

ANDRZEJ ŻEBROWSKI
IZABELA SZKURŁAT

ROLA INFORMACJI W ZARZĄDZANIU KRYZYSOWYM WYBRANE ASPEKTY

THE ROLE OF INFORMATION IN CRISIS MANAGEMENT SELECTED ASPECTS

Abstract. The changing conditions of the functioning of a country(ies) generate many complex threats that hinder and sometimes prevent the performance of basic tasks by individuals, social groups, a nation and a state. The scale and dynamics of occurring threats very often surprise both rulers and societies. In order to avoid a critical situation, eligible civil and military entities must continuously secure their information needs. It is essential to appreciate the importance of information, to be able to use it to prevent or minimize the consequences of a critical situation. This means the need to build the information system of the state, as well as subsystems at every level of its management, which are the basis for the decision-making process. Setting and evaluating tasks, the skillful use of information resources in the state crisis management process, all allow for its safe functioning in both internal and international environment.

Keywords: information; information warfare; crisis management.

WPROWADZENIE

Człowiek i informacja są ze sobą ściśle powiązane. To zależność sprawia, że jednostka, grupa społeczna, naród, państwo w zmieniającym się środowisku międzynarodowym i narodowym nieustannie poszukują informacji użytecznych

Prof. dr hab. inż. ANDRZEJ ŻEBROWSKI – Wyższa Szkoła Bezpieczeństwa Publicznego i Indywidualnego „APEIRON” w Krakowie, Wydział Bezpieczeństwa i Nauk Społeczno-Prawnych; adres do korespondencji: ul. Basztowa 10, 31-143 Kraków; e-mail: andrzejzebrowski@onet.pl; ORCID: <https://orcid.org/0000-0002-2779-9444>.

Dr IZABELA SZKURŁAT – Uniwersytet Pomorski w Słupsku, Instytut Bezpieczeństwa i Zarządzania; adres do korespondencji: ul. Kozińskiego 6-7, 76-200 Słupsk; e-mail: izabela.szkulat@upsl.edu.pl; ORCID: <https://orcid.org/0000-0001-6320-8421>.

z ich punktu widzenia, które zdominowane są przez ogólnoświatowy konflikt informacyjny. Przemiany cywilizacyjne są tym wyznacznikiem, który określa potrzeby informacyjne. Brak dostępu do informacji o określonych parametrach wymaga dostępu do takich źródeł znajdujących się w osobowej i technicznej przestrzeni informacyjnej, które pozwolą na zabezpieczenie potrzeb informacyjnych podmiotów uczestniczących w zarządzaniu sytuacją kryzysową. Informacje się starzeją, występują luki i szумы informacyjne, wiele podmiotów w procesie celowego i zorganizowanego działania zakłócają istniejące procesy, systemy informacyjne. Trwający postęp w technikach teleinformatycznych i komunikacyjnych sprawia, że mamy dostęp do informacji niemal w czasie rzeczywistym. Informacja nigdy nie występuje w czystej postaci, dlatego tak ważna jest wieloźródłowość i działalność analityczno-studyjna. Informacja to wiedza, to decyzje i skuteczne działania. Bez informacji ważnej i użytecznej trudno mówić o skutecznym zarządzaniu kryzysowym. W materiale wskazana została rola i znaczenie informacji, stanowiącej podstawę realizacji najważniejszych funkcji przez państwo, a sytuacja kryzysowa jest szczególnym stanem państwa. Informacja, mapy informacji i mapy wiedzy to podstawa skutecznego zarządzania kryzysowego.

Główny problem badawczy sformułowano w następującej postaci: Jak informacja wpływa na bezpieczeństwo państwa i zarządzanie kryzysowe? Dodatkowo zadano pytania szczegółowe, a mianowicie: 1) Jak skutecznie należy zarządzać informacją na poziomie państwa w sytuacji kryzysowej? 2) Jaką rolę powinien pełnić system informacyjny? W badaniach zastosowano analizę dokumentów, obserwację i opisy, co umożliwiło weryfikację złożonego problemu. Uwzględniono również poglądy różnych autorów.

1. CHARAKTERYSTYKA ŚRODOWISKA DZIAŁANIA PAŃSTWA

Zachodzące procesy w skali globalnej, to pasmo złożonych zjawisk, zdarzeń i procesów, które rzutują na poziom bezpieczeństwa poszczególnych państw i środowiska międzynarodowego. Jest to środowisko kooperacji pozytywnej i negatywnej o zróżnicowanych podłożach, gdzie zagrożenia naturalne i celowe spowodowane działalnością człowieka stanowią największe wyzwanie dla ludzkości w XXI wieku. Towarzyszące im przemiany cywilizacyjne, w tym rewolucja w technikach teleinformatycznych i komunikacyjnych, a także Internet są wszechobecne i uzależniają nasze codzienne życie od tych zdobyczy.

W globalną przestrzeń bezpieczeństwa wpisują się szczególnie niebezpieczne zagrożenia, których źródłem jest zamierzona działalność człowieka w celu przetrwania, posiadania i ekspansji (Narski, 2004, s. 5). Globalne środowisko bezpieczeństwa międzynarodowego to przestrzeń przymusu, siły i przewagi, co jest domeną państw dysponujących złożonym potencjałem, który pozwala na narzucanie swojej woli politycznej, ekonomiczno-gospodarczej i wojskowej. Jest to obecnie bardzo niebezpieczny trend, będący źródłem wielu złożonych zagrożeń o charakterze militarnym i pozamilitarnym, a takim przykładem jest konflikt Rosja–Ukraina. Umieędzynarodowiony problem to zaangażowanie się wielu uczestników stosunków międzynarodowych z dominującą pozycją Stanów Zjednoczonych Ameryki. Na uwagę zasługuje szczególne zaangażowanie i wspieranie polityki zagranicznej USA, które po zakończeniu tzw. zimnej wojny są nadal w konflikcie z Rosją. USA w tym dwustronnym konflikcie z Rosją wykorzystuje państwa słabe i zależne, gdzie Ukraina jest tylko instrumentem. Towarzysząca temu konfliktowi retoryka i podejmowane decyzje w sferach politycznej, ekonomiczno-gospodarczej i wojskowej, są źródłem wielu wielopłaszczyznowych zagrożeń, w tym o charakterze kryzysowym. W otoczeniu walczących stron mamy kryzys w obszarze pozamilitarnym, który przekłada się na poziom bezpieczeństwa jednostki, grupy społecznej, narodów, państw i środowiska międzynarodowego.

Tak złożone środowisko bezpieczeństwa globalnego generuje wiele istotnych zagrożeń, gdzie jesteśmy świadkami masowego przemieszczania się ludności. Można z dużym prawdopodobieństwem założyć, że to zjawisko jest wykorzystywane przez wrogie ośrodki dla państw członkowskich NATO, Unii Europejskiej, państw trzecich ze szczególnym uwzględnieniem państw Europy Środkowo-Wschodniej zaangażowanych w realizację polityki USA. Stanowi to naturalne możliwości przenikania agentury obcych państw (nie tylko rosyjskiej), członków zorganizowanych grup przestępczych o charakterze transnarodowym, członków organizacji terrorystycznych, a także innych wrogich podmiotów. Na uwadze należy mieć także sankcje ekonomiczno-gospodarcze nałożone na Rosję i Białoruś, które również generują zagrożenia dla państw je wprowadzających i popierających. Przekładają się one bezpośrednio m.in. na bezpieczeństwo ekonomiczne państwa, społeczne (w tym finansowe, zdrowotne), a także militarne.

Trwający konflikt zbrojny Rosja–Ukraina, któremu towarzyszy globalna wojna informacyjna, to nieustanna propaganda, dezinformacja, manipulacja, kłamstwo, maskowanie, a także dezintegracja środowiska międzynarodowego, co jest widoczne w Unii Europejskiej i Sojuszu Północnoatlantyckim.

Ewolująca sytuacja polityczno-wojskowa i społeczna w strefie bezpośredniego konfliktu i w jego otoczeniu wymusiła na państwach podjęcie działań w ramach zaistniałego kryzysu pozamilitarnego. Przejście funkcjonowania struktur państwa na realizowanie zadań w stanie kryzysu, to czas intensywnych zadań rozpoznawczych sprowadzających się do monitorowania otoczenia zewnętrznego i wewnętrznego państwa, ze szczególnym uwzględnieniem otoczenia zewnętrznego na styku uczestników konfliktu zbrojnego (Rosja–Ukraina) oraz państw niezaangażowanych bezpośrednio w jego przebieg.

Istniejący kryzys zdominował aktualne środowisko bezpieczeństwa, gdzie państwa znalazły się w impasie, gdzie brak racjonalnych decyzji i działań ukierunkowanych na zakończenie konfliktu Rosja–Ukraina.

Ta złożona sytuacja wymusza na państwach będących pośrednimi uczestnikami trwającego konfliktu (bez zaangażowania militarnego) uruchomienie systemu zarządzania kryzysowego. Podstawę jego funkcjonowania stanowi zabezpieczanie potrzeb informacyjnych uprawnionych podmiotów zarządzających państwem na poziomie: strategicznym, operacyjnym i taktycznym przez wyspecjalizowane służby, organy i instytucje państwa, właściwe w sferze bezpieczeństwa i porządku publicznego (Piwowarski i Rozwadowski, 2016, s. 348).

Bezpieczeństwo wewnętrzne i zewnętrzne państwa wiąże się z jakością zarządzania, w tym kryzysowego. Jak wskazują badacze, kluczowe jest tu zwłaszcza „sterowanie procesami, zasobami i informacjami dla realizacji zamierzonych celów w warunkach istniejących możliwości i ograniczeń oraz zgodnie ze społeczną racjonalnością działań: politycznych, finansowych, gospodarczych, wojskowych” (Penc, 1998, s. 5). Ewolująca globalna przestrzeń bezpieczeństwa, gdzie podmioty państwowe i niepaństwowe mają zróżnicowane interesy polityczne, ekonomiczno-gospodarcze i wojskowe, wykorzystują posiadane instrumenty polityczno-militarne i niemilitarne. Ten rodzaj działalności ma najczęściej charakter kooperacji negatywnej, generującej wiele złożonych zagrożeń o charakterze kryzysowym. Dlatego tak ważne jest kompleksowe podejście zarządzania bezpieczeństwem państwa, w tym i kryzysowym.

2. ZNACZENIE INFORMACJI

Skuteczne zarządzanie kryzysowe na poziomie państwa, województwa, powiatu i gminy zależy od posiadanych informacji. Informacja jest tu rozumiana jako każdy czynnik, dzięki któremu obiekt odbierający ją (człowiek, organizacja, siły zbrojne, instytucje państwowe, rządowe, administracja samorządowa,

służby) może polepszyć swoją znajomość otoczenia (w tym potencjalnego partnera lub przeciwnika), a dzięki temu sprawniej podjąć i zrealizować swoje działania (J.L., 1998, s. 16).

Skuteczność podmiotów uczestniczących w procesie zarządzania kryzysowego zależy od: wiedzy o tym, na co przeznaczają czas; koncentracji na otoczeniu zewnętrznym i wewnętrznym państwa; koncentracji na głównych kierunkach działania, podejmowania skutecznych decyzji (Penc, 1998, s. 6-7). Walka o informację toczy się od chwili ukształtowania się pierwszych interesów grupowych. Jest ona prowadzona w każdym obszarze, ze szczególnym wskazaniem na polityczny, społeczny, gospodarczy, militarny, walki z przestępczością transgraniczną czy terroryzmem. Jej cel strategiczny, to zdobycie przewagi informacyjnej nad przeciwnikiem, wprowadzanie go w błąd, uzyskanie zaskoczenia, a tym samym odniesienie sukcesu.

Z punktu widzenia potrzeb operacji informacyjnych można wyróżnić cztery zasadnicze formy informacji:

1) informacja o zawartości jako prosty wykaz danych o liczbie, lokalizacji i typach artykułów (tematów),

2) informacja w formie opisu kształtu i układu obiektów,

3) informacja behawioralna jako trójwymiarowa symulacja ułatwiająca przewidzenie zachowania przynajmniej obiektów fizycznych, a w końcowej formie osiągnięcie *poziomu gry wojennej* dającej sposobność przedstawienia przebiegu określonej akcji,

4) informacja o akcji umożliwiająca organom sztabowym szybkie podjęcie odpowiednich działań (J.L., 1999, s. 79).

Informacja jest elementem wiedzy, faktem, wiadomością, komunikatem lub wskazówką gromadzoną, komunikowana lub przekazywana komuś za pomocą jakiegoś kodu lub języka (Barczak i Sydoruk, 2022, s. 22). Każda wiadomość, która ma stanowić wartość dla procesu zarządzania kryzysowego, powinna być pełna i wyczerpująca. Poza treścią powinna zawierać w swoim składzie elementy pozwalające na jej identyfikację i ochronę, tzn.: czas nadania, czas odbioru, temat, nadawcę, odbiorcę i status (niesklasyfikowana, zastrzeżona, poufna, tajna, ściśle tajna) (Barczak i Sydoruk, 2022, s. 22).

Ponadto, w zarządzaniu kryzysowym potrzebne są koncepcje, metody i motywacja, wiedza specjalistyczna i wyobrażenia, potrzebny jest też czas na przemyślenia, ale informacje są niewątpliwie „najważniejsze, gdyż pozwalają poznać zmiany zachodzące w otoczeniu organizacji [państwa, województwa, powiatu i gminy, oraz otoczeniu zewnętrznym państwa – przyp. autorzy] i odpowiednio wcześniej dostosować do nich jej potencjał i przyszłe możliwości”

(Penc, 1998, s. 106). Oznacza to, że dostęp do wiedzy i zasobów informacyjnych, umożliwiających wczesną weryfikację zagrożeń lub reakcję na już zaistniałe, jest dla systemu zarządzania kryzysowego sprawą priorytetową (Kwečka, 2009, s. 336).

Należy mieć świadomość tego, że podmioty zarządzające bez znajomości środowiska bezpieczeństwa międzynarodowego i otoczenia wewnętrznego państwa oraz zachodzących tam procesów (generujących wiele złożonych zagrożeń), nie są w stanie budować scenariuszy, redukować niepewność działania, podejmować właściwe decyzje, wskazywać możliwe koncepcje rozwoju, a przede wszystkim budować strategie, dla których rozpoznanie zagrożeń i szans w otoczeniu, a także słabych i mocnych stron przeciwnika i własnych stanowią bazy danych, znajdujących się w różnych systemach informacyjnych właściwych podmiotów. Oznacza to, że posiadanie odpowiednich informacji jest dzisiaj dla każdego zarządzającego w sytuacji kryzysowej sprawą o fundamentalnym znaczeniu. Są one również traktowane jako podstawowy czynnik, który ma wpływ na skuteczność i jakość zarządzania, a także decyduje o sukcesie, a nawet porażce państwa.

Warto mieć na uwadze to, że istotą aktywności państwa w środowisku bezpieczeństwa międzynarodowego jest prowadzenie wielu złożonych działań, które obejmują zarówno formy kooperacji pozytywnej, jak i negatywnej. Państwo, jako organizacja społeczna, charakteryzuje się aktywnością wewnętrzną i zewnętrzną, gdyż każde państwo realizuje funkcję zewnętrzną i wewnętrzną i koncentruje swoją aktywność wokół zarządzania (Wojtaszczyk, 1998, s. 12, 22). Wiedza i świadomość istniejących zagrożeń wymaga nie tylko aktywności informacyjnej, ale i racjonalnych działań.

Trwające zmiany cywilizacyjne dotyczą praktycznie wszystkich sfer działania państwa, a także podmiotów pozapaństwowych. Na szczególną uwagę zasługują jednak procesy związane z technikami teleinformatycznymi i komunikacyjnymi, które zrewolucjonizowały oraz zdominowały nasze codzienne życie. Trudno bowiem wyobrazić sobie funkcjonowanie w otoczeniu wewnętrznym i zewnętrznym państwa bez dostępu do wspomnianych technik, Internetu. Państwa (także podmioty pozapaństwowe) funkcjonują w globalnej przestrzeni informacyjnej, gdzie wykonują przypisane im zadania w osobowej i technicznej przestrzeni informacyjnej. Podmioty państwowe i pozapaństwowe generują swoje cele w otoczeniu wewnętrznym i zewnętrznym zarówno przez aktywność informacyjną, jak i praktyczne działania w sferach: politycznej, ideologicznej, kulturowej, społecznej, ekonomiczno-gospodarczej, naukowej, wojskowej, walki z przestępczością zorganizowaną o charakterze transnaro-

dowym z terroryzmem międzynarodowym i innymi podmiotami naruszającymi istniejący porządek konstytucyjny.

Aktywność informacyjna może skutkować decyzjami o wprowadzeniu sankcji ekonomicznych, do użycia sił zbrojnych włącznie. Przyjmuje się, że w warunkach współczesnego świata podstawową formą każdej akcji w stosunku do innego państwa (państw) jest informacja docierająca do świadomości sprawujących władzę (Szpyra, 2003, s. 51). Należy jednak zawsze mieć świadomość tego, że w skrajnych przypadkach przemoc fizyczna zawsze będzie środkiem pozwalającym zarówno podmiotom państwowym, jak i pozapaństwowym na realizację swoich partykularnych celów.



Wykres 1. Zewnętrzne sfery oddziaływania oraz sfery zasilania procesów wewnętrznych

Źródło: Opracowanie własne na podstawie: Szpyra, 2003, s. 50.

Trwające przemiany cywilizacyjne są źródłem postępu i zagrożeń, co sprawia, że informacja współcześnie decyduje o sposobie wykorzystywania przez państwo (państwa) posiadanych zasobów (osobowych i materiałowych) i możliwości, co bezpośrednio przekłada się na zdolność dostosowania się do ewoluujących warunków i programowania swojego rozwoju w procesie poprzedzającym, a także w trakcie trwania sytuacji kryzysowej.

Podmioty będące uczestnikami zarządzania kryzysowego muszą znać swoje potrzeby informacyjne i wiedzieć, jakie informacje są konieczne do tworzenia planów, gromadzenia zasobów i wykonywania podstawowych funkcji i działań. Powinny również określić, jakie potrzeby informacyjne są zaspokajane w niedostatecznym stopniu, a jakie nie są w ogóle zaspokajane, a także w jakim stopniu przepływ informacji służy zarządzającym w procesie podejmowania decyzji i sprawnego kierowania (Penc, 1998, s. 107).

Informacja dla podmiotów realizujących ustawowe zadania w sferze zarządzania kryzysowego państwem powinna zapewniać wiedzę wspierającą proces decyzyjny, przekładającą się na realizację zadań, a tym samym celów w sytuacjach kryzysowych. Informacja powinna zmniejszać nieokreśloności lub niepewności co do stanu albo dalszego rozwoju sytuacji, której ta wiadomość dotyczy (Kroenke, 1989, s. 14). Oznacza to, że podmioty decyzyjne na każdym poziomie zarządzania kryzysowego muszą uwzględniać wszelkie symptomy i przesłanki uzasadniające uruchomienie systemu zarządzania kryzysowego, stawiać zadania dla aparatu zasilającego w informacje o odpowiedniej szczegółowości i terminie wykonalności.

Z punktu widzenia użytkowników informacji w procesie zarządzania kryzysowego powinna się ona charakteryzować pewnymi (istotnymi) cechami, do których zalicza się: aktualność, jakość, istotność, ścisłość, cennaść, kompletność, kosztowność, dostępność, spójność, ekonomiczność, powiązanie z wykonywanymi zadaniami. Pamiętać należy przy tym o znaczeniu występujących zakłóceń (Żebrowski, 2012, s. 114).

3. WALKA W OBSZARZE INFORMACJI

Nowoczesne koncepcje zarządzania kryzysowego oparte są na tworzeniu przewagi w sferze bezpieczeństwa (wewnętrznego i zewnętrznego) na podstawie kontrolowanej i rozstrzygającej przewadze informacyjnej i technologicznej. Potencjał informacyjny zabezpieczający potrzeby informacyjne uczestników zarządzania kryzysowego, jako element potencjału informacyjnego państwa (w tym o charakterze niejawnym), tworzą zasoby informacyjne systemu bezpieczeństwa i porządku publicznego oraz systemy informacyjne kształtujące krytyczną infrastrukturę informacyjną państwa (Szypra, 2003, s. 100).

Skala i dynamika zachodzących zmian w globalnej przestrzeni bezpieczeństwa narodowego i otoczeniu zewnętrznym państwa (państw), a także

towarzyszące im zagrożenia naturalne i celowe wymagają dostępu do szerokiego spektrum informacji.

Potrzeby informacyjne wynikają z istniejących luk informacyjnych, które są postrzegane i odnoszą się zawsze do konkretnego obserwatora. Należy podkreślić, że są one wrażliwe na czynniki czasu, który w asymetrycznym środowisku międzynarodowym, skali i dynamice występujących zagrożeń, gdzie nieprzewidywalność i chaos dają o sobie znać, ma kluczowe znaczenie dla skutecznego zarządzania kryzysowego. Na zakres i informacyjną strukturę luki informacyjnej oddziałują czynniki obiektywne oraz subiektywne. Pierwszy z nich ma ścisły związek z obiektywną wiedzą podmiotów zarządzających i dotyczy celowości prowadzonych obserwacji środowiska podatnego na zagrożenia, oraz z możliwością realizacji takiej obserwacji w ramach zarządzania kryzysowego. Stąd przeprowadzenie obserwacji i stopień jej kompletności, osiągniętej przydatności jest najczęściej kompromisem między oczekiwaniami a możliwościami ich realizacji. Z kolei czynniki subiektywne związane są z faktem, że luka jest zawsze czyjaś, a więc adresowana do konkretnego obserwatora (Flakiewicz, 2002, s. 31), który powinien dążyć do jej zminimalizowania.

Bogata historia walki w obszarze informacji wskazuje, jak ważna jest informacja dla ostatecznego wyniku działań militarnych i pozamilitarnych, w tym i dla zarządzania kryzysowego. Szczególną uwagę przypisuje się na problemy dominacji informacyjnej nad przeciwnikiem zewnętrznym i wewnętrznym państwa. W dobie powszechnej informatyzacji pola konfrontacji pokonanie przeciwnika w sferze informacyjnej może okazać się czynnikiem decydującym o ogólnym sukcesie w walce zbrojnej i niezbrojnej (Janczak, 2001, s. 5). Jednym z komponentów walki w obszarze informacji jest zakłócanie informacyjne, stanowiące zespół skoordynowanych przedsięwzięć i działań, które dostosowane są do zakłócania procesów zarządzania bezpieczeństwem państwa, zarządzania kryzysowego, dowodzenia wojskami i kierowania środkami walki (Janczak, 2001, s. 12). Zakłócanie informacyjne stanowi także element przeciwdziałania pozyskiwaniu informacji przez podmioty do tego nieuprawnione. W zależności od potrzeb zarządzania bezpieczeństwem państwa, zarządzania kryzysowego, dowodzenia wojskami, zakłócanie informacyjne realizują m.in.: kierownictwo państwa, siły i środki walki elektronicznej, działań psychologicznych, działań specjalnych i wojsk uczestniczących w walce (Janczak, 2001, s. 12). Aktywnymi uczestnikami tego złożonego procesu są również podmioty właściwe w sferze bezpieczeństwa i porządku publicznego, którym ustawodawca przypisał wiele zadań z obszaru zarządzania kryzysowego. Z uwagi na posiadane siły i środki, a przede wszystkim uprawnienia, do tych podmiotów

zalicza się m.in.: Policję, wywiad i kontrwywiad (cywilny i wojskowy), Straż Graniczną, Żandarmerię Wojskową, Państwową Straż Pożarną. Zakłócanie informacyjne należy postrzegać jako wszelkie formy oddziaływania na otoczenie zewnętrzne i wewnętrzne państwa (obszary zdobywania informacji – rejestratory danych, sygnały będące ich nośnikami, zbiory danych, programy, biblioteki itp.), które doprowadza do zaniku informacji pożądanej, jej definiowania (Janczak, 2001, s. 14) lub fizycznego zniszczenia.

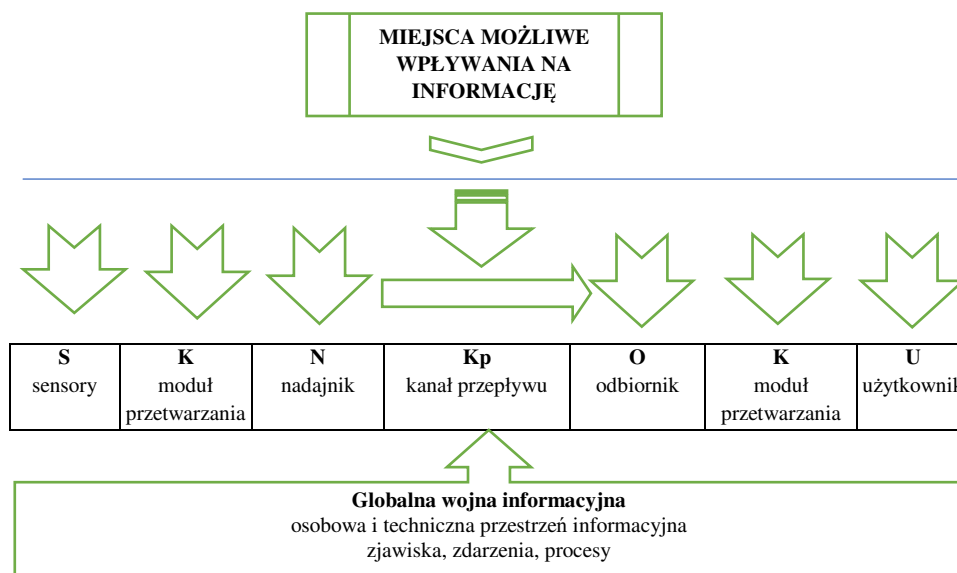
Istotą zakłócania informacyjnego w globalnej przestrzeni informacyjnej jest maksymalne ograniczanie napływu danych prawdziwych i powodowanie przez to zniekształcenia obrazu obszaru działania w sferach militarnej i pozamilitarnej, a także związanych z zarządzaniem kryzysowym. Ten fałszywy obraz pola konfrontacji negatywnej bezpośrednio przekłada się na proces decyzyjny oraz podejmowane działania (Komorowska, 2021, s. 196-197).

Tabela 1. Funkcje zakłócania informacyjnego

Lp.	FUNKCJE	TREŚĆ
1	Pozorowanie	ma na celu wprowadzanie w błąd przeciwnika; jego celem jest udostępnienie przeciwnikowi takich postaci danych, które po przetworzeniu będą przedstawić sytuację nierealną, a zarazem maksymalnie stwarzającą pozory działań rzeczywistych.
2	Dezorganizacja	pracy systemów zarządzania państwem, dowodzenia wojskami oraz dążenie do fizycznej destrukcji nośników danych.

Źródło: Janczak, 2001, s. 15.

Należy mieć na uwadze to, że walka w obszarze informacji przybiera formy aktywne i pasywne. Do form aktywnych (ofensywnych) zalicza się działania o charakterze zaczepnym, których celem jest zdobycie informacji oraz zakłócenie działań systemów zarządzania bezpieczeństwem państwa, zarządzania kryzysowego, łączności, rozpoznania, dowodzenie wojskami i kierowanie ogniem. Z kolei do pasywnych (defensywnych) należą działania o charakterze obronnym, tj. ochrona własnego systemu informacyjnego.



Wykres 2. Miejsce możliwego modyfikowania treści informacji

Źródło: Opracowanie własne na podstawie: Szpyra, 2003, s. 80.

W procesie zarządzania kryzysowego informacja spełnia kilka funkcji. Z punktu widzenia jego potrzeb i użyteczności można wyróżnić trzy rodzaje informacji: które mają służyć pomocą w podejmowaniu decyzji; które mają zapewnić odpowiednią komunikację między przełożonym a pracownikami; które mają zaspokoić innych użytkowników (Penc, 1998, s. 111).

Skuteczne zarządzanie kryzysowe państwem wymaga dostępu do szerokiego spektrum informacji. Uczestnicy zarządzania kryzysowego muszą dostosowywać się do zachodzących zmian w otoczeniu państwa (państw), muszą rozwiązywać coraz trudniejsze i coraz bardziej złożone problemy związane z pojawiającymi się zagrożeniami i szybko reagować w celu niedopuszczenia do ich wystąpienia lub zminimalizowania negatywnych następstw, które mogą zwrócić się ku np. państwu. To również waluta zarządzania, dowodzenia, łączności, rozpoznania i kierowania bronią precyzyjnego rażenia. Zarówno kooperacja pozytywna, jak i negatywna wymaga wypracowania przewagi informacyjnej i szybkich decyzji, a także prowadzenia działań zakłócających, aby nie dopuścić do osiągnięcia tego celu przez przeciwnika. Globalna przestrzeń bezpieczeństwa międzynarodowego zdominowana przez wspomnianą eksplozję informacyjną, okazała się bardziej rozległa niż militarna sfera zainteresowania (Szpyra, 2003, s. 85).

Wojna informacyjna koncepcyjnie podporządkowana operacjom informacyjnym jest definiowana jako operacje informacyjne prowadzone w czasie kryzysu lub konfliktu (a także w czasie pokoju) w celu zrealizowania lub wspierania specyficznych zamiarów w stosunku do danego przeciwnika lub przeciwników (J.L., 1999, s. 78).

Tabela 2. Przebieg walki w obszarze informacji

Lp.	ETAPY PRZEBIEGU WALKI W OBSZARZE INFORMACJI	
1	Zdobywanie	proces zdobywania informacji polega na ich gromadzeniu, segregowaniu, wstępnym analizowaniu, wyciąganiu pierwszych wniosków kontroli prawdziwości.
2	Walka radioelektroniczna	obejmuje elektroniczne rozpoznanie, obezwładnianie i dezorganizowanie pracy środków i systemów elektronicznych przeciwnika oraz osłonę własnych systemów dowodzenia i łączności.
3	Mylenie	należy rozumieć jako szereg przedsięwzięć związanych z maskowaniem, dezinformacją, wprowadzaniem w błąd, zaskoczeniem, identyfikacją, nawigacją oraz wprowadzaniem wirusów do sieci komputerowych.
4	Przekaz	obejmuje utrzymanie łączności, rozwinięcie sieci komputerowych na polu walki oraz multimedialną, elektroniczną korespondencję.
5	Opracowanie	to kolejny etap walki w obszarze informacji, obejmuje multimedialne opracowanie, fuzję i integrację danych.
6	Wsparcie procesu decyzyjnego	polega na umożliwieniu pracy zarządzających, dowództw i sztabów w cyfrowych systemach dowodzenia w czasie wypracowania decyzji, tj.: analizy informacji, oceny położenia, poszukiwania alternatyw, podjęcia samej decyzji, planowania, wykonania planu operacyjnego, postawienia zadań (dyrektywa, rozkaz), organizacji operacji oraz organizacji kierowania, dowodzenia i kontroli. Na tym etapie ważnym zadaniem walki w obszarze informacji jest elektroniczne kierowanie ogniem.
7	Ochrona informacji	obejmuje opracowanie nowoczesnych systemów ochrony informacji, skryte dowodzenie (kierowanie), cenzurę, identyfikację i nawigację.

Źródło: S.P., 1997, s. 30- 40.

Należy pamiętać o tym, że na każdym poziomie zarządzania kryzysowego powinien być zbudowany system wczesnego alarmowania i powiadamiania o zagrożeniach, który pozwoli na ich poznanie i podjęcie odpowiednich decyzji/działań. Oznacza to konieczność monitorowania otoczenia zewnętrznego i wewnętrznego państwa. System monitoringu należy traktować jako „system alarmowania, który służy do przekazywania dla określonego zespołu ludzi

bądź pojedynczych osób [...] sygnału (znaku umownego) do wykonania ustalonego wcześniej polecenia, zarządzenia, rozkazu nakazującego natychmiastowe przejście do określonego działania, zwykle w wypadku grożącego niebezpieczeństwa napadu (powietrznego, jądrowego, chemicznego, biologicznego) ze strony nieprzyjaciela” (*Leksykon wiedzy wojskowej*, 1973, s. 13).

Pozyskiwanie informacji, sposoby ich zbierania, gromadzenia i przepływu powinny być zorganizowane na zasadzie systemu, który obejmowałby całe zbiory informacyjne (zasoby informacyjne) oraz te elementy, które umożliwiają zasilanie, nabywanie i dostarczanie użytkownikom tych zasobów (Kisielnicki, 1992, s. 15). Współczesny system informacyjny powinien być rozumiany nowoczesnie, tzn. jako komputerowa metoda zbierania, opracowania, przechowywania (kodowania), aktualizowania, odtwarzania i przetwarzania danych oraz ich dostarczania w najprzydatniejszej formie kadrze kierowniczej do realizacji zadań i celów organizacji (w aspekcie prowadzonych rozważań celów państwa, jakim jest jego bezpieczeństwo) (Penc, 1999, s. 116).

Podstawową cechą systemu informacyjnego jest to, że stanowi on usystematyzowaną i uporządkowaną sieć powiązań informacyjnych między poszczególnymi elementami obiektu i służy zaspokajaniu potrzeb informacyjnych odbiorców, wynikających z realizowanych przez nich funkcji (Błażejczyk, 2002, s. 93). To na podmiotach zarządzających spoczywa obowiązek stworzenia systemu informacyjnego na poziomach: instytucje centralne, województwo, powiat i gmina. Muszą one być kompatybilne i zapewniać dostęp uprawnionym użytkownikom. System ten powinien funkcjonować jako podsystem informacyjny państwa (ze szczególnym uwzględnieniem jego charakteru niejawnego). Nie ma możliwości zarządzania kryzysowego bez wymiany informacji pomiędzy podmiotami, które są do tego uprawnione (Żebrowski, 2012, s. 115).

System informacji powinien spełniać m.in. następujące warunki:

- 1) system powinien być dostosowany do potrzeb zarządzania kryzysowego i obejmować wszystkie jego obszary, wszystkie poziomy kierowania i poziomy decyzyjne,
- 2) system powinien dostarczać informacji kompleksowych i aktualnych, aby gmina, powiat, województwo i państwo reagowało na zmianę warunków wewnętrznych i zewnętrznych,
- 3) system powinien dostarczać informacji tym, którzy ich rzeczywiście potrzebują, i to informacji w formie nadającej się bezpośrednio (bez przetwarzania) do użytku i najdogodniejszej dla podjęcia ostatecznych decyzji,
- 4) system powinien zapewnić efektywne wykorzystanie informacji, które jest warunkowane szybkością i częstotliwością ich obiegu – oznacza to, że dane powinny być aktualne, kompletne i odpowiednio posegregowane, gdyż to ułatwia ich obieg,

- 5) droga przepływu informacji powinna być możliwie najkrótsza i zgodna ze strukturą organizacyjną państwa, województwa, powiatu i gminy, a poszczególne podsystemy informacji powinny stanowić prosty zbiór, który można sobie szybko przyswoić i wykorzystać w podejmowaniu praktycznych decyzji (sensowne, zwarte raporty),
- 6) algorytmy opracowania informacji powinny zapewnić śledzenie przebiegu procesów zarządzania, konstruowanie ocen, prognozowanie przebiegu wydarzeń,
- 7) koszty pozyskiwania i przetwarzania informacji powinny być niewysokie, metody ich zbierania, opracowywania, przechowywania i przepływu powinny uwzględniać możliwości komputeryzacji systemu informacyjnego, a forma ich prezentacji powinna być dostosowana do możliwości odczytywania przez zainteresowanych,
- 8) system powinien być zabezpieczony przed niepożądanym wpływem informacji nieformalnych i stale doskonalony, aby mógł zapewnić właściwy przepływ informacji (Penc, 1999, s. 116).

System informacyjny w zarządzaniu kryzysowym musi być spójny wewnętrznie (państwo, województwo, powiat, gmina – gmina, powiat, województwo, państwo), ponadto kompatybilny z analogicznymi systemami działającymi na poziomie UE i NATO (Żebrowski, 2012, s. 117). Oznacza to konieczność zbudowania jakościowo nowych narzędzi, które pozwolą na skuteczne zarządzanie, w tym i koordynowanie działań w sytuacjach kryzysowych o charakterze wielosektorowym.

Unia Europejska stworzyła i nadal rozbudowuje systemy powiadamiania i alarmowania, których obszary zainteresowania są zróżnicowane. Przedstawia je tabela 3.

Tabela 3. System powiadamiania i alarmowania UE

Lp.	SYSTEM POWIADAMIANIA I ALARMOWANIA
1	Europejska Agencja Kosmiczna (ESA)
2	Globalny Monitoring dla Środowiska i Bezpieczeństwa (GMES)
3	Centrum Satelitarne Unii Europejskiej (EUSC)
4	Instytut Unii Europejskiej Studiów nad Bezpieczeństwem (ISS)
5	System Wczesnego Ostrzegania i Alarmowania (EWRS)
6	System Wczesnego Powiadamiania i Wymiany Informacji o Zagrożeniach Radiologicznych bądź Nuklearnych (ECURIE)
7	System Ochrony Sieci Ostrzegania o Zagrożeniach dla Infrastruktury Krytycznej (CIWIN)
8	Bezpieczny Ogólny System Szybkiego Ostrzegania (ARGUS)
9	System Wczesnego Ostrzegania Przed Biologiczno-Chemicznymi Atakami i Zagrożeniami (RAS – BICHAT)
10	System Powiadamiania EUROPOLU

11	System Ostrzegania przed Wadliwymi Produktami (RAPEX)
12	System Szybkiego Ostrzegania o Niebezpiecznych Produktach Żywnościowych (RASFF)
13	Zintegrowany i Skomputeryzowany System Weterynaryjny (TARCES)
14	Europejski System Wczesnego Powiadomiania i Wymiany Informacji o Zdrowiu Roślin (EUROPHYT)
15	System Zgłaszania Chorób Zwierząt (ADNS)
16	Centrum Monitoringu i Informacji (MIC)
17	Europejska Sieć Umacniania Prawodawstwa (LEN)

Źródło: Opracowanie własne

Służby wywiadowcze zarówno państw UE, jak i NATO posiadają niezbędne informacje, które są istotne z punktu widzenia zarządzania kryzysowego. Dlatego też niezbędna jest ponadnarodowa wymiana informacji również na poziomie niejawnym (Żebrowski, 2012, s. 121). Narodowe służby specjalne aktywność operacyjną prowadzą w osobowej i technicznej przestrzeni informacyjnej. Służby wywiadowcze państw członkowskich UE i NATO posiadają również dostęp do informacji wywiadowczych zdobytych za pośrednictwem wywiadu satelitarnego, który jest uprawiany przez nieliczne państwa członkowskie.

Obok rozpoznania osobowego (HUMINT), które stanowi podstawowe narzędzie pracy służb wywiadowczych każdego państwa, warto również zwrócić uwagę na inne kategorie działalności rozpoznawczej, i tak:

- 1) rozpoznanie geoprzestrzenne (GEOIT), oznacza wykorzystywanie analizy obrazów oraz informacji geoprzestrzennych w celu opisanego, oceny i wizualizacji cech fizycznych i geograficznych, jakie zachodzą na ziemi,
- 2) rozpoznanie obrazowe (IMINT), umożliwia wytwarzanie danych rozpoznawczych na podstawie zobrazowania pochodzącego ze zdjęć fotograficznych (PHOTINT), radiolokatorów, przyrządów elektrooptycznych pracujących w podczerwieni i termowizyjnych oraz innych urządzeń. Aby można było wykorzystać określone dane, obraz przekazany musi być czysty, czytelny i jednoznacznie przedstawić obiekt zainteresowania – wtedy również można szukać potwierdzenia w innych źródłach lub przekazać dane do innych elementów wsparcia informacyjnego,
- 3) rozpoznanie pomiarowe i sygnaturowe (MASINT), obejmuje naukowe i techniczne analizy ilościowe oraz jakościowe parametrów technicznych i charakterystycznych cech [...] uzyskiwanych z przyrządów technicznych w celu identyfikacji źródeł, nadajników, urządzeń promieniujących, umożliwiających dalszą identyfikację i porównanie,
- 4) rozpoznanie sygnałów elektromagnetycznych (SIGINT), jest podstawą wytwarzania danych rozpoznawczych pochodzących z przechwytywania sygnałów elektromagnetycznych (Nowacki, 2002, s. 54-55).

Dla skutecznego zarządzania kryzysowego na terytorium państw członkowskich UE i NATO, a także na obszarach znajdujących się w ich zainteresowaniu, ważnym źródłem informacji jest wspomniane rozpoznanie satelitarne. Dane z rozpoznania satelitarnego pozwalają na zobrazowanie sytuacji w obszarach zainteresowania w czasie niemal rzeczywistym. Rozpoznanie satelitarne może być prowadzone zarówno w czasie pokoju, stanach kryzysu, jak i wojny. Według współczesnych koncepcji nie jest możliwe skuteczne zarządzanie kryzysowe bez zastosowania rozpoznania satelitarnego. Satelity w zależności od przeznaczenia dzielą się na: rozpoznawcze, komunikacyjne, naukowo-badawcze, geofizyczne, astronomiczne, meteorologiczne. System wspomagają także inne instrumenty, w tym m.in. AWACS (Żebrowski, 2012, s. 122). Suma sił i środków zaangażowanych do rozpoznawania sytuacji kryzysowej (w sferach militarnej i pozamilitarnej), przy wieloźródłowych informacjach pozwala na podejmowanie właściwych decyzji. Należy jednak mieć świadomość tego, iż musi to być proces, a informacje w procesie analityczno-studyjnym i wnioskowaniu powinny przekładać się na racjonalne decyzje i działania.

Obok zabezpieczenia potrzeb informacyjnych z poziomu UE i NATO, każde państwo członkowskie (w tym i Polska) zobowiązane jest do stworzenia narodowego systemu informacyjnego, który powinien opierać się na rozbudowanej infrastrukturze informacyjnej uwzględniającej sieć wewnętrzną i zewnętrzną łączącą uprawnione podmioty uczestniczące w zarządzaniu kryzysowym. Sieć wewnętrzna powinna być zorganizowana na zasadzie tzw. mapy informacyjnej zmieniającej się z biegiem czasu pod wpływem zmian otoczenia (gminy, powiatu, województwa, państwa). Taka mapa musi zawierać węzły informacyjne (składające się z grup pracowników, dokumentów, wyszukiwania danych i komunikowania) oraz linie przepływu informacji między węzłami, ustalone zgodnie z wymaganiami tzw. odwróconej piramidy informacyjnej, która oznacza, że tam, gdzie koncentruje się władza, potrzebne są informacje mniej szczegółowe, a bardziej skondensowane o szerokim przekroju, dające pogląd na całość działania organizacji (gminy, powiatu, województwa, państwa – przyp. autora) i jej powiązania z otoczeniem, ułatwiające zintegrowane zarządzanie kryzysowe (Ingalls, 1979, s. 113). Oznacza to, że system informacyjny zarządzania kryzysowego powinien zawierać informacje uszeregowane według pewnej hierarchii, a mianowicie dla celów strategicznych, operacyjnych i taktycznych.

Mapa informacyjna pozwala na stworzenie mapy wiedzy, gdzie ma miejsce zapisywana informacja przy jednoczesnym posługiwaniu się obrazem i tekstem. W zarządzaniu kryzysowym mapy wiedzy wykorzystywane są do:

- 1) określania potrzeb informacyjnych,
- 2) planowania,

- 3) zarządzania czasem i zadaniami,
- 4) analizowania,
- 5) wizualizacji koncepcji,
- 6) wsparcia uprawnionych podmiotów decyzyjnych,
- 7) prowadzenia prezentacji,
- 8) strukturalizacji wiedzy rozpoznawczej,
- 9) kreatywnego poszukiwania innowacji,
- 10) opracowania dokumentacji,
- 11) stawianie zadań dla elementów wspólnoty rozpoznawczej (Żebrowski, 2017, s. 192).

Należy podkreślić, że mapa informacyjna i mapa wiedzy mają wartość poznawczą dla podmiotów zarządzania kryzysowego, pozwalają na poznanie niebezpieczeństw, gdzie źródłem jest wciąż zmieniające się i niepewne otoczenie gminy, powiatu, województwa i państwa, a także środowisko międzynarodowe. Dlatego uprawnione podmioty na wszystkich poziomach zarządzania kryzysowego w celu niedopuszczenia do zaistnienia zagrożenia lub minimalizowania jego negatywnych następstw potrzebują wyprzedzających informacji, pozwalających na skuteczne reagowanie na nadchodzące zmiany.

WNIOSKI

Informacja musi spełniać określone kryteria, a przede wszystkim być użyteczna dla podmiotów realizujących zadania w sferach: bezpieczeństwa państwa i zarządzania kryzysowego. W związku z tym podmioty te muszą stawiać precyzyjne zadania dla służb, instytucji i organizacji zabezpieczających ich potrzeby informacyjne. Skuteczne zarządzanie informacją wymaga dostępu do informacji aktualnych, prawdziwych i ważnych. Informacje te w połączeniu z posiadaną wiedzą pozwalają na podejmowanie racjonalnych decyzji i racjonalne wykonywanie zadań w procesie zarządzania kryzysowego. Natomiast system informacyjny w zarządzaniu kryzysowym powinien wpisywać się w system informacyjny zarządzania bezpieczeństwem państwa. Powinien być spójny z zarządzaniem kryzysowym na wszystkich poziomach państwa (taktycznym, operacyjnym, strategicznym).

Bezpieczeństwo państwa (państw) ma ścisły związek z informacją. Jest ona kluczem do sukcesu, ale i do porażki. Jej szczególna wartość i użyteczność jest niezbędna m.in. w procesie zarządzania kryzysowego. To podmioty zarządzające określają swoje potrzeby informacyjne, które zabezpieczane są przez uprawnione organy zewnętrzne i wewnętrzne państwa. Skuteczne wykonywanie

zadań wymaga posiadania dostępu do ogólnopaństwowego systemu informacyjnego, który powinien być kompatybilny z systemem informacyjnym wykorzystywanym w zarządzaniu kryzysowym na poziomie państwa, województwa, powiatu i gminy. Z uwagi na jego ważność powinien pełnić rolę systemu wczesnego ostrzegania i alarmowania. Stanowi podstawę tworzenia map informacji i map wiedzy, co bezpośrednio przekłada się na proces decyzyjny i wykonawczy. Zabezpieczanie potrzeb informacyjnych musi być procesem, a dostęp pozwala na skuteczne zarządzanie. Uczestnicy zarządzania kryzysowego zobowiązani są do stawiania precyzyjnych zadań organom, służbom i instytucjom nie tylko zabezpieczających ich potrzeby informacyjne, ale i własne. Są one również aktywnymi uczestnikami procesu niedopuszczenia, minimalizacji lub odtworzenia naruszonej infrastruktury krytycznej na każdym poziomie zarządzania kryzysowego w państwie.

BIBLIOGRAFIA

- Barczak A. i Sydoruk T. (2002), *Bezpieczeństwo systemów informatycznych*, Siedlce: Dom Wydawniczy Bellona.
- Błażejczyk W. (2002), *Systemy informacyjno-sterujące w walce zbrojnej*, [w:] G. Nowacki (red.), *Informacja w walce zbrojnej*, Warszawa: Akademia Obrony Narodowej, s. 93.
- Flakiewicz W. (2002), *Systemy informacyjne w zarządzaniu. Uwarunkowania, technologie, rodzaje*, Warszawa: Wydawnictwo C.H. Beck.
- Ingalls J. (1979), *Human Energy*, Menlo Park.
- Janczak J. (2001), *Zakłócanie informacyjne*, Warszawa: Akademia Obrony Narodowej.
- J.L. (1998), *Amerykańska koncepcja walki informacyjnej*, *Wojskowy Przegląd Zagraniczny*, nr 4, s. 16.
- J.L. (1999), *Operacje informacyjne w ujęciu amerykańskim*, *Wojskowy Przegląd Zagraniczny*, nr 4, s. 78-79.
- Kisielnicki J. (1992), *Informatyczna infrastruktura zarządzania*, Warszawa: PWN.
- Komorowska K. (2021), *Rola informacji we współczesnym świecie*, *Zeszyty Naukowe SGSP*, nr 79, s. 187-203.
- Kroenke D. (1989), *Management Information Systems*, New York: McGraw-Hill.
- Kwečka R. (2009), *Procesy informacyjne w ramach systemu reagowania kryzysowego Unii Europejskiej*, [w:] J. Gryz (red.), *System reagowania kryzysowego Unii Europejskiej. Struktura – charakter – obszary*, Toruń: Wydawnictwo Adam Marszałek.
- Leksykon wiedzy wojskowej* (1973), t.1, Warszawa: Ministerstwo Obrony Narodowej.
- Narski Z. (2004), *O dyktaturze kapitału globalnego*, Toruń: Wydawnictwo SUSPENS.
- Nowacki G. (2002), *Rozpoznanie satelitarne USA i Federacji Rosyjskiej*, Warszawa: Akademia Obrony Narodowej.
- Penc J. (1998), *Zrządzanie w praktyce. Menadżerskie myślenie i działania*, Warszawa: Wydawnictwo Infor Stan.

- Penc J. (1999), *Zarządzanie dla przyszłości. Twórcze kierowanie firmą*, Kraków: Wydawnictwo Profesjonalna Szkoła Biznesu.
- Piwowarski J. i Rozwadowski M. (2016), *System zarządzania kryzysowego jako element bezpieczeństwa narodowego*, Acta Scientifica Academiae Ostroviensis, nr 7, s. 348.
- S.P. (1997), *Informacja jako decydujący czynnik sukcesu w przyszłych konfliktach zbrojnych*, Wojskowy Przegląd Zagraniczny, nr 1, s. 30-40.
- Szpyra R. (2003), *Militarne operacje informacyjne*, Warszawa: Akademia Obrony Narodowej.
- Wojtaszczyk K.A. (1998), *Kompendium wiedzy o państwie współczesnym*, Warszawa: Polskie Wydawnictwo Profesjonalne.
- Żebrowski A. (2012), *Zarządzanie kryzysowe elementem bezpieczeństwa Rzeczypospolitej Polskiej*, Kraków: Wydawnictwo Naukowe Uniwersytetu Pedagogicznego.
- Żebrowski A. (2017), *Informacyjne przygotowanie pola walki*, [w:] A. Żebrowski i R. Żmigrodzki (red.), *Informacja jednym z elementów bezpieczeństwa państwa. Wybrane aspekty*, Kraków–Warszawa: Wydawnictwo Sztafeta, s. 192.

ROLA INFORMACJI W ZARZĄDZANIU KRYZYSOWYM WYBRANE ASPEKTY

Streszczenie

Zmieniające się środowisko funkcjonowania państwa (państw) generuje wiele złożonych zagrożeń, które utrudniają, a niekiedy i uniemożliwiają wykonywanie podstawowych zadań przez jednostki, grupy społeczne, naród i państwo. Skala i dynamika zachodzących zagrożeń, bardzo często zaskakuje rządzących i społeczeństwo. Celem niedopuszczenia do sytuacji kryzysowej uprawnione podmioty cywilne i wojskowe muszą zabezpieczać swoje potrzeby informacyjne w sposób ciągły; doceniać znaczenie informacji, potrafić je wykorzystać, by nie dopuścić do wystąpienia sytuacji kryzysowej lub zminimalizować jej następstwa. Oznacza to konieczność budowania systemu informacyjnego państwa, a także podsystemów na każdym poziomie jego funkcjonowania, które będą podstawą dla procesu decyzyjnego. Stawianie zadań, rozliczanie i umiejętne wykorzystywanie posiadanych zasobów informacyjnych w procesie zarządzania kryzysowego państwem pozwala na jego bezpieczne funkcjonowanie w otoczeniu wewnętrznym i środowisku międzynarodowym.

Słowa kluczowe: informacja; wojna informacyjna; zarządzanie kryzysowe.