Zeszyty Naukowe AON nr 2(95) 2014
ISSN 2299-6753

ZASADY ROZPOZNANIA WOJSKOWEGO

płk dr inż. Jarosław WIŚNIEWSKI
Akademia Obrony Narodowej

Abstract

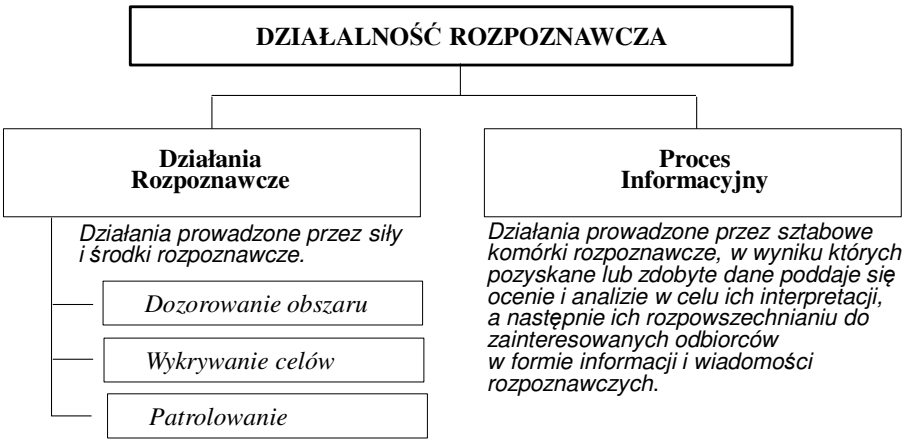
In the light of revision of Polish national doctrine D/2 Rozpoznanie wojskowe (Military Intelligence) it is worth to reconsider not only specific issues, what military society expects but also general conditions. As such, intelligence principles are found. The basis for considerations presented in the article are doubts connected with full implementation of Allied intelligence principles for national purposes in the original release of the doctrinal document. Is this what we consider as an interoperability? What about other national examples? The article articulates review of Polish, NATO, United States and Canada solutions to build up a set of requirements/rules/principles of intelligence as a basis to develop own (national) solutions.

Key words – intelligence, principles, interoperability, NATO and national approaches.

Obecne prace nad nowelizacją doktryny *D/2 Rozpoznanie wojskowe* skłaniają do refleksji na jej zawartością i kierunkami zmian. Przyjęte bowiem i w tej chwili obowiązujące rozwiązania ograniczają się w dużym zakresie do „suchego" przełożenia rozwiązań sojuszniczych i próby zaadaptowania ich na grunt narodowy. Skutek nie wydaje się pozytywny, gdyż po upływie niespełna roku od jej wprowadzenia rozpoczęły się prace nad nową wersją dokumentu.

Niemal powszechną jest opinia, iż dogłębne rozpatrywanie kwestii ogólnych nie jest rzeczą pożądaną przez odbiorców dokumentów doktrynalnych, którzy oczekują często bardzo konkretnych rozwiązań. Jednak zarówno ranga dokumentu (najwyższy poziom), jak i problematyka, którą porusza niniejszy artykuł upoważnia ją do zabrania głosu właśnie w tego rodzaju kwestii – są nią zasady rozpoznania. Jak już zostało powiedziane, aktualne uwarunkowania obowiązujące w Siłach Zbrojnych RP w tej kwestii zaczerpnięte zostały całkowicie z rozwiązania sojuszniczego. Czy faktycznie taka sytuacja powinna mieć miejsce, czy spojrzeliśmy na inne wzorce? Może warto dokonać szerszej analizy, wypracowując własne stanowisko. Zwłaszcza że przedmiotowe zasady znajdują swoje zastosowanie lub odniesienie w pełnym zakresie zawartości pojęcia *działalność rozpoznawcza*, znajdując swoje zastosowanie zarówno w procesie informacyjnym, jak i działaniach rozpoznawczych (rysunek 1). Implementować

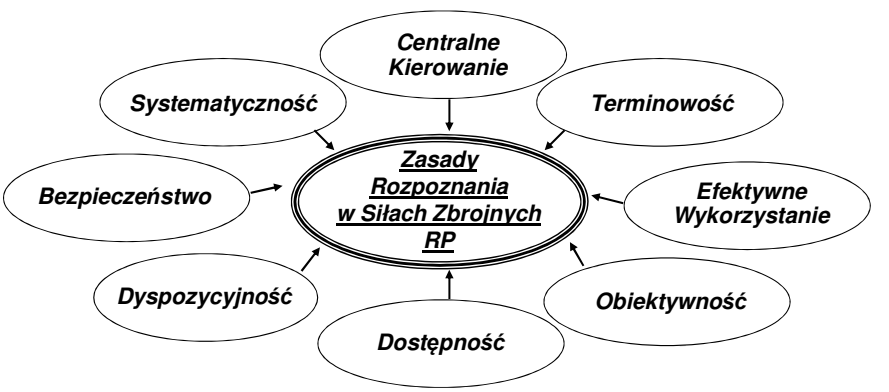
je zatem będą zarówno oficerowie sztabowych pionów rozpoznawczych wszystkich szczebli w ramach ukierunkowania, przetwarzania i upowszechniania, ale również ci, którzy w ramach działań rozpoznawczych będą dane, fakty i informacje pozyskiwać[1].



Źródło: Opracowanie własne na podstawie *Doktryna Rozpoznanie Wojskowe, D/2,* SGWP, Warszawa 2013, s. 9.

Rys. 1. Działalność rozpoznawcza w Siłach Zbrojnych RP

Obowiązujące wydawnictwo doktrynalne definiuje zasady rozpoznania wojskowego jako *obowiązujące normy postępowania w zakresie przygotowania i prowadzenia działalności rozpoznawczej*[2]. Zalicza się do nich osiem elementów przedstawionych na rysunku 2.



Źródło: opracowanie własne na podstawie *Doktryna Rozpoznanie Wojskowe, D/2,* SGWP, Warszawa 2013, s. 21–22.

Rys. 2. Zasady rozpoznania w Siłach Zbrojnych RP

[1] Cykl rozpoznawczy składając się z czterech faz: 1) ukierunkowanie, 2) gromadzenie, 3) przetwarzanie oraz 4) rozpowszechnianie opisuje szczegółowo *Doktryna Rozpoznanie wojskowe, D/2*, SGWP, Warszawa 2013, s. 22-32.

[2] *Doktryna Rozpoznanie wojskowe, D/2* …(2013), wyd. cyt., s. 21.

Centralne kierowanie. Działalność rozpoznawcza musi być centralnie kierowana i koordynowana przez sztabowe komórki rozpoznawcze w celu uniknięcia luk w zbieraniu informacji i niepożądanego dublowania zadań oraz zapewnienia wzajemnego wsparcia, skutecznego i ekonomicznego wykorzystania potencjału rozpoznawczego.

Terminowość. Dokładne i wiarygodne informacje rozpoznawcze są bezwartościowe, jeżeli zostaną dostarczone do użytkownika zbyt późno. Kolejność stawiania zadań musi uwzględniać zmiany sytuacji tak, aby przepływ informacji, wiadomości rozpoznawczych odbywał się bez opóźnień.

Efektywne wykorzystanie. System rozpoznania powinien być konfigurowany w sposób modułowy, stosownie do rodzaju, miejsca i czasu trwania działań. Potencjał rozpoznawczy musi być wykorzystywany zgodnie z ich przeznaczeniem. Zadania dla elementów wykonawczych systemu powinny być zawsze adekwatne do ich możliwości.

Obiektywność. Napływające informacje muszą być bezstronnie ocenione i porównane, tak by uniemożliwić próby dostosowywania wiadomości rozpoznawczych do wcześniej podjętej koncepcji działań.

Dostępność. Informacje i wiadomości rozpoznawcze muszą być udostępnione sztabowym komórkom rozpoznawczym i innym użytkownikom, zgodnie z ich potrzebami w wymaganym czasie. Wiadomości rozpoznawcze są bezwartościowe, jeżeli nie są dostarczone do tych osób funkcyjnych (komórek organizacyjnych), które je wykorzystają.

Dyspozycyjność. Elementy systemu rozpoznania muszą prowadzić działalność w sposób ciągły, zachowując zdolność do realizacji zadań stawianych przez dowódcę.

Bezpieczeństwo. Źródła informacji oraz potencjał rozpoznawczy muszą być właściwie chronione. Wymóg ten nabiera szczególnego znaczenia w stosunku do elementów wykonawczych systemu, działających w ugrupowaniu przeciwnika, i elementów rozpoznania osobowego.

Systematyczność. Wiadomości rozpoznawcze muszą być weryfikowane i uaktualniane w sposób ciągły. Należy uwzględniać przy tym nowe informacje oraz porównywać je z już posiadaną wiedzą[3].

Biorąc pod uwagę powyższą interpretację zasad rozpoznania, warto nadmienić, iż zostały one zaadaptowane na grunt Sił Zbrojnych RP z pierwowzoru wyartykułowanego w doktrynie sojuszniczej AJP-2 (2003)[4]. Taką właśnie intencję zawiera wprowadzenie (wstęp) zawarte w dokumencie narodowym[5]. Zestawienie narodowych i sojuszniczych (w oryginalnym brzmieniu) zasad rozpoznania zawiera tabela 1.

Pewną refleksję może wzbudzać fakt przyjmowania rozwiązań, nie tylko zresztą w zakresie zasad prowadzenia rozpoznania, sprzed 10 lat.

[3] Tamże, s. 21–22.

[4] AJP-2, *Allied Joint Intelligence, Counter-Intelligence and Security Doctrine*, NATO Standardization Agency 2003, s. 1-3-1.

[5] *Doktryna Rozpoznanie wojskowe, D/2* …(2013), wyd. cyt., s. 5.

Tabela 1

Ujęcie narodowe i sojusznicze zasad rozpoznania

Lp.	Zasady rozpoznania w wersji narodowej, D/2 (2013)	Zasady rozpoznania w wersji sojuszniczej, AJP-2 (2003)
1.	Centralne kierowanie	Centralised Control
2.	Terminowość	Timeliness
3.	Efektywne wykorzystanie	Systematic Exploitation
4.	Obiektywność	Objectivity
5.	Dostępność	Accessibility
6.	Dyspozycyjność	Responsiveness
7.	Bezpieczeństwo	Source Protection
8.	Systematyczność	Continuous Review

Źródło: opracowanie własne na podstawie *Doktryna Rozpoznanie Wojskowe, D/2,* SGWP, Warszawa 2013, s. 21–22 oraz AJP-2*, Allied Joint Intelligence, Counter-Intelligence and Security Doctrine*, NATO Standardization Agency 2003, s. 1-3-1.

Zważywszy na założoną analogię (co zdaniem autora nie jest złym rozwiązaniem), pewne wątpliwości budzi odniesienie pojęć powyższego zestawienia na poziomie 3 i 6. *Systematic Exploitation* (poz. 3 tabeli 1) odnosi się do systematycznego wykorzystywania sił i środków rozpoznania (źródeł i agencji) poprzez ciągłe obarczanie zadaniami, poparte gruntowną znajomością ich możliwości i ograniczeń[6]. Natomiast *Responsiveness* (poz. 6 tabeli 1 w brzmieniu narodowym *Dyspozycyjność*) stanowi raczej o zdolności działalności rozpoznawczej *(ang.: Intelligence)* do zmian, jakie niosą ze sobą wymagania dowódcy, zmieniające się w odniesieniu do sytuacji[7] (przecelowanie wysiłku). Przedstawione przykłady dowodzą, iż pozostając wierni ideałom rozpoznawczym Sojuszu, uwzględniamy narodowe implikacje.

NATO nie posiada autonomicznych sił oraz środków rozpoznania, a w przypadku prowadzenia operacji korzysta zarówno z wydzielonych, jak i narodowych zdolności rozpoznawczych, dlatego też potencjał rozpoznawczy NATO muszą tworzyć zintegrowane i kompatybilne ze sobą podsystemy narodowe państw członkowskich. Warunkiem takiego podejścia jest wymaganie, aby narodowe systemy i podsystemy rozpoznawcze posiadały jednakowe zdolności operacyjne, które w NATO określane są skrótem ISTAR *(ang.: **I**ntelligence, **S**urveillance, **T**arget **A**cquisition and **R**econnaissance)*. ISTAR jest definiowany jako operacyjna działalność rozpoznawcza, która integruje i synchronizuje planowanie oraz użycie potencjału rozpoznawczego z procesem informacyjnym, czyli gromadzeniem i przetwarzaniem danych faktów i informacji oraz rozpowszechnianiem wiadomości rozpoznawczych[8].

Termin ISTAR jest używany zarówno w odniesieniu do procesów operacyjnych, jak również personelu zaangażowanego w ten proces, dlatego też należy go rozpatrywać w dwóch aspektach: rzeczowym – potencjał rozpoznawczy oraz czynnościowym – wspominana już działalność rozpoznawcza.

[6] AJP-2, *Allied Joint Intelligence ... (2003), wyd. cyt.,* s. 1-3-1.

[7] Tamże.

[8] *Doktryna Rozpoznanie wojskowe, D/2* …(2013), wyd. cyt., s. 34–35.

Zasady działalności (systemu) ISTAR w zasadzie pokrywają się z zasadami rozpoznania, jednakże w przypadku tych pierwszych należy wyróżnić dodatkowo[9]:

− *ukierunkowanie przez dowódcę.* Ukierunkowanie wysiłku ISTAR musi być realizowane przez dowódcę na każdym szczeblu dowodzenia. Jeśli dowódca nie określi swoich wymagań dotyczących zasadniczych informacji, nie otrzyma wiadomości rozpoznawczych niezbędnych do podjęcia decyzji i prowadzenia operacji;

− *modułowa konfiguracja potencjału.* Dostępność szerokiego spektrum zdolności rozpoznawczych (potencjału rozpoznawczego) zapewnia dowódcy elastyczność operacyjną w zakresie doboru odpowiednich środków dla pozyskania wymaganych informacji. Ponadto umożliwia takie planowanie użycia potencjału rozpoznawczego, które zapewni zarówno wysoką efektywność procesu pozyskiwania informacji, jak i utrzymanie odpowiedniego tempa operacji (działań). System ISTAR powinien mieć modułową budowę, umożliwiającą konfigurację jego elementów adekwatnie do potrzeb operacji (działań), czyli rodzaju wykonywanych zadań oraz miejsca, czasu i rodzaju konfliktu;

− *sieciocentryczność.* Do zabezpieczenia świadomości sytuacyjnej dowódcy niezbędna jest zintegrowana i dopasowana do potrzeb sieć zbierania informacji i wiadomości rozpoznawczych. Żeby spełnić wymagania informacyjne dowódcy, sieć ta powinna zapewniać dostęp nie tylko do informacji i wiadomości rozpoznawczych pochodzących z własnych źródeł i instytucji, ale także z innych, w tym strategicznych, systemów zbierania informacji oraz źródeł narodowych, wielonarodowych i sojuszniczych[10].

Wraz z opublikowaniem w ubiegłym roku nowej wersji doktryny sojuszniczej dotyczącej działalności rozpoznawczej w wersji tzw. *projektu ratyfikacyjnego* (ang.: *Ratification Draft)* Sojusz przyjmuje nowe podejście do pryncypiów jej prowadzenia, tym razem wyraźnie zaznaczając, iż są one pochodną wytycznych w tym zakresie komitetu wojskowego *(ang.: Military Committee) MC 0128/8 – Policy Guidance for NATO Intelligence*[11]. Nowe, aktualne podejście w zakresie zasad działalności rozpoznawczej przedstawia rysunek 3.

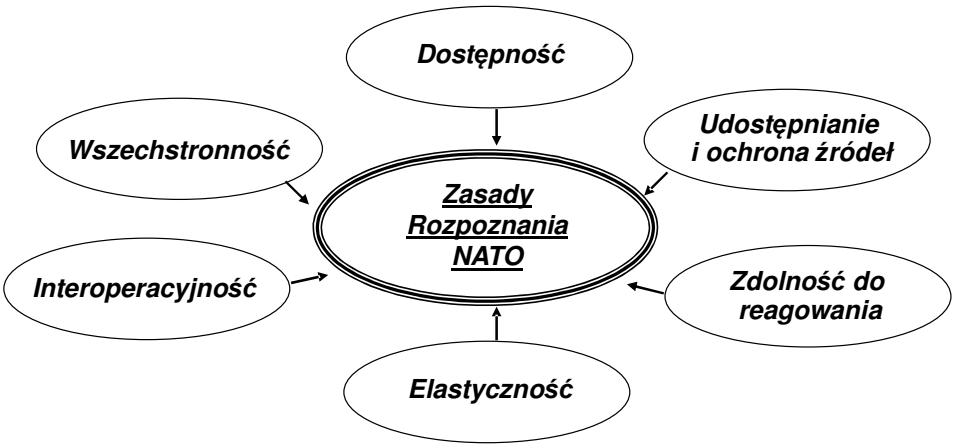
Dostępność. Oczekiwany wynik procesu informacyjnego realizowanego przez rozpoznawcze komórki sztabowe musi być dostępny dla stosownych odbiorców. Wysiłki podejmowane w ramach tego procesu nie będą miały żadnej wartości, jeżeli wyniki te nie będą rozpowszechniana lub udostępniane tym, którzy tego potrzebują.

Udostępnianie (wiadomości) i ochrona źródeł. Każdorazowo wymagane są pewne mechanizmy regulujące udostępnianie produktów działalności rozpoznawczej zarówno w ramach NATO, jak i z podmiotami spoza NATO zgodnie z obowiązującą sojuszniczą polityką bezpieczeństwa. Źródła informacji muszą być chronione, tak więc same wiadomości mogą być ograniczane na potrzeby ich udostępniania.

[9] Tamże, s. 36–38.

[10] Porównaj: AJP-2, *Allied Joint Intelligence ... (2003), wyd. cyt.,* s. 1-4-1 – 1-4-3.

[11] AJP-2*, Allied Joint Intelligence, Counter-Intelligence and Security Doctrine* (Edition A, Version 1, Ratification Draft 1), NATO Standardization Agency 2013, s. 3-3.



Źródło: opracowanie własne na podstawie AJP-2*, Allied Joint Intelligence, Counter-Intelligence and Security Doctrine* (Edition A, Version 1, Ratification Draft 1), NATO Standardization Agency 2013, s. 3-3 – 3-4.

Rys. 3. Sojusznicze zasady działalności rozpoznawczej – projekt 2013

Zdolność do reagowania. Na działalność rozpoznawczą wpływać będzie każda nowa informacja, czy też sytuacja, dlatego też sztabowe komórki rozpoznawcze, wspierające ośrodki/agencje, również te narodowe, powinny podejmować działania wyprzedzające w celu sprostania wymaganiom rozpoznawczym. Powinny one posiadać zdolność szybkiej analizy, syntezy, przetwarzania i przedstawiania produktów działalności rozpoznawczej decydentom.

Elastyczność. Personel sztabów odpowiedzialny za działalność rozpoznawczą odpowiada za dostarczanie całościowego obrazu sytuacji, który przedstawia aktualne, odpowiednie do sytuacji oraz zintegrowane wyniki procesu informacyjnego, dostosowane do zmieniających się wyzwań związanych z bezpieczeństwem. Wymaga to rozległej struktury rozpoznawczej, która jest w stanie zapewnić wszechstronne wsparcie dla przygotowywanej bądź realizowanej operacji.

Interoperacyjność. Jednolite, inaczej interoperacyjne, procesy, sieci i systemy skierowane są na ukierunkowanie, gromadzenie, przetwarzanie i rozpowszechnianie informacji i wiadomości, jak również na zarządzanie organizacją działalności rozpoznawczej. Siły i środki rozpoznania winny być centralnie koordynowane, aby uniknąć dublowania wysiłków, a jednocześnie zapewnić wzajemne wsparcie oraz efektywne i ekonomiczne wykorzystanie wszystkich zasobów.

Wszechstronność. Działalność rozpoznawcza powinna być wszechstronna w swojej naturze, zapewniając wyjaśnienie wszystkich powiązanych ze sobą elementów złożonego środowiska operacyjnego w sposób nie obciążony uprzedzeniami (bezstronny) i niezakłócony. Powinna ona również rozpatrywać sytuację z punktu widzenia kluczowych podmiotów (aktorów)[12], a tym samym podnosić wartość

[12] J. Wiśniewski, *System walki wojsk lądowych w szkoleniu dowództw i wojsk*, rozprawa doktorska, AON, Warszawa 2013, s.181 definiuje aktora jako *osobę lub organizację zarówno w wymiarze państwowym, jak i nie państwowym, funkcjonującą w ramach środowiska międzynarodowego i posiada-*

wszelkich ocen. W celu osiągnięcia wszechstronności rozpoznania Sojusz wykorzystuje model PMESII[13]. W niektórych przypadkach może on podlegać rozszerzeniu (np. o problematykę związaną z ochroną zdrowia czy też porządku prawnego)[14].

Jak wynika z powyższego opisu, w ciągu ostatniej dekady nastąpiło znaczące przeorientowanie zasad rozpoznania w NATO. Nie oznacza to jednak zapewne całkowitego odejścia od pierwotnych uwarunkowań. Trudno sobie bowiem wyobrazić, iż działalność rozpoznawcza nie będzie realizowana w myśl wymagań terminowości, czy też obiektywności.

W świetle powyższego warto przyjrzeć się uwarunkowaniom zasad rozpoznania obowiązujących w armiach innych państw.

Z pewnością na uwagę zasługują rozwiązania amerykańskie. Na przestrzeni czasu nieznacznie wykraczającego poza ramy ostatniego dziesięciolecia daje się zauważyć dynamiczną ewolucję w amerykańskich poglądach związanych z systemem walki, a w szczególności jego składem. Potwierdzenie tego faktu znajdujemy w podstawowych dokumentach normatywnych. Wraz początkiem XXI wieku i wprowadzeniem do użytku wydawnictwa FM 3-0 Operations (2001) pojawia się pojęcie: systemy działań pola walki *(ang.: Battlefield Operating Systems – BOSs)*[15]. W przyjętym rozwiązaniu znajdujemy 7 systemów, a jednym z nich jest System Działań Pola Walki Rozpoznanie *(ang.: Intelligence BOS)*[16].

Odpowiedzialność w zakresie systemu *Rozpoznanie* nie odbiega zasadniczo od naszych narodowych, a co za tym idzie i sojuszniczych wymagań, mówi się tu jednak, co zasługuje na uwagę, o kilku pryncypiach, a w konsekwencji właściwościach, które mogą okazać się inspiracją dla szczegółowej analizy specjalistycznej. Zestaw omawianych zasad przedstawia rysunek 4.

Ciągłe zaangażowanie (ang.: Always Engaged) – polegające na prowadzeniu działań rozpoznawczych w rejonach zainteresowania jeszcze w okresie pokoju, okresie poprzedzającym działania.

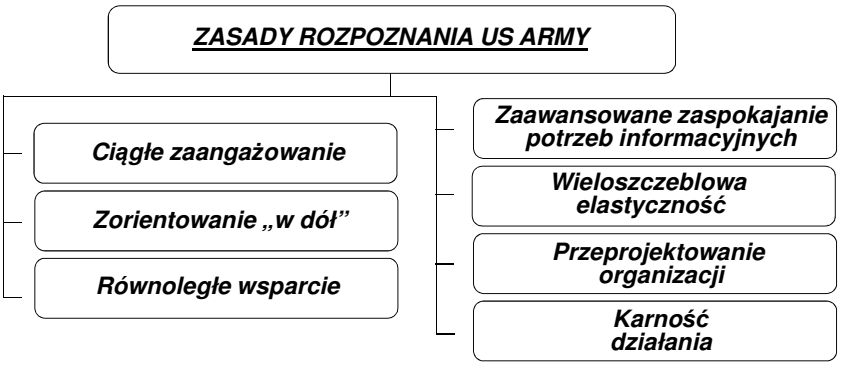
jącą zdolność lub dążącą do wywarcia wpływu na inne podmioty w ramach dążenia do realizacji własnych interesów lub celów. Zobacz również: *Allied Command Operations, Comprehensive Operations Planning Directive, COPD*, Interim v. 2.0, SHAPE, Belgium, 2013, s. L-1 oraz *Bi-SC Knowledge Development, Pre-Doctrinal Handbook*, Final Draft, 18 Nov 2010, s. 30.

[13] PMESII oznacza zintegrowane podejście do rozpatrywanej problematyki i obejmuje aspekty: polityczne *(ang.: Political)*, wojskowe *(ang.: Military),* ekonomiczne *(ang.: Economic),* społeczne *(ang.: Social),* jak również dotyczące infrastruktury *(ang.: Infrastructure*) i problematyki informacyjnej *(ang.: Information)*.

[14] AJP-2, *Allied Joint Intelligence* ... (2013), wyd. cyt., s. 3-3 – 3-4.

[15] FM 3-0, *Operations,* Headquarters Department of the Army, Washington DC 2001, s. 5–15.

[16] Obok Systemu Działań Pola Walki Rozpoznanie w przedmiotowym rozwiązaniu znalazły się: manewr *(ang.: Maneuver BOS)*, wsparcie ogniowe *(ang.: Fire Support BOS),* obrona przeciwlotnicza *(ang.: Air Defense BOS)*, mobilność, kontrmobilność, przetrwanie/przeżycie *(ang.: Mobility/counter mobility/survivability BOS)*, zabezpieczenie działań *(ang.: Combat Service Support BOS)* oraz dowodzenie i kontrola *(ang.: Command and Control BOS)*.



Źródło: opracowanie własne na podstawie *Norman M. Wade, The Operations SMARTbook – Third Revised Edition. Guide to FM 3-0 Full Spectrum Operations and Battlefield Operating Systems, The Lighting Press, Lakeland 2002, s. 2–11*.

Rys. 4. Zasady rozpoznania sił lądowych USA (2001–2007)

Zorientowanie „w dół" (ang.: Downwardly Focused) – ukierunkowanie na zaspokajanie potrzeb informacyjnych podwładnych, poprzez stosowny format wiadomości rozpoznawczych, ich adekwatność do szczebla czy obszaru/pasa/rejonu działania.

Równoległe wsparcie (ang.: Simultaneously Supported) – polegające na dostępności do informacji rozpoznawczych przez nadrzędny i podległy szczebel.

Zaawansowane zaspokajanie potrzeb informacyjnych (ang.: Coverage Enhanced) – oznacza otwartość na wykorzystanie technologii informatycznej zapewniającej przetworzenie informacji na obraz o wysokiej rozdzielczości, a co za tym idzie szczegółowości, dostarczany w realnym lub zbliżonym do realnego czasie, o dokładności, jak się zakłada, umożliwiającej jego wykorzystanie na potrzeby targetingu.

Wieloszczeblowa elastyczność (ang.: Skip Echelon Flexibility) – sprowadza się do swobodnego przesyłania informacji z pominięciem szczebli dowodzenia, gdy zaistnieje taka potrzeba.

Przeprojektowanie organizacji (ang.: Organizations Redesigned) – określa otwartość na zmiany organizacyjne wynikające z wykorzystania doświadczeń *(ang.: Lessons Learned)*, czy też korzyści wynikających z zastosowania nowych możliwości technologicznych ukierunkowanych na zaspokojenie potrzeb informacyjnych dowódców.

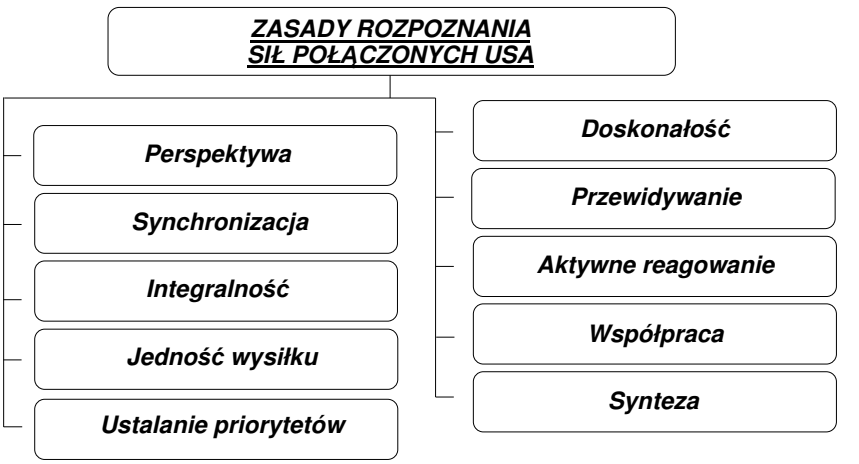
Karność działania (ang.: Disciplined Operations) – polega na działaniu w świetle obowiązującego prawa, regulaminów oraz oficjalnie przyjętych sposobów postępowania.

Nowe wydanie Field Manual No. 3-0, *Operations* z 2008 roku modyfikuje skład oraz zawartość poszczególnych systemów działań pola walki i nazywa je teraz funk-

cjami walki *(ang.: Warfighting Functions)*[17]. W ramach funkcji *Rozpoznanie* zdefiniowano następujące zadania:

- wsparcie na potrzeby generowania sił;
- wsparcie na potrzeby świadomości sytuacyjnej;
- prowadzenie działań w obszarach ISR[18];
- wsparcie targetingu i działań informacyjnych[19].

Mając na uwadze powyższe zadania, układ zasad prowadzenia rozpoznania w aspekcie działań połączonych *(ang.: Joint Intelligence)*[20] przedstawia się jak na rysunku 5.



Źródło: opracowanie własne na podstawie JP 2-0, *Joint Intelligence,* Joint Chiefs of Staff, Washington DC 2007, s. II-1 – II-12.

Rys. 5. Zasady rozpoznania sił połączonych USA (2007)

Perspektywa (ang.: Perspective) – myśl jak twój przeciwnik[21]. Analitycy wywiadu/rozpoznania muszą starać się zrozumieć proces myślowy przeciwnika, a także rozwijać i stale ulepszać swoją zdolność do myślenia jak przeciwnik. Powinni prezentować tę szczególną właściwość podczas wszystkich faz, etapów i czynności procesu dowodzenia. Dowódca powinien wymagać od oficerów pionu rozpoznawczego, aby oceniać wszystkie potencjalne działania z następującej perspektywy: *Jak*

[17] FM 3-0, *Operations*, Headquarters Department of the Army, Washington DC 2008, s. v oraz 4-1. Więcej informacji na temat funkcji walki *Rozpoznanie (ang.: Warfightig Function Intelligence)* znajdujemy w FM 2-0*, Intelligence*, Headquarters Department of the Army, Washington DC 2010, s. 1-3 – 1-4 oraz FM 7-15, *The Army Universal Task List*, Headquarters Department of the Army, Washington DC 2010, s. 2-1 – 2-54.

[18] ISR – Intelligence, Surveillance, Reconnaissance.

[19] Porównaj: J. Wiśniewski, *System walki wojsk lądowych ...,* s. 144–147, *FM 3-0, Operations... 2008,* s. 4-4 oraz *The US. Army Functional Concept for Intelligence 2016–2020*, TRADOC Pam 525-2-1, Department of the Army Headquarters 2010, s. 9–10.

[20] JP 2-0*, Joint Intelligence*, Joint Chiefs of Staff, Washington DC 2007, s. iii.

[21] Tamże, s. II-1 – II-2.

przeciwnik będzie postrzegał takie lub inne działania (wojsk własnych) i jaka będzie jego prawdopodobna odpowiedź? Wielce pomocna w tym względzie okazuje się analiza czynników ludzkich dowódców strony przeciwnej.

Synchronizacja (ang.: Synchronization) – synchronizuj działalność rozpoznawczą/wywiadowczą według planów i działań[22]. Działalność rozpoznawcza musi być zsynchronizowana z działaniami i planami w celu zapewnienia odpowiedzi na zapotrzebowanie z takim wyliczeniem, aby mogły one wpływać na podejmowane decyzje. Synchronizacja rozpoznania/wywiadu wymaga, aby wszystkie siły i środki oraz metody były stosowane w świetle obowiązujących planów i rozkazów. To dokumenty tego rodzaju stanowią główną siłę napędową dla działalności rozpoznawczej, która dyktuje terminy i kolejność działań wywiadowczych/rozpoznawczych. Z drugiej strony na potrzeby cyklu rozpoznawczego musi zostać zapewniona stosowna ilość czasu umożliwiającego integrację wiadomości rozpoznawczych w procesie podejmowania decyzji.

Integralność (ang.: Integrity) – pozostań uczciwy intelektualnie[23]. Uczciwość intelektualna musi być cechą oficera wywiadu/rozpoznania. Jest elementem kardynalnym w analizie i sprawozdawczości rozpoznawczej oraz podstawą, na której budowana jest wiarygodność w stosunku do odbiorcy informacji. Integralność wymaga trzymania się faktów i prawdomówności w każdych okolicznościach. Oznacza również odwagę moralną, która przejawia się odpornością na presję, aby dochodzić do wniosków poprzez naginanie interpretacji faktów. Metodologia działania, produkt działalności rozpoznawczej i jego wykorzystanie nie może być zmanipulowany w celu dostosowania się do oczekiwanego (pożądanego) wyniku.

Jedność wysiłku (ang.: Unity of Effort) – współpracuj na rzecz osiągnięcia wspólnego stanu końcowego działań[24]. Koordynacja dzięki współpracy i wspólnym zainteresowaniom dla osiągniecia pożądanego stanu końcowego jest kluczowa dla efektywności operacji wywiadowczych/rozpoznawczych. Jedność wysiłku jest zapewniana poprzez centralne planowanie i ukierunkowanie oraz zdecentralizowaną realizację działań wywiadowczych/rozpoznawczych. Umożliwia to dowódcy wykorzystanie wszystkich dostępnych sił i środków ISR mądrze, skutecznie i efektywnie. Dzięki takiemu podejściu optymalizuje się działalność rozpoznawczą poprzez adekwatne do potrzeb gromadzenie i przetwarzanie informacji oraz unikanie dublowania wysiłku. Wszystkie organizacje wywiadowcze/rozpoznawcze (połączone, narodowe i międzynarodowe) działające w danym obszarze operacyjnym muszą wykazać zrozumienie i akceptować pożądane przez dowódcę efekty, cele i stan końcowy działań.

Ustalanie priorytetów (ang.: Prioritization) – nadawaj priorytety informacyjne w oparciu o wytyczne dowódcy[25]. Ponieważ potrzeby operacyjne często przekraczają możliwości działalności rozpoznawczej, nadawanie priorytetów odnośnie do gromadzenia, analizy oraz alokacji zasobów ISR stają się kluczowymi aspektami planowania

[22] JP 2-0, *Joint Intelligence* … 2007, s. II-2 – II-3.

[23] Tamże, s. II-3 – II-4.

[24] Tamże, s. II-4 – II-6.

[25] Tamże, s. II-6.

działalności rozpoznawczej/wywiadowczej. Nadanie priorytetów oznacza wyselekcjonowanie zadań najważniejszych, a z drugiej strony uświadamia, iż pewne, obarczone niższym priorytetem, zadania mogą nie być zrealizowane ze względu na ograniczenia w siłach i środkach wywiadu/rozpoznania. Efektywne nadawanie priorytetów nie może obyć się bez aktywnej współpracy pomiędzy personelem sztabowych komórek rozpoznawczych a odbiorcami produktu działalności rozpoznawczej.

Doskonałość (ang.: Excellence) – należy dążyć do osiągnięcia najwyższych standardów jakości[26]. Aby osiągnąć najwyższe standardy jakości, produkty wywiadowcze/rozpoznawcze powinny cechować się następującymi atrybutami:

− *przewidywanie* potrzeb informacyjnych, przejawiające się pełnym zaangażowaniem w proces planowania działań na możliwie wczesnym etapie;

− *terminowość* – wiedza rozpoznawcza musi być dostępna, wtedy gdy dowódca jej potrzebuje, umożliwia to przewidywanie zdarzeń na polu walki, a z drugiej strony zapobiega zaskoczeniu przez stronę przeciwną;

− *dokładność* – wiedza rozpoznawcza musi być zgodna ze stanem faktycznym, odzwierciedlać fakty i sytuację faktycznie istniejącą, zapewnić najlepszą możliwą ocenę przeciwnika i jego przewidywane działanie na podstawie rzetelnej oceny wszystkich dostępnych informacji;

− *użyteczność* – wyniki działalności rozpoznawczej muszą być dostosowane do specyficznych potrzeb dowódcy oraz muszą być dostarczone w postaci odpowiedniej do bezpośredniego i pełnego zrozumienia;

− *kompletność* – kompletna wiedza rozpoznawcza odpowiada na pytania dowódcy co do przeciwnika w najwyższym możliwym stopniu;

− *adekwatność* – produkty działalności rozpoznawczej muszą cechować się adekwatnością w stosunku do potrzeb przygotowania (planowania i organizowania) oraz realizacji operacji;

− *obiektywizm* – dla wiedzy rozpoznawczej obiektywizm oznacza, iż jest ona bezstronna, nieobciążona założeniami, niezakłócona oraz jest wynikiem analizy;

− *dostępność* – produkty działalności rozpoznawczej muszą być łatwo dostępne dla dowódcy; dostępność jako funkcja jest nie tylko postrzegana jako terminowość i użyteczność, ale odnosi się również do odpowiedniej klauzuli tajności, interoperacyjności i łączności z innymi produktami.

Przewidywanie (ang.: Prediction) – akceptuj ryzyko przewidywania intencji (zamiarów) przeciwnika[27]. Mimo że działalność rozpoznawcza musi identyfikować i oceniać pełny zakres możliwości przeciwnika, to najbardziej pożądane jest, gdy koncentruje się na przyszłości, na zamiarach przeciwnika. Dowódca oczekuje szacunków co do intencji przeciwnika i jego wariantów działania w wystarczającym dla siebie stopniu szczegółowości. Jeśli brak jest wystarczających informacji, na których można prognozować działania przeciwnika, oficerowie sztabowych komórek rozpoznawczych muszą się upewnić, że dowódca ma taką świadomość, i że przyszłe działania należy przygotować z dużą dozą niepewności co do działań przeciwnika.

[26] Tamże, s. II-6 – II-9.

[27] Tamże, s. II-9 – II-10.

Aktywne reagowanie (ang.: Agility) – pozostań elastyczny i dostosowuj się do zmieniającej się sytuacji[28]. Aktywne reagowanie, to zdolność do przeorientowania wysiłku niemal natychmiastowo powiązana z przeniesieniem wszystkich posiadanych zdolności na rozwiązanie nowego problemu. Podkreśla się w takim przypadku jednoczesną kontynuację wcześniej rozpoczętych działań (pracy). Zakłada się, iż nieprzewidziane zdarzenia, nagłe zmiany w środowisku operacyjnym, a co za tym idzie oczekiwania odbiorców produktów rozpoznania wojskowego pozostawiają niewielki margines czasu na reakcję (przeorientowanie organizacji, przecelowanie sił i środków) czy też odtworzenie zdolności do działania. Dlatego kluczem do osiągnięcia aktywności w reagowaniu na zmiany jest planowanie i organizowanie działalności rozpoznawczej w przewidywaniu szeroko pojętych zmian. Utrzymywanie zdolności do reagowania w takich warunkach wymaga zachowania daleko idącej czujności i przezorności. Oficerowie sztabowych komórek rozpoznawczych powinni przewidywać nie tylko decyzje przeciwnika, ale również oczekiwania odbiorców wiadomości rozpoznawczych.

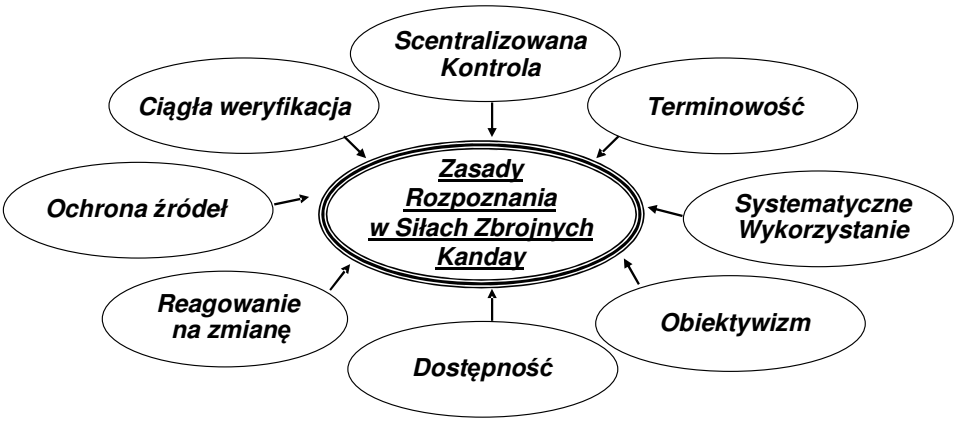
Współpraca (ang.: Collaboration) – równoważ zawartość różnorodnych zasobów analityczne[29]. Działalność rozpoznawcza ze swej natury jest niedoskonała, np. wszystko nie może być znane, analiza jest podatna na mylenie a każda informacja może być poddana alternatywnym interpretacjom. Najlepszym sposobem na uniknięcie tego rodzaju przeszkód, a tym samym osiągnięcie wyższego stopnia zgodności z rzeczywistością produktów działalności rozpoznawczej, jest zabieganie o opinie innych analityków i ekspertów, a w szczególności tych pochodzących z organizacji zewnętrznych.

Synteza (ang.: Fusion) – dociekaj danych i informacji ze wszystkich możliwych źródeł rozpoznawczych[30]. Synteza, można powiedzieć fuzja, jest tu rozumiana jako proces gromadzenia i analizy informacji ze wszystkich rodzajów oraz dostępnych źródeł rozpoznania/wywiadu. Ukierunkowana jest na uzyskanie kompletnej oceny rozpatrywanych działań. Opiera się ona na komplementarności ich mocnych stron *(ang.: all-source approach*).

Zasady prowadzenia rozpoznania w przedstawionym powyżej kształcie zostały podtrzymane w niezmienionym kształcie w nowym wydawnictwie amerykańskim dotyczącym rozpoznania w operacjach połączonych *JP 2-0, Joint Intelligence (2013)*[31]. Zasad prowadzenia działalności rozpoznawczej w siłach zbrojnych USA nie artykułuje się w wydawnictwie poziomu taktycznego[32]. Oznacza to zapewne pełne zastosowanie tych przytoczonych powyżej.

Innym przykładem zasad, którymi kieruje się działalność rozpoznawcza, jest rozwiązanie kanadyjskie. Wyróżnia się tutaj osiem pryncypiów, przedstawia je rysunek 6.

[28] Tamże, s. II-10 – II-11.
[29] Tamże, s. II-11.
[30] Tamże, s. II-11 – II-12.
[31] JP 2-0*, Joint Intelligence*, Joint Chiefs of Staff, Washington DC 2013, s. II-1 – II-12.
[32] Zobacz: FM 2-0*, Intelligence*, … (2010).



Źródło: opracowanie własne na podstawie: JDM, *Joint Intelligence Doctrine (B-GJ-005-200/FP-000)*, Canadian Army, Issued on Authority of the Chief of Defence Staff, 2003, s. 2–3.

Rys. 6. Zasady rozpoznania w armii kanadyjskiej

Scentralizowana Kontrola. Działalność rozpoznawcza musi być centralnie kierowana oraz kontrolowana, aby uniknąć nieuzasadnionego powielania pracy, wzajemnego wsparcia oraz zapewnienia efektywnego, ekonomiczne wykorzystanie wszystkich zasobów.

Terminowość. Produkt działalności rozpoznawczej staje się bezużyteczny, jeśli dociera do odbiorcy zbyt późno. W świetle tej samej zasady system, poprzez który źródła i agencje otrzymują zadania, musi być zdolny do odzwierciedlenia, bez zwłoki, wszystkich znaczących zmian w sytuacji operacyjnej.

Systematyczne wykorzystanie. Źródła i agencje (siły i środki rozpoznania) muszą być ciągle obarczanie zadaniami przy zachowaniu gruntownej znajomości ich możliwości i ograniczeń.

Obiektywizm. Unikać należy wszelkich pokus nadawania wiadomościom rozpoznawczym kształtu dopasowanego do przyjętych z góry założeń.

Dostępność. Stosowne wiadomości muszą być łatwo dostępne zarówno dla personelu rozpoznawczego/wywiadu jak i dla użytkowników/odbiorców w systemie rozpoznania. Produkt działalności rozpoznawczej nie przedstawia żadnej wartości, jeśli nie jest rozpowszechniany (udostępniany) tym, którzy go potrzebują.

Reagowanie na zmianę. Personel rozpoznania/wywiadu musi każdorazowo dostosowywać się do zmieniających się wymagań dowódcy zarówno w etapie przygotowania, jak i prowadzenia działań.

Ochrona źródeł. Wszystkie źródła informacji muszą być odpowiednio chronione.

Ciągła weryfikacja. Produkt działalności rozpoznawczej/wywiadowczej musi być permanentnie weryfikowany i w razie potrzeby uaktualniany, biorąc pod uwagę wszystkie nowe dane, fakty i informacje i porównanie ich z tym, co jest już znane[33].

[33] JDM, *Joint Intelligence Doctrine (B-GJ-005-200/FP-000),* Canadian Army, Issued on Authority of the Chief of Defence Staff, 2003, s. 2–3.

Jak wynika z powyższego zestawienia zasad rozpoznania i ich interpretacji, Kanadyjczycy w ówczesnych uwarunkowaniach (2003 r.) zaadaptowali rozwiązanie sojusznicze w całości.

Obok typowych zasad prowadzenia działalności rozpoznawczej w przytaczanych powyżej rozwiązaniach znajdujemy jeszcze inne zestawy zasad funkcjonujące w ramach działalności rozpoznawczej, które bezpośrednio rzutują na omawianą w niniejszym opracowaniu problematykę.

Dla przykładu, w opracowaniach amerykańskich mowa jest o zasadach zarządzania zbieraniem danych i informacji rozpoznawczych *(ang.: Principles of Collection Management)*. Wyróżnia się tutaj:

- odpowiednio wczesną identyfikację wymagań rozpoznawczych;
- ustalanie priorytetów;
- podejście interdyscyplinarne;
- pierwszeństwo w stawianiu zadań dostępnym w danej sytuacji siłom i środkom[34].

To samo wydawnictwo akcentuje kilka ciekawych kwestii w odniesieniu do samej działalności analitycznej. Wyróżnia się tu, między innymi, poniższe zasady:

- precyzyjne podejście do zdefiniowania tego, co jest już znane;
- rozróżnianie pomiędzy faktem, informacją i wiadomością rozpoznawczą;
- uwzględnianie merytorycznej złożoności rozpatrywanej problematyki;
- uwzględnianie możliwości mylenia ze strony przeciwnika[35].

Wydawnictwo poddaje również pod rozwagę tzw. atrybuty dobrego rozpoznania, które w świetle dotychczasowych rozważań mogłyby być rozpatrywane jako swoiste uzupełnienie zestawu zasad prowadzenia działalności rozpoznawczej[36].

W podobnym duchu problematyka atrybutów rozpoznania w odniesieniu do jego zasad jest artykułowana w doktrynie NATO. Rozwiązanie sojusznicze ogranicza jednak liczbę atrybutów do pięciu w porównaniu do 7–8 amerykańskich[37]. Ich zestaw przedstawia rysunek 7.

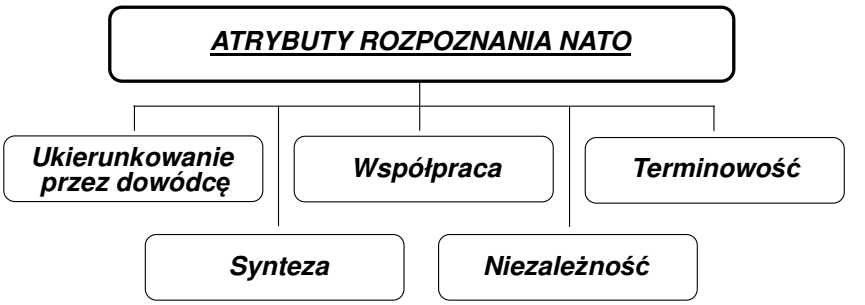
Jak wynika z powyższych rozważań, istnieje pokaźny zbiór zasad rozpoznania i związanych z tym pojęciem uwarunkowań. Mogą one stanowić pochodną rozwiązań sojuszniczych, koalicyjnych, jak i narodowych. Wydaje się, iż troska o zachowanie interoperacyjności, nie tylko w zakresie rozpoznania wojskowego i rozważanych w tym artykule jego zasad, nie powinna równać się skopiowaniu czy też zaimplementowaniu na płaszczyznę narodową rozwiązań sojuszniczych. Może przecież wynikać z głębokiej analizy różnorodnych uwarunkowań, być dostosowana do narodowych wymagań i możliwości, nawet wynikać z pewnej tradycji, a co najważniejsze stanowić ich wypadkową w stosunku do rozwiązań Sojuszu.

[34] JP 2-01, *Joint and National Intelligence Support to Military Operations*, Joint Chiefs of Staff, Washington DC 2012, s. III-14 – III-16.

[35] Więcej: JP, 2-01, *Joint and National Intelligence ...,* s. D-7 – D-8.

[36] Porównaj: JP 2-01, *Joint and National Intelligence ...,* s. III-66 oraz JP 2-0*, Joint Intelligence*..., 2013, s. II-7 – II-8.

[37] Porównaj: AJP-2, *Allied Joint Intelligence ...* (2013), s. 3-4 – 3-5 oraz JP 2-0*, Joint Intelligence*…, 2013, s. II-7 – II-8.



Źródło: opracowanie własne na podstawie AJP-2, *Allied Joint Intelligence, Counter-Intelligence and Security Doctrine (Edition A, Version 1, Ratification Draft 1), NATO Standardization Agency 2013, s. 3-4 – 3-5.*

Rys. 7. Atrybuty rozpoznania NATO

Tabela 2 przedstawia propozycję zasad prowadzenia rozpoznania wojskowego wyselekcjonowanych w wyniku przeprowadzonej powyżej analizy mogącą stanowić swego rodzaju zbiór wyjściowy (kolejność nie jest związana z rangą zasady). Na dobrą sprawę każda z nich zawiera odrębną i istotną treść i, jak już była o tym mowa, ich interpretacja może różnić się pomiędzy poszczególnymi krajami czy samym Sojuszem.

Tabela 2

Zestawienie możliwych zasad prowadzenia działalności rozpoznawczej

Zasady rozpoznania			
1.	Zaspokajanie potrzeb dowódcy	2.	Wszechstronność
3.	Centralne kierowanie	4.	Elastyczność
5.	Terminowość	6.	Ciągłe zaangażowanie
7.	Efektywne wykorzystanie	8.	Zorientowanie w dół
9.	Obiektywność	10.	Równoległe wsparcie
11.	Dostępność	12.	Zaawansowane zaspokajanie potrzeb info
13.	Dyspozycyjność	14.	Wieloszczeblowa elastyczność
15.	Bezpieczeństwo (ochrona źródeł)	16.	Przeprojektowanie organizacji
17.	Systematyczność	18.	Karność działania
19.	Podział zadań	20.	Perspektywa
21.	Zdolność przecelowania wysiłku	22.	Synchronizacja
23.	Modułowa konfiguracja potencjału	24.	Jedność wysiłku
25.	Sieciocentryczność	26.	Ustalanie priorytetów
27.	Wiarygodność	28.	Wczesna identyfikacja potrzeb
29.	Interoperacyjność	30.	Szeroka współpraca
31.	Ciągła weryfikacja potrzeb	32.	Synteza źródeł
33.	Odporność na mylenie	34.	Interdyscyplinarność
35.	Przewidywanie	36.	Doskonałość
37.	Integralność	38.	...

Źródło: opracowanie własne.

Co szczególnego warto dodać do powyższego zestawienia, to wymaganie/zasada w zakresie zachowania rozdzielności danych, faktów, informacji oraz wiadomości rozpoznawczych, tzn. materiału wyjściowego oraz produktu działalności rozpoznawczej. Wydaje się, iż prawidłowość taka pozostaje kluczową w aspekcie procesu informacyjnego realizowanego przez komórki sztabowe rozpoznania wojskowego.

W świetle realizowanych aktualnie prac nad nowelizacją *Doktryny Rozpoznanie Wojskowe* autor wyraża nadzieję, iż przedstawiony sposób rozważenia powyższych zasad stanowić będzie przyczynek do głębokiej analizy nie tylko ogólnej problematyki, ale również szczegółowych aspektów rozpoznania wojskowego.

Bibliografia

ACO, *Comprehensive Operations Planning Directive, COPD*, Interim v. 2.0, SHAPE, Belgium, 2013.

AJP-2, *Allied Joint Intelligence, Counter-Intelligence And Security Doctrine,* NATO Standardization Agency 2003.

AJP-2, *Allied Joint Intelligence, Counter-Intelligence And Security Doctrine* (Edition A, Version 1, Ratification Draft 1), NATO Standardization Agency 2013.

Bi-SC *Knowledge Development, Pre-Doctrinal Handbook*, Final Draft, 2010.

Doktryna Rozpoznanie wojskowe, D/2, SGWP, Warszawa 2013.

FM 2-0, *Intelligence,* Headquarters Department of the Army, Washington DC 2010.

FM 3-0, *Operations,* Headquarters Department of the Army, Washington DC 2001.

FM 3-0, *Operations,* Headquarters Department of the Army, Washington DC 2008.

FM 7-15, *The Army Universal Task List*, Headquarters Department of the Army, Washington DC 2010.

JDM, *Joint Intelligence Doctrine (B-GJ-005-200/FP-000),* Canadian Army, Issued on Authority of the Chief of Defence Staff, 2003.

JP 2-0, *Joint Intelligence*, Joint Chiefs of Staff, Washington DC 2007.

JP 2-01, *Joint and National Intelligence Support to Military Operations*, Joint Chiefs of Staff, Washington DC 2012.

The US. Army Functional Concept for Intelligence 2016–2020, TRADOC Pam 525-2-1, Department of the Army Headquarters 2010.

Wade Norman M., *The Operations SMARTbook – Third Revised Edition. Guide to FM 3-0 Full Spectrum Operations and Battlefield Operating Systems,* The Lighting Press, Lakeland 2002.

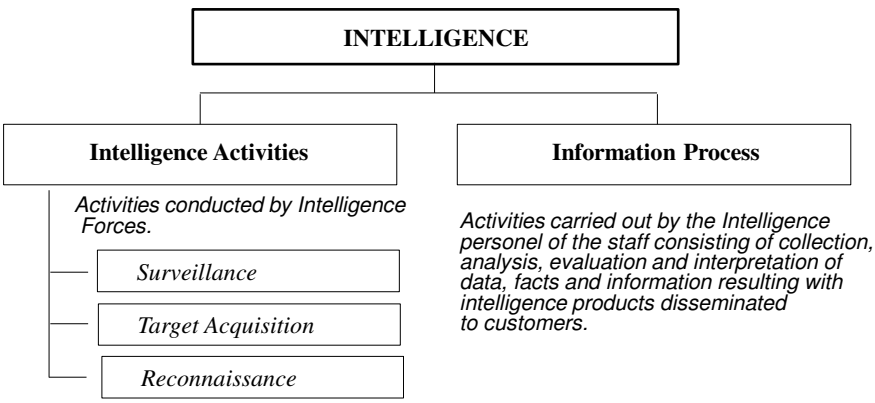
Wiśniewski J., *System walki wojsk lądowych w szkoleniu dowództw i wojsk,* rozprawa doktorska, AON, Warszawa 2013.

INTELLIGENCE PRINCIPLES

The work currently being carried out on the amendment of Polish national doctrine *D/2 Military Intelligence* includes afterthoughts on its contents and directions of change. Indeed, the existing solutions are limited, to a great extent, to

„dry" translation of the NATO document and adaptation to national requirements. The effect does not seem to be positive, because less than a year after its release, work on a new version of the document has begun.

An almost universal opinion is that in-depth consideration of the general issues in doctrines is not desirable for military personnel, who expect very specific solutions. However, both the rank of a document (the highest level), as well as the issues that are considered here, provoke discussion about such matters - they are intelligence principles. As it has already been said, the current principles which are obligatory in the Polish Armed Forces have been borrowed completely from Allied solutions. Should such a situation really occur? Did we look at other patterns? It might be worthwhile making a broader analysis when working out one's own position, especially when these principles are applied or referenced in the full spectrum of intelligence operations – intelligence activities and information process (see Figure 1). Thus, they are implemented by staff officers, especially from the functional intelligence area within the framework of direction, processing and dissemination, but also by those who, within intelligence activities, are responsible for data, facts and information collection[1].



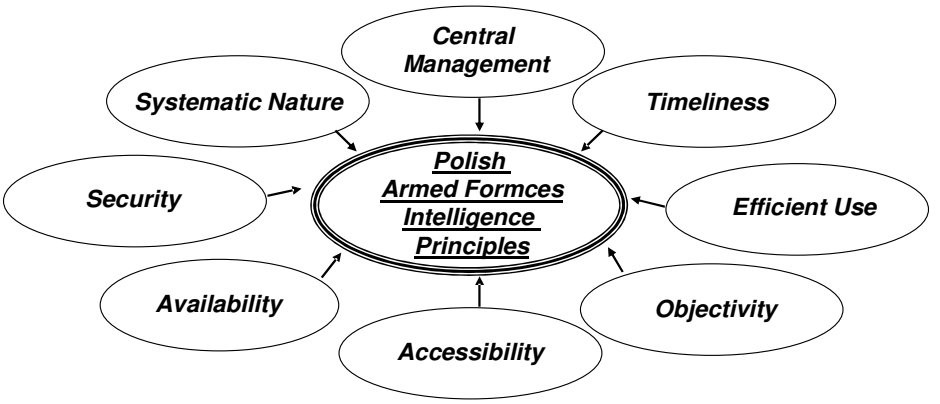
Source: own development based on *Doktryna Rozpoznanie Wojskowe, D/2,* SGWP, Warszawa 2013, p. 9.

Fig. 1. Composition of Intelligence in the Polish Armed Forces

The current release of the National Intelligence Doctrine defines the principles of military intelligence as the applicable standards of conduct for the preparation and execution of Intelligence[2]. The set of the standards consists of eight elements as shown in Figure 2.

[1] Intelligence cycle consists of four phases: 1) direction, 2) collection, 3) processing and 4) dissemination; for details see *Doktryna Rozpoznanie wojskowe, D/2*, SGWP, Warszawa 2013, p. 22-32.

[2] *Doktryna Rozpoznanie wojskowe, D/2* …(2013), op. cit., p. 21.



Source: own development based on *Doktryna Rozpoznanie Wojskowe, D/2,* SGWP, Warszawa 2013, p. 21-22.

Fig. 2. Intelligence principles in the Polish Armed Forces

Central Management. Intelligence activities must be centrally directed and coordinated by the staff intelligence personnel in order to avoid gaps in information collection and unwanted duplication of tasks, provide mutual support, as well as effective and economical use of the intelligence resources.

Timeliness. An accurate and reliable intelligence product is worthless if it is delivered to the customer too late. The task distribution tasks must take into account changes in the situation, so that the flow of information and intelligence product proceed without delay.

Efficient Use. The intelligence system should be configured in a modular manner, according to the type, area and duration of operations. Intelligence resources must be used in accordance with their essential task list and tasks for respective elements should always be appropriate to their capabilities.

Objectivity. Incoming information must be impartially evaluated and compared in order to prevent attempts to adjust the intelligence product to the previously assumed course of action.

Accessibility. Intelligence products must be available to staff and all other customers according to their needs at the required time. They are worthless if they are not provided to staff personnel.

Availability. Elements of an intelligence system must operate continuously, while maintaining the ability to perform the tasks set by the commander.

Security. Sources and agencies must be properly protected. This requirement is of particular importance in relation to the system of executive elements operating in the enemy operational/combat formation and HUMINT.

Systematic Nature. Information must be verified and updated continuously. It should be done after the information comes by comparing it with knowledge already acquired (Basic Intelligence)[3].

[3] Ibidem, p. 21-22.

Bearing in mind the above interpretation of the Intelligence principles, it is worth mentioning that they have been adopted for the Polish Armed Forces from the original principles articulated in the NATO doctrine AJP-2 (2003)[4]. Such a kind of intention is assumed in the introduction to the Polish national doctrine[5]. Specification of national and Allied intelligence principles is reflected in Table 1.

Some thoughts can be inspired by adopting solutions, not only in the field of principles of intelligence, which are out of date because they are ten years old.

Table 1

National and Allied expressions of Intelligence principles

No.	Polish National Intelligence Principles, D/2 (2013)	Allied Intelligence Principles, AJP-2 (2003)
1.	Central Management	Centralised Control
2.	Timeliness	Timeliness
3.	Efficient Use	Systematic Exploitation
4.	Objectivity	Objectivity
5.	Accessibility	Accessibility
6.	Availability.	Responsiveness
7.	Security	Source Protection
8.	Systematic nature	Continuous Review

Source: own development based on *Doktryna Rozpoznanie Wojskowe, D/2,* SGWP, Warszawa 2013, p. 21-22 and AJP-2*, Allied Joint Intelligence, Counter-Intelligence And Security Doctrine*, NATO Standardization Agency 2003, p. 1-3-1.

Given the established analogy (which in the author's opinion is not a bad option), some questionable points arising from the above statement of reference terms at level 3 i 6. *Systematic Exploitation* (No. 3, Table 1) refer to the systematical exploitation of sources and agencies by methodical tasking, based on a thorough knowledge of their capabilities and limitations[6]. While *Responsiveness* (No. 6 table 1, in the Polish national approach - *Availability)* stands for the intelligence staff who must be responsive to the Intelligence Requirements of the commander at all times[7].

The above mentioned examples prove that we fully support NATO solutions, but still take into account national implications.

NATO has no autonomous forces and means of Intelligence, and in the case of operations use both detached and national intelligence capabilities. Therefore, NATO intelligence capabilities must be created from integrated and compatible national intelligence sub-systems of Member States. The condition of this approach is the requirement that national intelligence systems and subsystems have the same operational capabilities, which are abbreviated as ISTAR *(**I**ntelligence, **S**urveillance,*

[4] AJP-2, *Allied Joint Intelligence, Counter-Intelligence And Security Doctrine*, NATO Standardization Agency 2003, p. 1-3-1.

[5] *Doktryna Rozpoznanie wojskowe, D/2* …(2013), op. cit., p. 5.

[6] AJP-2, *Allied Joint Intelligence … (2003), op. cit.,* p. 1-3-1.

[7] Ibidem.

***T**arget **A**cquisition and **R**econnaissance)*. ISTAR is defined as operational intelligence that integrates and synchronises planning and execution of forces and means with the information process, including: collection and processing of data, facts, information and dissemination of intelligence products[8].

The ISTAR term is used both for the operational processes and the personnel involved in this process and, therefore, it should be considered in two aspects:

− aspect of the material – forces, means and Intel staff elements; and

− functional aspect – mentioned before Intelligence.

ISTAR (system) principles basically coincide with the principles of Intelligence; however, in the case of the first addition it is necessary to additionally distinguish[9]:

− *Command Driven*. Direction of the ISTAR effort and determination of priorities must be driven by the Commander at each level of command. Unless the Commander devotes sufficient effort to these requirements, he may not receive the intelligence he requires for his decision-making and conduct of operations.

− *Modular design of intelligence forces and means.* Availability of a wide range of intelligence capabilities provides commanders' operational flexibility in the selection of appropriate forces and the means to obtain the required intelligence product. It also allows such planning of the exploitation of intelligence capabilities that provide both high efficiency of the process of obtaining information and maintenance of the appropriate tempo of operations. ISTAR should have a modular design adequately enabling the configuration of its components to the needs of operations, that is the kind of tasks assigned and the area, time and nature of the conflict;

− *Networkcentric.* A specific information network, integrated and tailored to operational needs is necessary to achieve situational awareness. To meet commanders' information requirements, the network should provide access to not only one's own sources but also others, to include, strategic, national, multinational and allied ones[10].

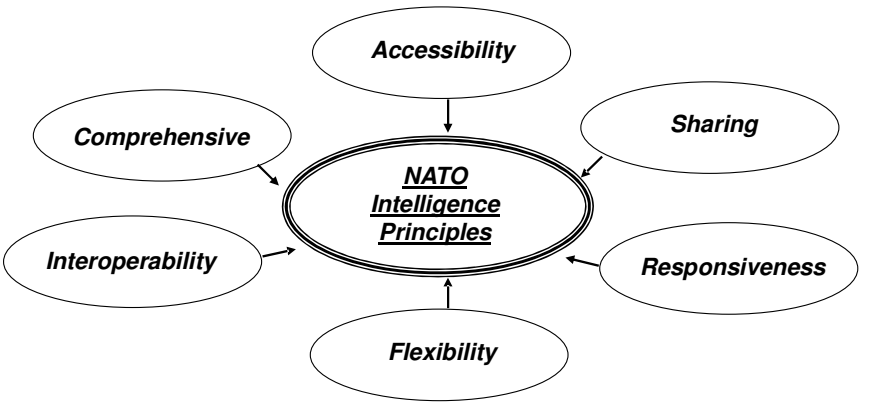
In 2013, with the publication of a new version of the Allied Intelligence doctrine (as a Ratification Draft), NATO took a new approach to the principles of its conduct, this time specifying clearly that they were in line with the guidelines provided by the Military Committee in this regard, in the form of the document *MC 0128/8 - Policy Guidance for NATO Intelligence*[11]. The new, current approach to the principles of intelligence is shown in Figure 3.

[8] *Doktryna Rozpoznanie wojskowe, D/2 …*(2013), op. cit., p. 34-35.

[9] Ibidem, p. 36-38.

[10] Compare: AJP-2, *Allied Joint Intelligence ... (2003), op. cit., p*. 1-4-1 – 1-4-3.

[11] AJP-2*, Allied Joint Intelligence, Counter-Intelligence and Security Doctrine* (Edition A, Version 1, Ratification Draft 1), NATO Standardization Agency 2013, p. 3-3.



Source: own development based on AJP-2*, Allied Joint Intelligence, Counter-Intelligence and Security Doctrine* (Edition A, Version 1, Ratification Draft 1), NATO Standardisation Agency 2013, p. 3-3 – 3-4.

Fig. 3. Allied Intelligence Principles – variant 2013

Accessibility. Relevant information and intelligence must be processed by intelligence staff and be readily available to intelligence consumers. Intelligence is of no value if it is not disseminated or accessible to those who require it.

Sharing. Mechanisms are required whereby intelligence can be shared, in a timely manner, within NATO and with non-NATO entities guided by the idea of the need to share in accordance with NATO's existing security policy. The source of the information might be protected and the information itself might be sanitised to protect the source.

Responsiveness. Intelligence will be influenced by any new situation or information; therefore, the intelligence staff should be pro-active in order to meet the intelligence requirements at all times. Intelligence staff should be able to quickly analyse, fuse, process and present products for decision makers.

Flexibility. It is necessary to establish an overall picture that provides timely, relevant, integrated and focused intelligence, suited to evolving security challenges. This requires a robust intelligence structure that can support intelligence driven operations.

Interoperability. Requirements exists for common or interoperable processes, networks and systems to support intelligence direction, collection, processing and dissemination, and the management of the intelligence organisation. Intelligence assets should be centrally coordinated to avoid duplication of effort, provide mutual support and ensure the efficient, economical use of all resources.

Comprehensive. In its nature, Intelligence should be comprehensive and should explain the inter-related elements of a complex operational environment in an unbiased and undistorted manner. It should also consider the situation from the perspective of key actors[12], thus improving the predicative content of any assessment. To achieve

[12] For more details see: *Allied Command Operations, Comprehensive Operations Planning Directive, COPD*, Interim v. 2.0, SHAPE, Belgium, 2013, p. L-1. Compare also: J. Wiśniewski, *System walki wojsk lądowych w szkoleniu dowództw i wojsk*, AON, Warszawa 2013 (PhD dissertation), p. 181 and *Bi-SC Knowledge Development, Pre-Doctrinal Handbook*, Final Draft, 18 Nov 2010, p. 30.

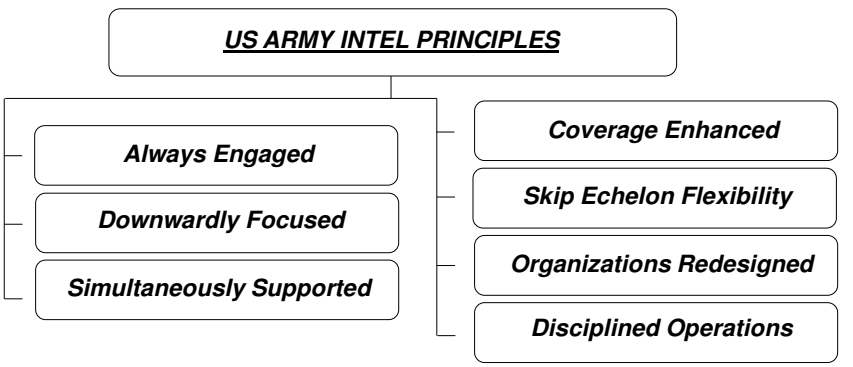
comprehensive intelligence, NATO utilises the Political, Military, Economic, Social, Infrastructure and Information (PMESII) model. For some environments, there might be other elements of relevance such as health and legal[13].

As indicated above there has been significant reorientation in the scope of intelligence principles in NATO. This does not mean, however, total renunciation of original determinations. It is difficult to imagine that intelligence does not meet requirements in the area of timeliness or objectivity.

In light of this, it is worth examining the determinants of intelligence principles in the armed forces of other countries.

The American approach certainly seems to be noteworthy. Over time, slightly outside the context of the last decade, the dynamic evolution of American beliefs associated with the combat system can be observed, in particular its composition. Confirmation of this fact can be found in the basic normative documents. At the beginning of the twenty-first century a new concept appears – *Battlefield Operating Systems (BOSs)*[14] and was put into service FM 3-0 *Operations* (2001). At that time, the solution assumed 7 systems and *Intelligence BOS* was one of them[15].

Responsibilities for the system do not differ significantly from our national solutions and, consequently, Allied requirements. The doctrine articulates, however, some principles and features of Intelligence BOS which seem to be significant,. As such they can be an inspiration for detailed analysis. A set of them is shown in Figure 4.



Source: own development based on *Norman M. Wade, The Operations SMARTbook – Third Revised Edition. Guide to FM 3-0 Full Spectrum Operations and Battlefield Operating Systems, The Lighting Press, Lakeland 2002, p. 2-11.*

Fig. 4. US Army Intelligence Principles (2001-2007)

[13] AJP-2, *Allied Joint Intelligence ...* (2013), op. cit., p. 3-3 – 3-4.

[14] FM 3-0, *Operations,* Headquarters Department of the Army, Washington DC 2001, p. 5-15.

[15] Beside *Intelligence BOS* the following systems exist in the mentioned doctrine: *Maneuver BOS*, *Fire Support BOS, Air Defense BOS*, *Mobility/counter mobility/survivability BOS*, *Combat Service Support BOS* and *Command and Control BOS)*.

Always Engaged. Through continuous peacetime intelligence operations, commanders are provided with intelligence support throughout the range of military operations. Early intelligence preparation is critical to the commander's decision making and planning process for force projection operations.

Downwardly Focused. Commanders must focus intelligence downwardly to the commander on the ground. Intelligence should get to the subordinate commander, when requested, in a usable format, and focused on his echelon and battle space.

Simultaneously Supported. Commanders at multiple echelons have to be provided with a common picture of the battlefield derived from various assets. Thus, intelligence products are available and, simultaneously, support the needs of higher and lower echelon commanders.

Coverage Enhanced. It means that the capabilities and technologies embedded in intelligence systems enhance the commander's ability to see the width and depth of the battlefield at a higher, more consistent degree of resolution than ever. As a result, decision makers have at their disposal more near-real time and real-time information with targeting accuracy.

Skip Echelon Flexibility. The intelligence battlefield operating system's flexibility of supports the skip echelon „push" of critical perishable intelligence from the above level to the tactical commander. At the same time, a tactical unit is capable of conducting the skip echelon „pull" of information from theatre, joint, and national data bases to answer the commander's intelligence requirements.

Organisations Redesigned. The principle defines openness to organisational changes resulting from experience (Lessons Identified/Learned) and benefits arising from the use of new technologies aimed at meeting the information requirements of commanders.

Disciplined Operations. This is about operating in the light of the applicable law, doctrines, regulations and officially adopted procedures[16].

The revised edition of FM 3-0 *Operations,* dated 2008, modifies composition and content of battlefield operating systems and names them from now on *Warfighting Functions*[17]. The *Intelligence Warfighting Function* includes the following tasks:

- support to force generation;
- support to situational understanding;
- conducting ISR[18];
- providing intelligence support to targeting and information capabilities[19].

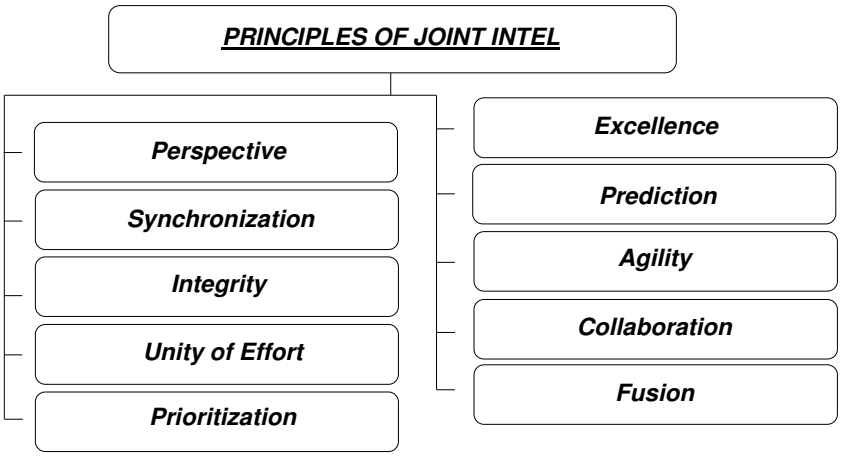
[16] Tactics, Techniques, Procedures (TTPs).

[17] FM 3-0, *Operations*, Headquarters Department of the Army, Washington DC 2008, p. v and 4-1. More information on *Warfighting Function Intelligence* can be found in FM 2-0*, Intelligence*, Headquarters Department of the Army, Washington DC 2010, p. 1-3 – 1-4 and FM 7-15, *The Army Universal Task List*, Headquarters Department of the Army, Washington DC 2010, p. 2-1 – 2-54.

[18] ISR – Intelligence, Surveillance, Reconnaissance.

[19] Compare: J. Wiśniewski, *System walki wojsk lądowych ..., op. cit., p*. 144-147, FM 3-0*, Operations... 2008, op. cit., p*. 4-4 and *The US. Army Functional Concept for Intelligence 2016-2020*, TRADOC Pam 525-2-1, Department of the Army Headquarters 2010, p. 9-10.

Given the above tasks, the layout of intelligence principles in the context of joint operations (*Joint Intelligence)*[20] is presented in Figure 5.



Source: own development based on JP 2-0, *Joint Intelligence,* Joint Chiefs of Staff, Washington DC 2007, p. II-1 – II-12.

Fig. 5. US Joint Forces' Intelligence Principles (2007)

Perspective – think like the adversary[21]. Intelligence analysts must seek to understand the adversary's thought process and should develop and continuously refine their ability to think like the adversary. They must offer this particular expertise during planning, execution, and assessment of operations. The commander should require the Intel Staff to assess all proposed actions from the following perspective: *"How will the adversary likely perceive this action and what are the adversary's probable responses?"* A human factor analysis of adversary leaders assists in gaining insights into their probable responses.

Synchronisation – synchronise intelligence with plans and operations[22]. Intelligence must be synchronised with operations and plans in order to provide answers to intelligence requirements in time to influence the decision they are intended to support. Intelligence synchronisation requires that all intelligence sources and methods be applied in concert with the OPLAN and OPORD. These documents' requirements therefore constitute the principal driving force that dictates the timing and sequencing of intelligence operations. On the other hand, the intelligence cycle must be accomplished with sufficient lead time to permit the integration of the intelligence product in operational decision-making and plan execution.

Integrity – remain intellectually honest [23]. Intellectual integrity must be the hallmark of the intelligence profession. It is the cardinal element in intelligence analysis and reporting and the foundation on which credibility with the intelligence

[20] JP 2-0*, Joint Intelligence*, Joint Chiefs of Staff, Washington DC 2007, p. iii.
[21] Ibidem, p. II-1 – II-2.
[22] Joint Publication 2-0, *Joint Intelligence* … 2007, op. cit., p. II-2 – II-3.
[23] Ibidem, p. II-3 – II-4.

consumer is built. Integrity requires adherence to facts and the truthfulness with which those facts are interpreted and presented. Moral courage is required to remain intellectually honest and to resist the pressure to reach intelligence conclusions that are not supported by facts. The methodology, production, and use of intelligence must not be directed or manipulated to conform to a desired result.

Unity of Effort – cooperate to achieve a common end state[24]. Coordination through cooperation and common interests to achieve a desired end state is essential for effective joint intelligence operations. Unity of effort is facilitated by centralised planning and direction and decentralised execution of intelligence operations, which enables commanders to apply all available ISR assets wisely, efficiently, and effectively. It optimises intelligence operations by reducing unnecessary redundancy and duplication in intelligence collection and production. All intelligence organisations (joint, national, and multinational) operating in a commander's operational area must have a clear understanding and common acceptance of the command's desired effects, objectives, and end state.

Prioritisation – prioritise requirements based on commander's guidance[25]. Because operational needs for intelligence often exceed intelligence capabilities, prioritisation of collection and analysis efforts and ISR resource allocation are vital aspects of intelligence planning. Prioritisation offers a mechanism for addressing requirements and effectively managing risk by identifying the most important tasks and applying available resources to those tasks. Effective prioritisation is absolutely dependent upon active cooperation and coordination between intelligence producers and intelligence consumers.

Excellence – strive to achieve the highest standards of quality[26]*. To achieve the highest standards of quality* intelligence products should be characterised by the following attributes:

− *anticipation* – requires the aggressive involvement of intelligence staff in operation planning at the earliest time possible;

− *timely* – intelligence must be available when the commander requires it. Timely intelligence enables the commander to anticipate events in the operational area. This, in turn, enables the commander to time operations for maximum effectiveness and to avoid being surprised;

− *accurate* – intelligence must be factually correct, convey an appreciation for facts and the situation as it actually exists, and provide the best possible estimate of the enemy situation and courses of action based on sound judgment of all information available*;*

− *usable* – intelligence must be tailored to the specific needs of the commander and must be provided in forms suitable for immediate comprehension;

− *complete* – complete intelligence answers the commander's questions about the adversary to the fullest degree possible;

[24] Ibidem, p. II-4 – II-6.
[25] Ibidem, p. II-6.
[26] Ibidem, p. II-6 – II-9.

− *relevant* – intelligence must be relevant to the planning and execution of the operation at hand. It must aid the commander in the accomplishment of the command's mission;

− *objective* – for intelligence to be objective, it should be unbiased, undistorted, and free of prejudicial judgment;

− *available* – intelligence must be readily accessible to the commander. Availability is a function of not only timeliness and usability, but also appropriate security classification, interoperability, and connectivity.

Prediction – accept the risk of predicting adversary intentions[27]. Although intelligence must identify and assess the full range of adversary capabilities, it is most useful when it focuses on the future and adversary intentions. Commanders require and expect timely intelligence estimates that accurately identify adversary intentions. If there is inadequate information upon which to base forecasts, the intelligence staff must ensure that the commander is aware of this shortcoming and that the future contains much uncertainty.

Agility – remain flexible and adapt to changing situations[28]. Agility is the ability to shift focus nearly instantaneously and bring to bear the skill sets necessary to address the new problem at hand while simultaneously continuing critical preexisting work. It is assumed that due to military contingencies or political challenges, sudden changes in the operational environment and requirements of intelligence consumers allow little reaction and recovery time. Therefore, the key to achieving agility is preparation and organisation for all contingencies well in advance. Maintaining responsiveness under such circumstances requires considerable vigilance and foresight. Intelligence professionals must anticipate not only the future decisions of adversaries, but of intelligence consumers as well.

Collaboration – leverage expertise of diverse analytic resources[29]. By its nature, intelligence is imperfect (i.e., everything cannot be known, analysis is vulnerable to deception, and information is open to alternative interpretations). The best way to avoid these obstacles and achieve a higher degree of fidelity is to consult with, and solicit the opinions of, other analysts and experts, particularly in external organisations.

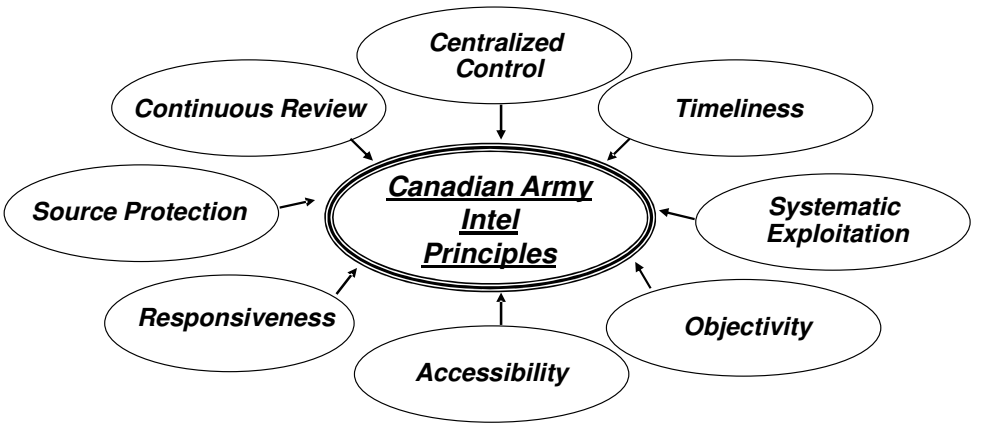
Fusion – exploit all sources of information and intelligence[30]. Fusion is the process of collecting and examining information from all available sources and intelligence disciplines to derive as complete an assessment as possible of detected activity. It draws on the complementary strengths of all intelligence disciplines and relies on an all-source approach to intelligence collection and analysis.

Intelligence principles in the above form were maintained unchanged in the new release of the American doctrine referring to joint intelligence operations – *JP 2-0,*

[27] Ibidem, p. II-9 – II-10.
[28] Ibidem, p. II-10 – II-11.
[29] Ibidem, p. II-11.
[30] Ibidem, p. II-11 – II-12.

Joint Intelligence (2013)[31]. Unfortunately, they cannot be found in the tactical level doctrine[32]. That probably means full application of those listed above.

Another example of intelligence principles comes from the Canadian armed forces. Here are eight principles that govern the production of intelligence and the organisation and activities of those who produce it. They are as shown in Figure 6.



Source: own development based on JDM, *Joint Intelligence Doctrine (B-GJ-005-200/FP-000)*, Canadian Army, Issued on Authority of the Chief of Defence Staff, 2003, p. 2-3.

Fig. 6. Canadian army Intelligence Principles

Centralised Control. Intelligence must be centrally controlled to avoid unwarranted duplication of work, provide mutual support and ensure the efficient, economical use of all resources.

Timeliness. Intelligence is useless if it arrives at its destination too late. By the same token, the system through which sources and agencies are tasked must be capable of reflecting, without delay, any significant changes in the operational situation.

Systematic Exploitation. Sources and agencies must be systematically exploited by methodical tasking, based on a thorough knowledge of their capabilities and limitations.

Objectivity. Any temptation to distort information to fit preconceived ideas must be resisted.

Accessibility. Relevant information and intelligence must be readily accessible to intelligence staff and to users. Intelligence is of no value if it is not disseminated nor made accessible to those who require it.

Responsiveness. The intelligence staff must be responsive to the intelligence requirements of the commander at all times.

Source Protection. All sources of information must be adequately protected.

[31] JP 2-0*, Joint Intelligence*, Joint Chiefs of Staff, Washington DC 2013, p. II-1 – II-12.

[32] See: FM 2-0*, Intelligence*, … (2010), op. cit.

Continuous Review. Intelligence must be continuously reviewed and, where necessary, revised, taking into account all new information and comparing it with that which is already known [33].

Resulting from the above composition and the content of the elements at that time (2003), the Canadians adopted the NATO solution in its entirety.

In addition to the typical principles of intelligence reflected in the above mentioned solutions, another set of intelligence rules can be found. They all directly affect the issues discussed in this paper. Therefore, it is worth mentioning them here.

For example, American doctrinal documents articulate the so called *Principles of Collection Management*. They are as follows:

- early identification of information requirements;
- prioritisation of requirements;
- multidisciplinary approach;
- tasking available assets first[34].

The same publication emphasises some interesting issues in relation to the analytical activities. The following rules, among others, apply:

- precise approach to what is known;
- careful distinguishing between data/fact/information and estimative judgment;
- consideration of substantive complexity;
- taking into account the possibility of deception[35].

The document also defines the so-called attributes of good intelligence, which could be considered as a kind of complement to the principles[36].

The issue of the identification of attributes of intelligence in relation to its principles is adequately articulated in the NATO doctrine. However, in contrast to the American 7-8 attributes the NATO solution limits the number of attributes to five[37]. These are depicted in Figure 7.

As shown above, a substantial set of intelligence principles and the associated notion of conditions exist in available documents. They can be derived from allied or national solutions. It seems that the aspiration to achieve and maintain interoperability, not only in the scope of military intelligence and its principles considered here, should not equate to copying or transferring them from NATO. They should rather result from a deep analysis of the various conditions to include tradition, to be adapted to current national requirements and possibilities and, most importantly, constitute their resultant.

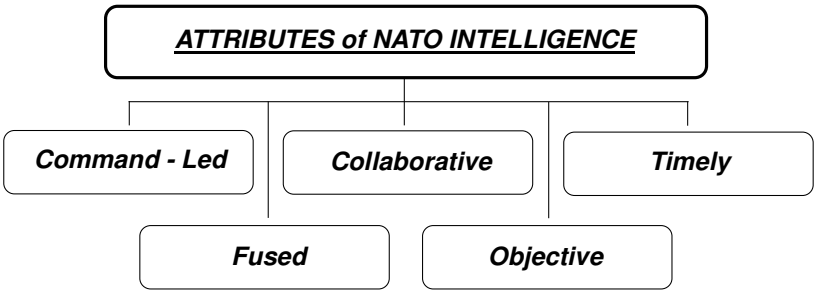
[33] JDM, *Joint Intelligence Doctrine (B-GJ-005-200/FP-000),* Canadian Army, Issued on the Authority of the Chief of Defence Staff, 2003, p. 2-3.

[34] JP 2-01, *Joint and National Intelligence Support to Military Operations*, Joint Chiefs of Staff, Washington DC 2012, p. III-14 – III-16.

[35] For more information see: JP 2-01, *Joint and National Intelligence ..., op. cit.*, p. D-7 – D-8.

[36] Compare: JP 2-01, *Joint and National Intelligence ..., op. cit.*, p. III-66 and JP 2-0*, Joint Intelligence* … 2013, op. cit., p. II-7 – II-8.

[37] Compare: AJP-2, *Allied Joint Intelligence ...* (2013), op. cit., p. 3-4 – 3-5 and JP 2-0*, Joint Intelligence* … 2013, op. cit., p. II-7 – II-8.



Source: own development based on AJP-2, *Allied Joint Intelligence, Counter-Intelligence and Security Doctrine (Edition A, Version 1, Ratification Draft 1), NATO Standardisation Agency 2013, p. 3-4 – 3-5.*

Fig. 7. NATO Intelligence's attributes

Table 2 presents a proposal of a set of intelligence principles selected as a result of the above analysis, which can be considered as an initial file (sequence is not related to the principles' ranking). Each of the principles contains a distinct and important content and, as it has already been mentioned, their interpretation may differ between countries or the NATO allies.

Table 2

Summary of possible intelligence principles

Principles of Intelligence			
1.	Command-Led	2.	Comprehensive
3.	Centralized Control	4.	Flexibility/Agility
5.	Timeliness	6.	Always Engaged
7.	Systematic Exploitation	8.	Downwardly Focused
9.	Objectivity	10.	Simultaneously Supported
11.	Accessibility/Sharing	12.	Coverage Enhanced
13.	Availability	14.	Skip Echelon Flexibility
15.	Source Protection	16.	Organizations Redesigned
17.	Continuous Review	18.	Disciplined Operations
19.	Tasks' Distribution	20.	Perspective
21.	Responsiveness	22.	Synchronization
23.	Modular Configuration of Resources	24.	Unity of Effort
25.	Networkcentric	26.	Prioritization
27.	Credibility	28.	Early Identification of Requirements
29.	Interoperability	30.	Collaboration
31.	Continuous Verification of Requirements	32.	Fusion
33.	Deception Resistance	34.	Multidisciplinary Approach
35.	Prediction	36.	Excellence
37.	Integrity	38.	…

Source: own development.

The last, and probably the most important, proposal that needs to be incorporated into the above table is a requirement/rule/principle in maintaining the separation of data, facts, information and outcomes (products of intelligence). It seems that the principle remains a key aspect of the information process.

In light of ongoing work on the amendment of the *Polish National Intelligence Doctrine,* the author hopes that above presentation considering intelligence principles contributes to the deep analysis of the general issues as well as the specific aspects of military intelligence.

Bibliography

ACO, *Comprehensive Operations Planning Directive, COPD*, Interim v. 2.0, SHAPE, Belgium, 2013.

AJP-2, *Allied Joint Intelligence, Counter-Intelligence And Security Doctrine,* NATO Standardization Agency 2003.

AJP-2, *Allied Joint Intelligence, Counter-Intelligence And Security Doctrine* (Edition A, Version 1, Ratification Draft 1), NATO Standardization Agency 2013.

Bi-SC *Knowledge Development, Pre-Doctrinal Handbook*, Final Draft, 2010.

Doktryna Rozpoznanie wojskowe, D/2, SGWP, Warszawa 2013.

FM 2-0, *Intelligence,* Headquarters Department of the Army, Washington DC 2010.

FM 3-0, *Operations,* Headquarters Department of the Army, Washington DC 2001.

FM 3-0, *Operations,* Headquarters Department of the Army, Washington DC 2008.

FM 7-15, *The Army Universal Task List*, Headquarters Department of the Army, Washington DC 2010.

JDM, *Joint Intelligence Doctrine (B-GJ-005-200/FP-000),* Canadian Army, Issued on Authority of the Chief of Defence Staff, 2003.

JP 2-0, *Joint Intelligence*, Joint Chiefs of Staff, Washington DC 2007.

JP 2-01, *Joint and National Intelligence Support to Military Operations*, Joint Chiefs of Staff, Washington DC 2012.

The US. Army Functional Concept for Intelligence 2016-2020, TRADOC Pam 525-2-1, Department of the Army Headquarters 2010.

Wade Norman M., *The Operations SMARTbook – Third Revised Edition. Guide to FM 3-0 Full Spectrum Operations and Battlefield Operating Systems,* The Lighting Press, Lakeland 2002.

Wiśniewski J., *System walki wojsk lądowych w szkoleniu dowództw i wojsk,* rozprawa doktorska, AON, Warszawa 2013.