**Leszek Wiszniewski**

# Rola i znaczenie analizy informacji wywiadowczej w zapewnianiu bezpieczeństwa państwa

W XXI w. ludzie są zmuszeni do odbioru coraz większej ilości informacji, mniej lub bardziej przydatnych. Jednym z głównych czynników wpływających na to zjawisko jest technologia rozwijająca się w zawrotnym tempie. Osoby korzystające z Internetu, w tym z portali społecznościowych (m.in. takich, jak Facebook, Twitter, YouTube) są adresatami 34 gigabajtów danych, co według naukowców z University of California w San Diego przekłada się na 100 tys. słów dziennie (ponad dwa razy tyle co na początku lat 80. poprzedniego stulecia)[1]. To powoduje konieczność szybkiego przetwarzania wiadomości i przyporządkowywania im odpowiednich stopni ważności. Z podobnymi problemami zmagają się politycy sprawujący w kraju funkcje kierownicze. Nadmiar informacji często utrudnia im podjęcie decyzji, od których może zależeć życie i zdrowie obywateli. Z tego względu, z uwagi na dynamicznie zmieniające się środowisko bezpieczeństwa państwa oraz mnogość wyzwań i zagrożeń wynikających z tego procesu, nastąpi wzrost znaczenia analizy informacji. Dla rządów szczególnie istotne będą materiały opracowane na podstawie danych pochodzących ze źródeł niejawnych. Tego rodzaju materiały umożliwiają właściwą ocenę sytuacji geopolitycznej (m.in. w przypadku działań hybrydowych prowadzonych przez przeciwnika, w tym dezinformacji) oraz podejmowanie działań wyprzedzających (np. zapobieganie zamachom terrorystycznym przez aresztowania osób zaangażowanych w ich przygotowania czy prewencyjne stosowanie środków bezpieczeństwa w przypadku nieprecyzyjnych sygnałów o potencjalnym zagrożeniu). Zwiększy się także rola służb specjalnych (wywiadu, kontrwywiadu) i formacji mundurowych, którym ustawodawca przyznał kompetencje do operacyjnego gromadzenia informacji oraz sporządzania na ich podstawie odpowiednio przygotowanych produktów analitycznych dla decydentów.

W pierwszej części opracowania zostanie omówiony problem analizy informacji w ujęciu teoretycznym, w tym kwestie definicyjne oraz cykl analityczny, ze szczególnym uwzględnieniem sposobów pozyskiwania informacji oraz rodzajów analizy. W drugiej części zostaną przedstawione uwarunkowania prawne dotyczące wybranych

[1] *The American Diet: 34 Gigabytes a Day*, https://bits.blogs.nytimes.com/2009/12/09/the-american-diet-34-gigabytes-a-day/?_r=0 [dostęp: 3 IX 2019].

polskich instytucji odpowiedzialnych za zapewnianie bezpieczeństwa państwa, które w ramach swoich kompetencji przygotowują analizy.

## Kwestie definicyjne

Na początku rozważań nad problemem analizy informacji należy odwołać się do literatury naukowej, aby poprawnie rozumieć terminy używane w niniejszej pracy. W *Słowniku języka polskiego PWN* znajdują się definicje, zgodnie z którymi a n a l i z a to ‘myślowe wyodrębnienie właściwości lub składników badanego zjawiska czy też przedmiotu’[2], a i n f o r m a c j a to ‘powiadomienie o czymś, zakomunikowanie czegoś; wiadomość, pouczenie’[3]. W materiałach akademickich pojawia się także sformułowanie, że „informacja” to (…) *zbiór faktów, zdarzeń, cech itp. określonych obiektów (rzeczy, procesów, systemów) zawarty w wiadomości (komunikacie), tak ujęty i podany w takiej postaci (formie), że pozwala odbiorcy ustosunkować się do zaistniałej sytuacji i podjąć odpowiednie działania umysłowe lub fizyczne*[4]. W literaturze specjalistycznej z dziedziny wojskowości i bezpieczeństwa można przeczytać, że (…) *analiza informacji w dziedzinie bezpieczeństwa państwa polega na nadawaniu sensu tej informacji, czyli (1) obejmuje poprawne wnioskowanie o konsekwencjach treści informacji i (2) maksymalizuje użyteczność informacji w podejmowaniu decyzji przez odbiorcę, dzięki sformułowaniu rekomendacji określonych działań*[5]. Istotne pozostaje także rozumienie pojęcia b e z p i e c z e ń s t w o i n f o r m a c y j n e. W literaturze przedmiotu jest ono używane w dwóch kontekstach. Pierwszy z nich odnosi się bardziej do zagrożeń związanych z przetwarzaniem informacji, co potwierdzają Piotr Potejko (*bezpieczeństwo informacyjne stanowi zbiór działań, metod, procedur, podejmowanych przez uprawnione podmioty, zmierzających do zapewnienia integralności gromadzonych, przechowywanych i przetwarzanych zasobów informacyjnych, poprzez zabezpieczenie ich przed niepożądanym, nieuprawnionym ujawnieniem, modyfikacją, zniszczeniem*[6]) i Krzysztof Liedel (*bezpieczeństwo informacyjne bardzo często rozumiane jest jako ochrona informacji przed niepożądanym – przypadkowym lub świadomym – ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania*[7]). Nieco inne rozumienie tego terminu proponuje Leszek Korzeniowski, który uważa, że (…) *przez bezpieczeństwo informacyjne podmiotu (człowieka lub organizacji) należy*

---

[2] L. Drabik, E. Sobol, *Słownik języka polskiego,* Warszawa 2005, s. 14.

[3] Tamże, s. 277.

[4] P. Sienkiewicz, *10 wykładów,* Warszawa 2005, s. 62.

[5] J. Konieczny, *Analiza informacji w dziedzinie bezpieczeństwa państwa*, Warszawa 2014, s. 256.

[6] P. Potejko, *Bezpieczeństwo informacyjne*, w: *Bezpieczeństwo państwa*, K.A. Wojtaszczyk, A. Materska-Sosnowska (red.), Warszawa 2009, s. 194.

[7] K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2008, s. 19.

*rozumieć możliwość pozyskania dobrej jakości informacji oraz ochrony posiadanej informacji przed jej utratą*[8]. Ten pogląd podzielają Krzysztof Liderman (*bezpieczeństwo informacyjne oznacza uzasadnione zaufanie podmiotu do jakości i dostępności pozyskiwanej oraz wykorzystywanej informacji*[9]) oraz Józef Janczak i Andrzej Nowak, którzy twierdzą, że (…) *kiedy mówi się o bezpieczeństwie informacyjnym, to zawsze dotyczy to podmiotu, który jest zagrożony poprzez brak informacji lub możliwość utraty zasobów informacyjnych*[10]. Próbę doprecyzowania terminu bezpieczeństwo informacyjne państwa podjęli eksperci Biura Bezpieczeństwa Narodowego. W projekcie *Doktryny bezpieczeństwa informacyjnego RP* z 2015 r. przedstawili „bezpieczeństwo informacyjne państwa" jako:

> (…) transsektorowy obszar bezpieczeństwa, którego treść odnosi się do środowiska informacyjnego (w tym cyberprzestrzeni) państwa; proces, którego celem jest zapewnienie bezpiecznego funkcjonowania państwa w przestrzeni informacyjnej poprzez panowanie we własnej, wewnętrznej, krajowej infosferze oraz efektywną ochronę interesów narodowych w zewnętrznej (obcej) infosferze. Osiąga się to poprzez realizację takich zadań, jak: zapewnienie adekwatnej ochrony posiadanych zasobów informacyjnych oraz ochrony przed wrogimi działaniami dezinformacyjnymi i propagandowymi (w wymiarze defensywnym) przy jednoczesnym zachowaniu zdolności do prowadzenia wobec ewentualnych przeciwników (państw lub innych podmiotów) działań ofensywnych w tym obszarze. Zadania te konkretyzowane są w strategii (doktrynie) bezpieczeństwa informacyjnego (operacyjnej i preparacyjnej), a do ich realizacji utrzymuje się i rozwija odpowiedni system bezpieczeństwa informacyjnego[11].

Na potrzeby pracy warto przyjąć szerszą – proponowaną przez Korzeniowskiego czy Lidermana – definicję terminu „bezpieczeństwo informacyjne", która odnosi się do możliwości pozyskiwania informacji pozwalających decydentom na zapewnienie bezpieczeństwa państwa.

Podrozdział poświęcony kwestiom definicyjnym jest także miejscem, w którym należy wytłumaczyć, czym jest propaganda (dezinformacja) oraz zjawisko szumu informacyjnego, które w ostatnim czasie stały się przedmiotem debaty w polskiej przestrzeni publicznej. „Dezinformacja" to komunikat sprzeczny z rzeczywistością, który może być (…) *elementem walki informacyjnej pomiędzy konkurującymi podmiotami*[12] (np. państwami czy przedsiębiorstwami). „Propaganda" i „dezinformacja" zostały szerzej zdefiniowane w projekcie *Doktryny bezpieczeństwa*

---

[8] L.F Korzeniowski, *Podstawy nauk o bezpieczeństwie*, Warszawa 2012, s. 147.

[9] K. Liderman, *Bezpieczeństwo informacyjne*, Warszawa 2012, s. 22.

[10] J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne. Wybrane problemy*, Warszawa 2013, s. 18.

[11] *Projekt Doktryny Bezpieczeństwa Informacyjnego RP*, https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf [dostęp: 3 IX 2017].

[12] K. Liedel, P. Piasecka, T.R. Aleksandrowicz, *Analiza informacji. Teoria i praktyka*, Warszawa 2012, s. 36.

*informacyjnego RP*. Jest to: (…) *rozpowszechnianie zmanipulowanych lub sfabrykowanych informacji (albo kombinacji jednych i drugich), w celu skłonienia ich odbiorców do określonych zachowań korzystnych dla dezinformującego, lub też w celu odwrócenia ich uwagi od faktycznie zaistniałych wydarzeń*[13]. Terminem „szum informacyjny" językoznawcy określają 'nadmiar informacji utrudniający wyodrębnienie informacji prawdziwych i istotnych'[14].

## Cykl wywiadowczy

Analiza danych jest tylko jednym z wielu etapów procesu, którego celem jest wsparcie informacyjne władz danego państwa w podejmowaniu decyzji pozwalających zapewnić obywatelom szeroko rozumiane bezpieczeństwo. W literaturze przedmiotu ten proces tradycyjnie określa się mianem cyklu wywiadowczego, na który składa się przeważnie – w zależności od taksonomii przyjętej przez poszczególnych naukowców – od czterech do sześciu etapów. Na potrzeby niniejszej publikacji przyjęto cztery etapy tego cyklu, obejmujące:

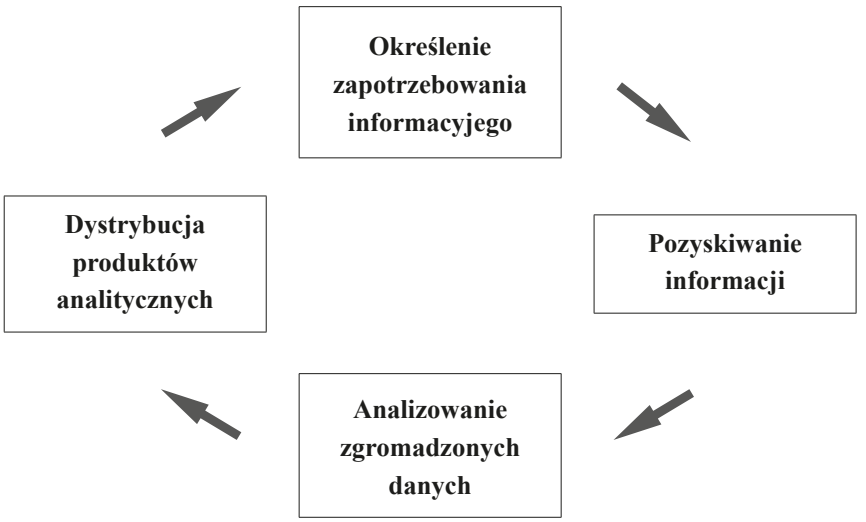
1) **określenie zapotrzebowania informacyjnego** przez organy państwowe, upoważnione do tego na podstawie obowiązującego prawa, oraz zlecenie zadań podległym im instytucjom (m.in. służbom bezpieczeństwa i porządku publicznego, agencjom wywiadowczym i kontrwywiadowczym). Ten etap jest ściśle skorelowany z bieżącymi wydarzeniami na świecie czy zjawiskami (np. konfliktami zbrojnymi, terroryzmem), które mogą negatywnie wpływać na bezpieczeństwo państwa. To na ich podstawie rząd określa kierunki działania służb. W tym kontekście jest konieczna umiejętność priorytetyzacji zagrożeń przez decydentów;
2) **pozyskiwanie informacji przez służby zgodnie z potrzebami władz**;
3) **analizowanie zgromadzonych danych**[15];
4) **przekazywanie odbiorcom** (zgodnie z właściwością rzeczową) **gotowych produktów analitycznych**. Tomasz Aleksandrowicz zauważa, że ten etap – w przypadku braku reakcji władz na otrzymany dokument – zamyka cykl wywiadowczy, a jeżeli pojawia się kolejne zlecenie, to mamy do czynienia z tzw. otwartym cyklem wywiadowczym[16].

[13] *Projekt Doktryny Bezpieczeństwa Informacyjnego RP*…

[14] http://sjp.pwn.pl/sjp/;3067966 [dostęp: 13 V 2017].

[15] Problem pozyskiwania informacji oraz ich przetwarzania zostanie przedstawiony w dalszej części opracowania.

[16] T.R. Aleksandrowicz, *Analiza informacji w administracji i biznesie*, Warszawa 1999, s. 55–56.




**Rysunek.** Cykl wywiadowczy.

Źródło: Opracowanie własne.
Wykorzystane materiały: K. Liedel, P. Piasecka, T.R. Aleksandrowicz, *Analiza informacji. Teoria i praktyka*, Warszawa 2012, s. 82–87.

Warto przedstawić kilka przykładów naruszeń cyklu wywiadowczego. Eksperci wyróżniają błędy popełniane zarówno przez decydentów, jak i analityków. Odbiorcy finalnych produktów mogą:

- w sposób nieprecyzyjny formułować swoje potrzeby, co może wynikać z braku umiejętności wykorzystania posiadanych sił i środków, w tym służb specjalnych;
- nie wykorzystywać wiedzy i konkluzji przekazywanych w dokumentach[17]. W tym kontekście warto wskazać na problem opisany w psychologii społecznej przez Irvinga Janisa, tj. syndrom grupowego myślenia (ang. *groupthink syndrome*, GTS). Definiuje się go jako (…) *nieracjonalny wzorzec myślenia i zachowania w grupie, który narzuca sztuczny konsensus i tłumi głosy sprzeciwu*[18]. To oznacza, że osoby podejmujące decyzje (czy to politycy, czy dowódcy wojskowi) jako członkowie większej grupy mogą jej ulec i – w obawie przed wykluczeniem – dobrowolnie ograniczyć swoje zdolności intelektualne do właściwej oceny sytuacji. Wśród przykładów GTS – wymienionych przez Janisa w artykule zatytułowanym *Groupthink*, opublikowanym w 1971 r. – znajdują się błędne decyzje podjęte przez Amerykanów, w tym brak właściwego przygotowania się na atak Japończyków na Pearl Harbor, przegrana

[17] J. Konieczny, *Analiza informacji w dziedzinie*…, s. 248.

[18] K. Albrecht, *Inteligencja praktyczna. Sztuka i nauka zdrowego rozsądku*, Gliwice 2009, s. 217.

podczas inwazji w Zatoce Świń oraz decyzja o zwiększeniu zaangażowania USA w wojnę w Wietnamie[19].

Błędy mogą powstać także na etapie opracowywania materiału analitycznego dla finalnego odbiorcy. Wśród najczęstszych należy wymienić[20]:

- przekonanie o wystarczającej ilości materiałów potrzebnych do sporządzania produktu analitycznego dla odbiorcy zewnętrznego oraz brak chęci do wykorzystania informacji, które wpływają na ocenę zagrożeń (np. tego rodzaju zachowanie może wynikać z tzw. lenistwa analityka, który ma już przygotowany i zatwierdzony projekt opracowania, a nowe dane diametralnie zmieniają przyjęte założenia, co wiąże się z koniecznością dalszej pracy nad tym samym dokumentem);
- brak odpowiedniej weryfikacji informacji dostarczanych przez źródło. Nieprawdziwe wiadomości mogą zniekształcać obraz rzeczywistości, co może doprowadzić do podjęcia przez polityków błędnych decyzji;
- tworzenie opracowań w sposób zgodny z oczekiwaniami adresatów materiałów czy przełożonych (np. osoby odpowiedzialne za przetwarzanie danych w obawie o karierę mogą umieszczać w analizach tezy i oceny zgodne ze sposobem postrzegania świata przez kierownictwo danej instytucji);
- spóźnione przekazywanie materiałów (brak informacji w odpowiednim czasie uniemożliwia podjęcie właściwej decyzji).

## Sposoby pozyskiwania informacji

Analizę informacji poprzedza proces ich zdobywania. W literaturze przedmiotu wymienia się wiele sposobów gromadzenia wiedzy dotyczącej bezpieczeństwa państwa. Obecnie można wskazać co najmniej kilka takich sposobów. Wśród najpopularniejszych należy wymienić:

- **OSINT** (ang. *Open Source Intelligence*), zwany także białym wywiadem – pozyskiwanie informacji ze źródeł otwartych, tj. mediów tradycyjnych i elektronicznych, portali społecznościowych (np. Facebooka), oficjalnych rejestrów państwowych, dokumentów administracji publicznej udostępnianych obywatelom, wykładów, konferencji naukowych oraz materiałów, do których dostęp nie wymaga specjalnych upoważnień czy umiejętności. W ostatnich latach OSINT – w związku z postępującym zjawiskiem cyfryzacji, coraz szerszym dostępem ludzi do internetu oraz ich otwartością na dzielenie się szerokim spektrum informacji z życia prywatnego za pośrednictwem portali społecznościowych – staje się nieocenionym źródłem wiedzy;

[19] I. Janis, *Groupthink*, „Psychology Today" 1971, nr 6, s. 43–46, 74–76.

[20] K. Liedel, P. Piasecka, T.R. Aleksandrowicz, *Analiza informacji*…, s. 112–115.

- **HUMINT** (ang. *Human Intelligence*), czyli zdobywanie wiedzy od tzw. osobowych źródeł informacji. Przez HUMINT należy rozumieć klasyczne działania wywiadowcze. Najczęściej instytucje państwowe (np. służby specjalne) uprawnione do prowadzenia działań operacyjno-rozpoznawczych starają się pozyskiwać materiały od osób posiadających informacje mogące mieć istotne znaczenie dla bezpieczeństwa zewnętrznego i wewnętrznego państwa, porządku konstytucyjnego, a także pozycji kraju na arenie międzynarodowej oraz jego potencjału militarnego i gospodarczego. W celu nawiązywania kontaktów oraz późniejszego werbunku funkcjonariusze służb korzystają z szerokiego spektrum narzędzi. W literaturze przedmiotu wskazuje się na różne motywacje osób, które godzą się na współpracę z organami bezpieczeństwa. Najpopularniejsza teoria zamyka się w angielskim skrócie **MICE** (tj. *money, ideology, coercion, ego*). Zgodnie z jej założeniami ludzie przekazują służbom informacje ze względu na m.in.: pieniądze otrzymywane w zamian, wyznawane poglądy, strach przed kompromitacją, zaspokojenie własnych ambicji;
- **SIGINT** (ang. *Signals Intelligence*)[21], na który składa się m.in. **COMINT** (ang. *Communication Intelligence* – informacje komunikacyjne, w tym pochodzące z rozmów telefonicznych, konwersacji przeprowadzanych za pomocą radiostacji oraz innych środków), **ELINT** (ang. *Electronic Intelligence* – dane pochodzące z rozpoznania sygnałów elektromagnetycznych nieużywanych w telekomunikacji) oraz **TELINT** (ang. *Telemetry Intelligence* – techniczne i wywiadowcze informacje pochodzące ze zgromadzonych i przetworzonych sygnałów świetlnych czy obcej telemetrii). Reasumując, SIGINT polega na pozyskiwaniu informacji za pomocą radarów, podsłuchów telefonicznych, mikrofonów kierunkowych oraz – być może przede wszystkim – kontroli przepływu danych w internecie. Obecnie, gdy weźmie się pod uwagę niską świadomość wielu użytkowników w zakresie zapewnienia bezpieczeństwa działań prowadzonych w cyberprzestrzeni, materiały pochodzące z tego typu źródeł stają się niezwykle cenne nie tylko dla hakerów czy grup przestępczych, lecz także dla służb państwowych, które w sposób niejawny i zgodnie z obowiązującym prawem powinny zdobywać interesującą je wiedzę. Jednocześnie ze względu na dużą liczbę informacji przesyłanych w sieciach teleinformatycznych, ich pozyskiwanie oraz analiza wymagają specjalistycznych umiejętności oraz programów komputerowych, które wspierają proces przetwarzania zgromadzonych materiałów;
- **IMINT** (ang. *Imagery Intelligence*) nazywany w literaturze także **PHOTINT** (ang. *Photo Intelligence*)[22] **–** pozyskiwanie wiedzy m.in. ze zdjęć wykonanych przez satelity wyposażone w wysokiej klasy aparaty fotograficzne lub przez

[21] Tłumaczenie własne za: *Global National Security and Intelligence Agencies Handbook*, Washington 2015, s. 279.

[22] Tamże.

funkcjonariuszy dzięki prowadzeniu obserwacji osób czy zainstalowaniu środków technicznych. Informacje zdobyte w ten sposób pozwalają wskazać czy też potwierdzić niepożądane zmiany w środowisku bezpieczeństwa (np. ruchy wojsk przeciwnika, budowanie nowych obiektów o przeznaczeniu militarnym);

- **MASINT** (ang. *Measurements and Signatures Intelligence*) – informacje wywiadowcze o charakterze naukowym i technicznym, otrzymywane przez jakościową i ilościową analizę danych (metryczną, kątową, przestrzenną, długości fal, zależności czasowych, modulacji, hydromagnetyczną), pochodzące z wyspecjalizowanych sensorów technicznych[23].

## Typy analiz i techniki analityczne

Kolejnym etapem cyklu wywiadowczego jest analiza wiedzy zgromadzonej zgodnie z zapotrzebowaniem polityków pełniących funkcje kierownicze w państwie. Można wskazać co najmniej dwa główne **typy analiz** stanowiących wsparcie w procesie decyzyjnym. Są nimi:

- **analiza strategiczna** – rozumiana jako kompleksowa diagnoza wydarzeń z przeszłości i teraźniejszości, która umożliwia przygotowanie prognozy dotyczącej szeroko pojmowanych zagrożeń bezpieczeństwa oraz wniosków i rekomendacji. Ułatwiają one odbiorcom takiego materiału podjęcie decyzji przynoszących skutki długofalowe;
- **analiza sygnalna** – przygotowywana na podstawie bieżącej pracy służb. Zazwyczaj przybiera formę tzw. kostki informacyjnej jedno- lub dwuakapitowej. W materiale zawierającym tylko jeden akapit (formą przypomina depeszę prasową) znajdują się odpowiedzi na najbardziej podstawowe pytania (kto? co? gdzie? kiedy?). W przypadku analiz dwuakapitowych wskazuje się dodatkowo krótkie wnioski i ewentualne rekomendacje.

Osobnym zagadnieniem są **techniki analityczne** wykorzystywane w toku opracowywania dokumentów istotnych dla bezpieczeństwa państwa. Wśród ciekawszych można wskazać:

- **analizy zdarzeń o wysokim wpływie i niskim prawdopodobieństwie** (ang. *high impact*, *low probability events*). Ich autorzy opisują zdarzenia, które mogą implikować poważne konsekwencje dla bezpieczeństwa państwa, ale prawdopodobieństwo ich wystąpienia jest niewielkie. Ważnymi elementami takiego opracowania są: diagnoza, w jaki sposób może dojść do niepożądanej sytuacji, oraz wskaźniki (tzw. czerwone flagi) ostrzegające przed zbliżającym się niebezpieczeństwem;

[23] K. Liedel, P. Piasecka, T.R. Aleksandrowicz, *Analiza informacji*…, s. 59.

- **analizy typu scenariusze możliwych zdarzeń**. Na podstawie zgromadzonych informacji, własnego doświadczenia oraz wiedzy o typowości przypadków analitycy przygotowują prognozę wydarzeń w perspektywie krótko-, średnio- i długookresowej. Zazwyczaj taka analiza składa się z trzech możliwych wariantów (scenariuszy): optymistycznego (najkorzystniejszego dla państwa), pesymistycznego (negatywnego) oraz najbardziej prawdopodobnego;
- **analizy typu „czerwony kapelusz"**. Ich celem jest odtworzenie sposobu myślenia przeciwnika (osób, organizacji terrorystycznych) oraz przewidywanie – z uwzględnieniem wszystkich zmiennych – jego możliwych zachowań w przyszłości (w tym potencjalnych decyzji np. godzących w bezpieczeństwo państwa).

## Pozyskiwanie i przetwarzanie informacji przez wybrane instytucje państwowe

W polskim systemie bezpieczeństwa funkcjonuje wiele instytucji państwowych, które przygotowują decydentom produkty analityczne. Zakres informacji potrzebnych do przygotowania analiz, które są pozyskiwane i przetwarzane przez poszczególne podmioty, jest różny i wynika z ich ustawowych kompetencji. Inne dane gromadzą cywilne służby specjalne, inne wojskowe, a jeszcze inne służby o charakterze policyjnym.

Polski kontrwywiad i wywiad – działając na podstawie i w granicach prawa – odpowiadają odpowiednio za (…) *uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego*[24] (Agencja Bezpieczeństwa Wewnętrznego) oraz za (…) *uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej oraz jej potencjału ekonomicznego i obronnego*[25] (Agencja Wywiadu). Szefowie ABW i AW są jednocześnie zobligowani do niezwłocznego przekazywania prezydentowi Rzeczpospolitej Polskiej i Prezesowi Rady Ministrów informacji mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczpospolitej Polskiej. Ponadto, jeżeli Prezes Rady Ministrów nie zdecyduje inaczej, szefowie ABW i AW przekazują te informacje także ministrom konstytucyjnym, zgodnie z ich właściwością rzeczową[26].

Na etapie gromadzenia informacji funkcjonariusze korzystają z uprawnień określonych w rozdziale 4. *Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*. Wśród nich należy wymienić m.in.:

- kontrolę operacyjną (obejmującą m.in. uzyskiwanie i utrwalanie treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą

[24] *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (t.j.: DzU z 2020 r. poz. 27), art. 5.

[25] Tamże, art. 6.

[26] Tamże, art. 18.

sieci telekomunikacyjnych, oraz obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne)[27];
- tajną współpracę z osobami niebędącymi funkcjonariuszami[28];
- pomoc organów administracji państwowej, które są zobowiązane do przekazywania do ABW i AW informacji istotnych dla bezpieczeństwa zewnętrznego i międzynarodowej pozycji Rzeczpospolitej Polskiej[29].

Przetwarzanie zgromadzonych informacji odbywa się w wyspecjalizowanych jednostkach organizacyjnych poszczególnych służb. Na podstawie otwartych źródeł informacji nie ma możliwości ustalenia szczegółowego zakresu ich kompetencji, gdyż te zagadnienia są regulowane przepisami o ochronie informacji niejawnych. O rosnącym znaczeniu analizy informacji w ABW świadczy jednak zmiana struktury organizacyjnej tej formacji. W listopadzie 2018 r. weszło w życie *Zarządzenie nr 163 Prezesa Rady Ministrów z 26 września 2018 r. w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego*[30]. Zgodnie z jego postanowieniami wyodrębniono – jak można przypuszczać z Biura Ewidencji i Analiz (zwanego także Biurem E) – nowy Departament Informacji, Analiz i Prognoz (Departament VIII). Obecnie to jego funkcjonariusze zapewne odpowiadają za przygotowywanie produktów analitycznych w ABW[31]. Ponadto można wnioskować – na podstawie wywiadu przeprowadzonego przez Krzysztofa Liedela z gen. Adamem Rapackim – że analizę dotyczącą zagrożeń terrorystycznych może prowadzić w pewnym zakresie Centrum Antyterrorystyczne, które zostało powołane do życia na mocy *Zarządzenia nr 102 Prezesa Rady Ministrów z dnia 17 września 2008 r. zmieniającego zarządzenie w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego* (akt uchylony – przyp. red.). Adam Rapacki wskazywał, że (…) *poza przetwarzaniem informacji o charakterze operacyjnym w Centrum będą opracowywane analizy dotyczące poszczególnych zagadnień po to, aby wiedza dystrybuowana z Centrum była jednolita dla wszystkich podmiotów*[32].

W przypadku AW nawet takie rozważania były do niedawna niemożliwe, gdyż statut tej instytucji nie ujawniał, która jednostka organizacyjna odpowiada za analizę informacji (prawie wszystkie nosiły nazwę „Biuro")[33]. Zmiana w tej materii również nastąpiła w 2018 r. Zgodnie z *Zarządzeniem nr 106 Prezesa Rady Ministrów z dnia*

[27] Tamże, art. 27.

[28] Tamże, art. 36.

[29] Tamże, art. 41.

[30] M.P. z 2018 r. poz. 927.

[31] Tamże, § 3.

[32] K. Liedel, *Zwalczanie terroryzmu międzynarodowego w polskiej polityce bezpieczeństwa,* Warszawa 2010, s. 132.

[33] *Obwieszczenie Prezesa Rady Ministrów z dnia 14 września 2016 r. w sprawie ogłoszenia jednolitego tekstu zarządzenia Prezesa Rady Ministrów w sprawie nadania statutu Agencji Wywiadu* (M.P. z 2016 r. poz. 936), § 3.

*3 lipca 2018 r. zmieniającym zarządzenie w sprawie nadania statutu Agencji Wywiadu*[34] utworzono nową jednostkę – Departament Informacyjny, który – tak jak w przypadku ABW – zapewne przygotowuje opracowania analityczne dla władz RP[35].

Inny zakres informacji pozyskują i przetwarzają wojskowe służby specjalne. Służba Kontrwywiadu Wojskowego (SKW) jest zobowiązana do (…) *uzyskiwania, gromadzenia, analizowania, przetwarzania i przekazywania właściwym organom informacji mogących mieć znaczenie dla obronności państwa, bezpieczeństwa lub zdolności bojowej Sił Zbrojnych RP czy pozostałych jednostek organizacyjnych MON*[36]. Z kolei Służba Wywiadu Wojskowego (SWW) uzyskuje, gromadzi, analizuje, przetwarza i przekazuje właściwym organom informacje, które mogą mieć istotne znaczenie dla potencjału obronnego Rzeczpospolitej Polskiej, bezpieczeństwa i zdolności bojowej Sił Zbrojnych RP oraz warunków realizacji przez nie zadań poza granicami państwa. Ta służba rozpoznaje również i analizuje zagrożenia, które mogą wpływać na obronność państwa, występujące m.in. w rejonach konfliktów[37]. Zgromadzone i przetworzone informacje szefowie SKW i SWW przekazują niezwłocznie – po powiadomieniu ministra obrony narodowej – prezydentowi RP i Prezesowi Rady Ministrów. Ponadto, jeżeli te informacje dotyczą spraw objętych zakresem działania właściwego ministra, przekazują je również temu ministrowi, chyba że Prezes Rady Ministrów zadecyduje inaczej[38].

Na etapie gromadzenia informacji funkcjonariusze SKW i SWW korzystają z uprawnień określonych w rozdziale 3. *Ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego*. Są one w wielu przypadkach zbieżne z uprawnieniami przewidzianymi dla ABW i AW (m.in. kontrola operacyjna czy tajna współpraca z osobami niebędącymi funkcjonariuszami). Jednocześnie trudno określić, które jednostki organizacyjne w SWW i SKW odpowiadają za analizę informacji, gdyż ich struktura pozostaje niejawna (prawodawca posługuje się określeniami: departament, zarząd, biuro[39]).

Centralne Biuro Antykorupcyjne, utworzone w 2006 r. na podstawie *Ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym*[40] (…) *jako służba specjalna do spraw zwalczania korupcji w życiu publicznym i gospodarczym, w szczególności w instytucjach państwowych i samorządowych, a także do zwalczania*

---

[34] M.P. z 2018 r. poz. 660.

[35] Tamże, § 1.

[36] *Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego* (t.j.: DzU z 2019 r. poz. 687).

[37] Tamże, art. 6.

[38] Tamże, art. 19.

[39] *Zarządzenie Ministra Obrony Narodowej z dnia 21 kwietnia 2017 r. w sprawie nadania statutu Służbie Kontrwywiadu Wojskowego* (M.P. z 2017 r. poz. 431) oraz *Zarządzenie Ministra Obrony Narodowej z dnia 13 czerwca 2018 r. zmieniające zarządzenie w sprawie nadania statutu Służbie Wywiadu Wojskowego* (M.P. z 2018 r. poz. 694).

[40] Tekst jednolity: DzU z 2019 r. poz. 1921, ze zm.

*działalności godzącej w interesy ekonomiczne państwa*[41], zostało zobligowane (…) *do prowadzenia działalności analitycznej dotyczącej zjawisk występujących w obszarze właściwości CBA oraz przedstawiania w tym zakresie informacji Prezesowi Rady Ministrów, Prezydentowi Rzeczypospolitej Polskiej, Sejmowi oraz Senatowi*[42].

Na etapie gromadzenia informacji funkcjonariusze CBA korzystają z uprawnień określonych w rozdziale 3. ustawy o CBA. Również w przypadku CBA są one często zbieżne z uprawnieniami przewidzianymi dla ABW, AW, SKW oraz SWW (m.in. kontrola operacyjna, tajna współpraca z osobami, które nie są funkcjonariuszami). Za przetwarzanie i analizowanie informacji zgromadzonych w wyniku czynności operacyjno-rozpoznawczych odpowiada prawdopodobnie Departament Analiz[43].

Podczas realizacji swoich zadań ustawowych informacje o charakterze wywiadowczym pozyskują także Policja i Straż Graniczna (SG), które podlegają ministrowi spraw wewnętrznych i administracji. Charakter tych informacji determinuje katalog zadań wskazanych tym służbom przez ustawodawcę. Z tego względu Policja przetwarza dane związane z (…) *ochroną bezpieczeństwa i porządku publicznego, w tym zapewnieniem spokoju w miejscach publicznych oraz w środkach publicznego transportu i komunikacji publicznej, w ruchu drogowym i na wodach przeznaczonych do powszechnego korzystania*[44]. Z kolei Straż Graniczna (…) *gromadzi i przetwarza informacje z zakresu ochrony granicy państwowej, kontroli ruchu granicznego, zapobiegania i przeciwdziałania nielegalnej migracji*[45]. Proces analizy informacji oraz ich przekazywania decydentom następuje w jednostkach organizacyjnych poszczególnych służb funkcjonujących w ramach odpowiednio Komendy Głównej Policji (KGP) oraz Komendy Głównej Straży Granicznej (KG SG). W KGP istnieje m.in.:

- Gabinet Komendanta Głównego Policji, do którego zadań należy (…) *koordynowanie przygotowywania materiałów na posiedzenia komisji i podkomisji parlamentarnych oraz udziału w ich pracach Komendanta Głównego Policji i jego zastępców, przygotowywanie analiz dotyczących funkcjonowania Policji na doraźne potrzeby kierownictwa KGP*[46];
- Główny Sztab Policji, którego zadaniem jest (…) *zarządzanie bieżącymi informacjami o stanie bezpieczeństwa i porządku* (…)*, w tym gromadzenie i analizowanie informacji o bieżących zdarzeniach i zagrożeniach na terenie kraju oraz podejmowanie działań służących ich zapobieganiu i eliminowaniu*[47].

---

[41] Tamże, art. 1.

[42] Tamże, art. 2.

[43] *Zarządzenie Nr 72 Prezesa Rady Ministrów z dnia 6 października 2010 r. w sprawie nadania statutu Centralnemu Biuru Antykorupcyjnemu* (M.P. z 2010 r. nr 76 poz. 953), § 3.

[44] *Ustawa z dnia 6 kwietnia 1990 r. o Policji* (t.j.: DzU z 2020 r. poz. 360), art. 1.

[45] *Ustawa z dnia 12 października 1990 r. o Straży Granicznej* (t.j.: DzU z 2020 r. poz. 305), art. 1.

[46] http://www.policja.pl/pol/kgp/gabinet-komendanta-glo/ [dostęp: 3 IX 2019].

[47] http://www.policja.pl/pol/kgp/glowny-sztab-policji [dostęp: 3 IX 2019].

Z kolei w strukturze KG SG funkcjonuje:

- Zarząd do spraw Cudzoziemców, do którego zadań należy (…) *przygotowywanie cyklicznych i okresowych analiz i opracowań, w szczególności w zakresie powrotów cudzoziemców z terytorium RP*[48];
- Biuro Analityczno-Informacyjne, które odpowiada m.in. za (…) *zapewnienie Komendantowi Głównemu Straży Granicznej i jego zastępcom wsparcia w procesie decyzyjnym, w szczególności poprzez opracowanie i dostarczanie informacji i analiz oraz dokumentów o charakterze strategicznym dla działalności Straży Granicznej*[49].

Wymienienie zakresu kompetencji tylko kilku instytucji pokazuje, jak wiele podmiotów zajmuje się analizą informacji. Materiały zdobywane przez te podmioty oraz ich obszary zainteresowania – pomimo różnych zadań – często się pokrywają. Z tego względu prawodawca podjął w 2007 r. próbę usprawnienia systemu bezpieczeństwa państwa w zakresie przepływu danych pomiędzy jego poszczególnymi komponentami. *Ustawą z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*[50] powołał do życia Rządowe Centrum Bezpieczeństwa (RCB) – podmiot, który koordynuje obieg informacji oraz pełni funkcję Krajowego Centrum Zarządzania Kryzysowego. Do podstawowych zadań RCB należą: (...) *analiza i ocena możliwości wystąpienia zagrożeń lub ich rozwoju, gromadzenie informacji o zagrożeniach i analiza zebranych materiałów, wypracowywanie wniosków i propozycji zapobiegania i przeciwdziałania zagrożeniom*[51]. O roli i znaczeniu informacji w działalności RCB świadczy wyodrębnienie w strukturze organizacyjnej tej instytucji osobnej komórki, tj. Biura Analiz i Reagowania, które składa się m.in. z Centrum Operacyjno-Analitycznego. Jego zadania to: (...) *monitorowanie i analizowanie sytuacji w obszarze stanu bezpieczeństwa narodowego oraz występujących w tym zakresie zagrożeń; sporządzanie sprawozdań, raportów i ocen: – z działań prowadzonych w sytuacjach kryzysowych przez Centrum – w zakresie powierzonym przez Radę Ministrów lub Prezesa Rady Ministrów, z działań prowadzonych w sytuacjach kryzysowych przez organy administracji publicznej właściwe w sprawach zarządzania kryzysowego*[52].

[48] http://strazgraniczna.pl/pl/straz-graniczna/struktura-sg/komenda-glowna-sg/komorki-organizacyjne-k/zarzad-do-spraw-cudzozi/1909,Zarzad-do-Spraw-Cudzoziemcow-Komendy-Glownej-Strazy-Granicznej.html [dostęp: 3 IX 2019].

[49] https://strazgraniczna.pl/pl/straz-graniczna/struktura-sg/komenda-glowna-sg/komorki-organizacyjne-k/biuro-analityczno-sytua/7895,Biuro-Analityczno-Sytuacyjne.html [dostęp: 9 XII 2019].

[50] Tekst jednolity: DzU z 2019 r. poz. 1398, ze zm.

[51] Tamże, art. 11.

[52] http://rcb.gov.pl/centrum-operacyjno-analityczne-2/ [dostęp: 3 IX 2019].

## Wnioski

Autor opracowania jest świadomy, że nie wyczerpał tematu. Jego zamiarem było jedynie zasygnalizowanie kilku ciekawych aspektów pracy analitycznej oraz aktualnych rozwiązań systemowych w obszarze tworzenia dla władz RP produktów analitycznych, które wspomagają proces decyzyjny w sferze bezpieczeństwa państwa. Na tej podstawie można jednak, reasumując dotychczasowe rozważania oraz mając na uwadze, że pełne przedstawienie problemu wymagałoby przygotowania wielostronicowego opracowania, wyciągnąć pewne wnioski:

1. W związku z dużą liczbą informacji pojawiających się każdego dnia (potencjalnie istotnych dla życia, zdrowia i mienia polskich obywateli, porządku konstytucyjnego czy pozycji międzynarodowej RP) rola i znaczenie analizy danych będą rosły. Z tego względu na rynku pracy będą poszukiwani fachowcy, którzy potrafią priorytetyzować zagrożenia oraz opisywać niepożądane zjawiska w sposób syntetyczny.
2. Odrębnym wyzwaniem, wynikającym z coraz większej liczby danych, pozostaje tworzenie nowych narzędzi i bieżące usprawnianie już istniejących, w tym programów komputerowych, które pomagają analitykom sprawnie przetwarzać i porządkować zgromadzoną wiedzę.
3. W Polsce za przygotowywanie analiz na temat potencjalnych zagrożeń bezpieczeństwa państwa odpowiada wiele podmiotów. Często mają one podobne kompetencje, dlatego może dochodzić do niepotrzebnego dublowania się wysiłków w sferze rozpoznawania, gromadzenia i przetwarzania informacji. Z tego względu istotna wydaje się stała intensyfikacja współpracy pomiędzy nimi, w tym również polegającej na wymianie wiedzy, w celu osiągnięcia efektu synergii.
4. Warto rozpocząć dyskusję na temat zreformowania systemu bezpieczeństwa, w tym utworzenia jednego, centralnego podmiotu lub przekształcenia już istniejącego (np. Rządowego Centrum Bezpieczeństwa), który zajmowałby się analizowaniem informacji uzyskanych od służb specjalnych oraz urzędów. Następnie jego zadaniem byłoby przygotowanie każdego dnia jednego kompleksowego materiału, którego odbiorcami byłyby najważniejsze osoby w państwie. Ten wniosek wydaje się słuszny, jeśli weźmie się pod uwagę postulaty zgłaszane również przez byłego szefa Służby Wywiadu Wojskowego Andrzeja Kowalskiego (w 2013 r. wskazywał on na konieczność utworzenia przy koordynatorze służb specjalnych Centrum Analiz Strategicznych[53]), autorów *Białej Księgi Bezpieczeństwa Narodowego*[54] czy innych ekspertów

[53] *Plan zmian w służbach opracowywany od kilku lat*, http://niezalezna.pl/73124-plan-zmian-w-sluzbach-opracowywany-od-kilku-lat-znamy-szczegoly-wideo [dostęp: 13 V 2017].

[54] Twórcy tego dokumentu sygnalizowali konieczność budowy „(…) komórki (biura, centrum, departamentu itp.) odpowiedzialnej za dokonywanie strategicznych syntez informacji dostarczanych

zajmujących się problematyką bezpieczeństwa (np. z Fundacji im. Kazimierza Pułaskiego[55]).

## Bibliografia

Albrecht K., *Inteligencja praktyczna. Sztuka i nauka zdrowego rozsądku*, Gliwice 2009, Helion.

Aleksandrowicz T.R., *Analiza informacji w administracji i biznesie*, Warszawa 1999, Wyższa Szkoła Handlu i Prawa.

*Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2013, Biuro Bezpieczeństwa Narodowego.

Drabik L., Sobol E., *Słownik języka polskiego*, Warszawa 2005, Wydawnictwo Naukowe PWN.

*Global National Security and Intelligence Agencies Handbook*, Washington 2015, International Business Publications.

Janczak J., Nowak A., *Bezpieczeństwo informacyjne. Wybrane problemy*, Warszawa 2013, AON.

Janis I., *Groupthink*, „Psychology Today" 1971, nr 6.

Konieczny J., *Analiza informacji w dziedzinie bezpieczeństwa państwa*, Warszawa 2014, ABW.

Korzeniowski L.F., *Podstawy nauk o bezpieczeństwie*, Warszawa 2012, Difin.

Liderman K., *Bezpieczeństwo informacyjne*, Warszawa 2012, Wydawnictwo Naukowe PWN.

Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2008, Wydawnictwo Adam Marszałek.

Liedel K., *Zwalczanie terroryzmu międzynarodowego w polskiej polityce bezpieczeństwa*, Warszawa 2010, Difin.

Liedel K., Piasecka P., Aleksandrowicz T.R., *Analiza informacji. Teoria i praktyka*, Warszawa 2012, Difin.

*Obwieszczenie Prezesa Rady Ministrów z dnia 14 września 2016 r. w sprawie ogłoszenia jednolitego tekstu zarządzenia Prezesa Rady Ministrów w sprawie nadania statutu Agencji Wywiadu* (M.P. z 2016 r. poz. 936).

przez służby specjalne i wypracowywanie zintegrowanych ocen na potrzeby kierowania bezpieczeństwem narodowym. Jej zadaniem byłoby zbieranie informacji od wszystkich służb państwa odpowiedzialnych za poszczególne sfery bezpieczeństwa, a następnie dokonywanie ich analizy i oceny na potrzeby najwyższych organów kierowania państwem". Zob. *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2013, s. 210.

[55] G. Małecki, *Reforma służb specjalnych z perspektywy 15 lat*, https://pulaski.pl/wp-content/uploads/2015/02/Raport_reforma_sluzb__FKP.pdf [dostęp: 13 V 2017].

Potejko P., *Bezpieczeństwo informacyjne*, w: *Bezpieczeństwo państwa*, K.A. Wojtaszczyk, A. Materska-Sosnowska (red.), Warszawa 2009, Oficyna Wydawnicza ASPRA.

Sienkiewicz P., *10 wykładów*, Warszawa 2005, AON.

## Akty prawne

*Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* (t.j.: DzU z 2019 r. poz. 1398, ze zm.).

*Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym* (t.j.: DzU z 2019 r. poz. 1921, ze zm.).

*Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego* (t.j.: DzU z 2019 r. poz. 687).

*Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (t.j.: DzU z 2020 r. poz. 27).

*Ustawa z dnia 12 października 1990 r. o Straży Granicznej* (t.j.: DzU z 2020 r. poz. 305).

*Ustawa z dnia 6 kwietnia 1990 r. o Policji* (t.j.: DzU z 2020 r. poz. 360).

*Zarządzenie nr 163 Prezesa Rady Ministrów z dnia 26 września 2018 r. w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego* (M.P. z 2018 r. poz. 927).

*Zarządzenie nr 106 Prezesa Rady Ministrów z dnia 3 lipca 2018 r. zmieniające zarządzenie w sprawie nadania statutu Agencji Wywiadu* (M.P. z 2018 r. poz. 660).

*Zarządzenie Ministra Obrony Narodowej z dnia 13 czerwca 2018 r. zmieniające zarządzenie w sprawie nadania statutu Służbie Wywiadu Wojskowego* (M.P. z 2018 r. poz. 694).

*Zarządzenie Ministra Obrony Narodowej z dnia 21 kwietnia 2017 r. w sprawie nadania statutu Służbie Kontrwywiadu Wojskowego* (M.P. z 2017 r. poz. 431).

*Zarządzenie Nr 72 Prezesa Rady Ministrów z dnia 6 października 2010 r. w sprawie nadania statutu Centralnemu Biuru Antykorupcyjnemu* (M.P. z 2010 nr 76 poz. 953).

## Źródła internetowe

http://niezalezna.pl/73124-plan-zmian-w-sluzbach-opracowywany-od-kilku-lat-znamy-szczegoly-wideo [dostęp: 3 IX 2019].

http:// https://rcb.gov.pl/centrum-operacyjno-analityczne-2/ [dostęp: 3 IX 2019].

http://sjp.pwn.pl/sjp/;3067966 [dostęp: 3 IX 2019].

http://strazgraniczna.pl/pl/straz-graniczna/struktura-sg/komenda-glowna-sg/komorki-organizacyjne-k/zarzad-do-spraw-cudzozi/1909,Zarzad-do-Spraw-Cudzoziemcow-Komendy-Glownej-Strazy-Granicznej.html [dostęp: 3 IX 2019].

http://www.policja.pl/pol/kgp/gabinet-komendanta-glo/ [dostęp: 3 IX 2019].

http://www.policja.pl/pol/kgp/glowny-sztab-policji [dostęp: 3 IX 2019].

https://bits.blogs.nytimes.com/2009/12/09/the-american-diet-34-gigabytes-a-day/?_r=0 [dostęp: 3 IX 2019].

https://pulaski.pl/wp-content/uploads/2015/02/Raport_reforma_sluzb__FKP.pdf [dostęp: 3 IX 2019].

https://strazgraniczna.pl/pl/straz-graniczna/struktura-sg/komenda-glowna-sg/komorki-organizacyjne-k/biuro-analityczno-sytua/7895,Biuro-Analityczno-Sytuacyjne.html [dostęp: 9 XII 2019].

https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf [dostęp: 3 IX 2019].

## Abstrakt

W tekście przedstawiono zagadnienia dotyczące analizy informacji i jej rolę w zapewnianiu bezpieczeństwa państwa. W pierwszej części zwrócono uwagę na teoretyczne aspekty przetwarzania wiadomości istotnych z punktu widzenia decydentów, w tym kwestie definicyjne, sposoby pozyskiwania informacji oraz rodzaje analizy danych. W głównej części tekstu wskazano na wiele podmiotów odpowiedzialnych za dostarczanie analiz politykom pełniącym funkcje kierownicze w państwie. We wnioskach postulowano zintensyfikowanie współpracy w zakresie przepływu informacji między poszczególnymi komponentami systemu bezpieczeństwa państwa oraz powołanie nowej instytucji odpowiedzialnej za koordynację i opracowywanie zbiorczych produktów analitycznych m.in. dla prezydenta RP i Prezesa Rady Ministrów.

**Słowa kluczowe**: analiza, informacja, bezpieczeństwo narodowe, służby specjalne, proces decyzyjny.

## Abstract

The article presents the issue of data analysis in the process of providing national security. In the first part, there were highlighted theoretic aspects, including

definitions of terms data and analysis or means of collecting information. Moreover, there was shown types of analysis and the intelligence cycle. In the second part, the author pointed out legal frames in the field of Polish security institutions which are responsible for preparation of analytical products. In conclusion, the author suggested i.a. intensification of cooperation between those agencies.

**Keywords**: analysis, data, national security, intelligence services, decision making process.