwalają na modyfikację obrazu. To oznacza, że w kolejnych latach poziom możliwości obróbki obrazu może być na tyle istotny, że będzie pozwalał na zamianę obrazu i przesyłanie fałszywych danych. A przecież informacje zebrane z obrazów są przekazywane na szczebel dowodzenia. Muszą być pewne i wiarygodne. Nie jest to jeszcze możliwe przy wykorzystaniu sztucznej inteligencji jako jedyne źródła. Z tego powodu - niezależnie od postępu technologicznego

– czynnik ludzki będzie w dalszym ciągu integralnym elementem prowadzenia rozpoznania wojskowego.

Będąc w obszarze analizy obrazu warto odnieść się do koncepcji *Coalition Shared Data (CSD)*¹⁶, czyli koncepcji i wdrożenia elastycznej architektury NATO umożliwiającej wymianę danych w określonym standardzie, w celu wsparcia wszystkich poziomów dowodzenia. „Tylko w zakresie rozpoznania obrazowego, gdzie występuje duża różnorodność źródeł informacji, konieczne było opracowanie szeregu standardów, tj.:

- a. STANAG 7023 - który dotyczy formatu danych obrazów pierwotnych,
- b. STANAG 4545 - dotyczący formatu danych obrazów wtórnych,
- c. STANAG 4607 - dotyczy formatu danych GMTI (*Ground Moving Target Indicator*),
- d. STANAG 4609 - dotyczący formatu danych wizyjnych uzyskiwanych z sensorów EO / IR (*Electro-Optical / Infrared*).

Świadomość problemów związanych z zapewnieniem interoperacyjności w rozpoznawaniu obrazowym doprowadziła do opracowania standardu STANAG 4559 (*NATO Standard ISR Library Interface - NSIL*), w którym zdefiniowano interfejs umożliwiający dostęp w koalicji środowiskowej do wszystkich bibliotek danych ISR oraz narodowych baz danych, w których przechowywane są produkty powstałe w wyniku rozpoznawania obrazów¹⁷.

Komercyjną implementacją STANAG 4559, jest projekt dotyczący systemu przechowywania i rozpowszechniania zasobów wywiadu, obserwacji i rozpoznania o nazwie *Coalition Shared Data server*. W ramach tego projektu rozwijana jest „(...) seria systemów do kompilacji informacji z wielu różnych źródeł w różnych formatach (klipy wideo, zdjęcia, radary itp.), dostarczających analitykom wywiadu niezbędnych narzędzi do wymiany informacji ISR i przepływu pracy (...)”¹⁸.

Integracja z serwerem CSD stanowi wyzwanie dla polskich rozwiązań. Klauzula tajności NATO oznacza, że polskie systemy muszą być budowane z uwzględnieniem tego poziomu bezpieczeństwa informacji.

W Polsce jednostką wojskową odpowiedzialną za zarządzanie całym podsystemem rozpoznania obrazowego, zapewniającym zdolność do przetwarzania i analizy danych obrazowych oraz prowadzenia kompleksowych ocen środowiska bezpieczeństwa, przy wykorzystaniu danych

¹⁶ *Distributed Information Management through Coalition Shared Data*, Barbara Essendorfer, Achim Kuwertz, Jennifer Sander, The Science and Technology Organization, Fraunhofer IOSB, Germany, s.1-6

¹⁷ *Gromadzenie i wymiana danych rozpoznawczych w aspekcie wymagań NATO*, J. Milewski, P. Kaniewski, R. Urban., XI Konferencja Naukowo-Techniczna, Systemy Rozpoznania i Walki Radioelektronicznej 2016, Ołtarzew, 21 – 23.11.2016r., s. 5.

¹⁸ „CSD”, https://www.gmv.com/DocumentosPDF/csd/CSD_ENG.PDF

obrazowych pozyskiwanych z różnych systemów rozpoznawczych jest Ośrodek Rozpoznania Obrazowego (ORO) w Białobrzegach.

PODSUMOWANIE

NATO stoi w obliczu istotnych zmian w sztuce osiągnięcia celów militarnych, szczególnie biorąc pod uwagę złożoność środowiska operacji wojskowych. Kluczowe znaczenie dla sprawności realizowanych celów Sojuszu ma właściwe zrozumienie i wykorzystanie aplikacji i implementacji ISR. Jednocześnie, wyzwaniem dla NATO jest również niezwykle dynamiczny rozwój domeny cybernetycznej, która stanowi bezpośrednie zagrożenie dla poprawnego funkcjonowania wszystkich systemów, procedur i zastosowań ISR. Atak dronów na dwie kluczowe instalacje naftowe na terenie Arabii Saudyjskiej w 2019 roku pokazał, jak krucha jest infrastruktura bezpieczeństwa. Rozwój technologiczny rozwiązań informatycznych nigdy wcześniej nie był tak dynamiczny jak obecnie. Wykorzystanie wszystkich rodzajów inteligencji, takich jak analiza obrazu, prowadzi do pozyskania informacji czasu rzeczywistego, które należy odpowiednio przetworzyć i wykorzystać. Potrzeba lepszych algorytmów do ekstrakcji najlepszych i użytecznych informacji wciąż rośnie. Istnieje już wiele aplikacji typu *open-source*, które opracowują dostępne dane dla celów komercyjnych. Z drugiej strony zdarzają się konflikty, szczególnie te angażujące siły partyzanckie, których przebieg będzie możliwy do zweryfikowania i oceny jedynie poprzez zasoby ludzkie na miejscu zdarzenia. Z obserwacji różnych misji wynika, że rozwój technologiczny spowodował, iż w różnych krajach lokalne grupy partyzanckie opracowały systemy komunikacji potrafiące wprowadzić skutecznie w błąd systemy teleinformatyczne i polegają wyłącznie na kontakcie bezpośrednim. Wbrew rozwojowi technologii, to zwiększyło znaczenie udziału człowieka w wybranych operacjach wywiadowczych.

W związku z powyższym kluczowym dla Sił Zbrojnych RP i ich zasobów jest - biorąc również pod uwagę ostatnie doświadczenia z misji w Iraku i Afganistanie - rozwój zdolności, narzędzi i sprzętu rozpoznawczego. Musi być on dostosowany do poziomu rozwiązań stosowanych w innych państwach członkowskich NATO. Informacje o położeniu wojsk i infrastruktury to tylko część obrazu pola walki. Najważniejszym jest, by tego typu dane były dostępne i analizowane w czasie rzeczywistym. Równie ważne są systemy ISR, które pozwalają przewidzieć ruchy przeciwnika. To ostatnie może zdecydować o wygraniu lub przegraniu nie tylko bitwy, ale i wojny.

Poza koniecznością rozbudowywania istniejących systemów ISR, zwłaszcza z uwagi na narastanie nowych konfliktów w Europie, takich jak ten między Rosją a Ukrainą, należy rozszerzać bieżące

rozwiązania o kolejne obszary¹⁹. Polska pozyskuje rakiety HIMARS (*High Mobility Artillery Rocket System*) o dalekim zasięgu oraz deklaruje zakup samolotów piątej generacji F-35. Oznacza to konieczność integracji systemów analizy obrazowej z systemami satelitarnymi, radarowymi oraz powietrznymi. Biorąc pod uwagę krytyczne znaczenie zagrożeń z powietrza, Polska w przyszłości powinna zastanowić się również nad posiadaniem własnych samolotów wczesnego ostrzegania i kontroli przestrzeni powietrznej AEW&C (*Airborne Early Warning and Control*). Nie bez znaczenia pozostaje również rozstrzygnięcie postępowania na pozyskanie „Systemu Analizy Obrazowej”, który sojusznicy w NATO rozwijają już od lat.

BIBLIOGRAFIA **REFERENCES LIST**

PIŚMIENICTWO **LITERATURE**

- Aleksander Iwanowicz Kuk, *Kanwa wywiadu agenturalnego. Podstawy wywiadu osobowego*, Akademia Sztuki Wojennej, Warszawa 2020r.
- K. Danielewicz, *Komórka sztabowa 2X w operacji typu COIN – wybrane zagadnienia*, Przegląd Bezpieczeństwa Wewnętrznego 8/13.
- Gromadzenie i wymiana danych rozpoznawczych w aspekcie wymagań NATO*, J. Milewski, P. Kaniewski, R. Urban, XI Konferencja Naukowo-Techniczna, Systemy Rozpoznania i Walki Radioelektronicznej 2016, Ołtarzew, 21 – 23.11.2016.
- Zbigniew Modrzejewski, Piotr Balon, *System rozpoznania w operacjach poza granicami kraju*, Akademia Sztuki Wojennej, Warszawa 2017.
- Intelligence Sources in the Process of Collection of Information by the U.S. Intelligence Community*, Mariusz Kamiński, Security Dimensions, NO. 32; 2019 (82–105), s. 90-93, DOI:10.5604/01.3001.0014.0988.
- Hands-On Machine Learning with Scikit-Learn, Keras and Tensorflow: Concepts, Tools and Techniques to Build Intelligent Systems*, Aurelien Geron, 2nd Edition, Helion S.A. 2020.
- Joint Publication 2-01, *Joint and National Intelligence Support to Military Operation*, 5 July 2017.
- AJP-2.7 Allied Joint Doctrine for Intelligence, Counterintelligence and Security*, Published by NATO, 11 July 2016.
- Roger Faligot, Remy Kauffer, *Służby specjalne. Historia wywiadu i kontrwywiadu na świecie*, Wyd. ISKRY, Warszawa 2006.

¹⁹ Vide: Kierunki rozwoju. Główne cele rozwoju systemu rozpoznania wojskowego, [w:] *System rozpoznania Sił Zbrojnych RP : doświadczenia i wnioski z funkcjonowania ISTAR. Cz. 2, Rozpoznanie specjalistyczne*, red. nauk. Jarosław Wiśniewski ; Akademia Sztuki Wojennej. - Warszawa : Wydawnictwo Akademii Sztuki Wojennej, 2016.

Sposoby zdobywania informacji [w:] System rozpoznania Sił Zbrojnych RP. Doświadczenia i wnioski z funkcjonowania ISTAR. Część I. ISTAR jako element systemu walki, red. naukowa Szymon Markiewicz, Akademia Sztuki Wojennej. - Warszawa : Wydawnictwo Akademii Sztuki Wojennej, 2016.

Distributed Information Management through Coalition Shared Data, Barbara Essendorfer, Achim Kuwertz, Jennifer Sander, The Science and Technology Organization, Fraunhofer IOSB, Germany.

Główne cele rozwoju systemu rozpoznania wojskowego, [w:] System rozpoznania Sił Zbrojnych RP : doświadczenia i wnioski z funkcjonowania ISTAR. Cz. 2, Rozpoznanie specjalistyczne, red. nauk. Jarosław Wiśniewski ; Akademia Sztuki Wojennej. - Warszawa : Wydawnictwo Akademii Sztuki Wojennej, 2016.

Benes, Libor. *OSINT, New Technologies, Education: Expanding Opportunities and Threats. A New Paradigm*. Journal of Strategic Security 6, no. 3 Suppl. (2013): 22-37.

Science & Technology Trends 2020-2040, NATO Science & Technology Organization, Brussels, March 2020.

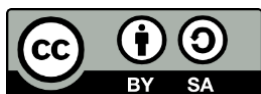
NATO/ Multinational Joint Intelligence, Surveillance and Reconnaissance Unit, A feasibility Study, Joint Air Power Competence Centre, Germany, October 2015.

ŹRÓDŁA SOURCES

Dokument pdf na stronie firmy GMV, https://www.gmv.com/DocumentosPDF/csd/CSD_ENG.PDF (dostęp: 16.12.2019)
Strona Federation of American Scientists: <https://fas.org/irp/program/masint.htm> (dostęp: 29.01.2021)



Copyright (c) 2021 Kamila MATELA



This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.