*prof. nadzw. dr hab. inż. Gabriel Nowacki*
Wojskowa Akademia Techniczna w Warszawie

# Znaczenie informacji w obszarze bezpieczeństwa narodowego

## WPROWADZENIE

Postęp naukowo-techniczny oraz rozwój w sferze informatyki, telekomunikacji i multimediów spowodowały nadejście nowej ery – ery społeczeństwa informacyjnego, która ma miejsce wtedy, gdy większa część dochodu narodowego pochodzi z działalności związanej z przetwarzaniem informacji, a nie z produkcji przemysłowej[1].

Wszelkie działania celowe firm, organizacji oraz państw stają się zależne od napływu aktualnych i wartościowych informacji, przekazywanych z wykorzystaniem systemów informacyjnych, w których na szeroką skalę stosuje się osiągnięcia nowych technologii.

Uważa się, że zasoby wiedzy i zdolności intelektualne będą wpływać w dużym stopniu na wartość organizacji oraz decydować o możliwości dostosowywania się do zmian zewnętrznych. Zachodzi przy tym konieczność kojarzenia dwóch pozornie sprzecznych zdolności: do elastycznego i szybkiego dostosowywania się do zmieniającej się sytuacji zewnętrznej oraz do przewidywania przyszłych warunków działania. Z jednej strony występuje potrzeba ciągłego obserwowania sytuacji zewnętrznej, w otoczeniu konkurencyjnym, a z drugiej, podejmowania w porę takich działań, które dawałyby duże szanse osiągnięcia sukcesu w przyszłości.

Siły polityczne z rzekomo mało znaczących regionów mają dzisiaj dostęp do tego rynku technologicznego. Niezbędne środki (komputery osobiste, oprogramowanie itp.) są dostępne na całym świecie. Dlatego też siły te nie muszą już dzisiaj wydawać ogromnych kwot na zakup systemów uzbrojenia i broni, które zresztą objęte są zakazem eksportu do tych regionów. Rozwój w tym obszarze będzie trwał w tych regionach z pewnością jeszcze dłuższy czas, dlatego już teraz muszą być poczynione wysiłki, które uodpornią własne systemy na oddziaływanie środków operacji informacyjnych potencjalnego agresora.

Potencjalny przeciwnik, oddziałując tylko na systemy informacyjne, może obezwładnić czy wręcz zniszczyć istotne elementy infrastruktury cywilnej i wojskowej. Ponadto atakujący może ukryć swoją tożsamość, a zaatakowane pań-

[1] T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, Wydawnictwo Fundacji Postępu i Telekomunikacji, Kraków 1999.

stwo nie będzie w stanie jednoznacznie wskazać agresora. Wynika z tego, że zagrożenia w sferze informacyjnej stają się realnym zagrożeniem dla bezpieczeństwa narodowego. Aby się przed tym uchronić, potrzebna jest wiedza o stanie otoczenia i rodzących się przesłankach zagrożeń, które z natury rzeczy będą utrzymywane przez zainteresowanego w jak największej tajemnicy.

Działania na rzecz utrzymania właściwego stanu polskiej infrastruktury informacyjnej są jednym z warunków zapewnienia odpowiedniego potencjału obronnego i bezpieczeństwa kraju, zarówno wewnętrznego, jak i zewnętrznego.

## ROLA I ZNACZENIE INFORMACJI

### Terminologia dotycząca informacji

Termin „informacja" jest używany w wielu różnych i odmiennych znaczeniach. W powszechnym znaczeniu „informacja jest utożsamiana z przedmiotami myślowymi odzwierciedlającymi wszelkie postacie wiadomości, wieści, nowin, rzeczy zakomunikowanych, wiedzy o zdarzeniach" itp.[2]

W cybernetyce „informacja" stanowi jeden z podstawowych terminów, którego desygnat jest nie w pełni definiowalny z uwagi na jego pierwotny i elementarny charakter.

N. Wiener[3] określa informację jako „nazwę treści zaczerpniętej ze świata zewnętrznego, w miarę jak się do niego dostosowujemy i jak przystosowujemy doń swoje zmysły".

N. Couffignal[4] stwierdza, że „w cybernetyce informacją nazywa się wszelkie działanie fizyczne, któremu towarzyszy działanie psychiczne".

Według W. Głuszkowa[5], „informacja to wszelkie wiadomości o procesach i stanach dowolnej natury, które mogą być odbierane przez organy zmysłowe człowieka".

Zdaniem H. Greniewskiego[6], „informacja to stany wyróżnione wejść i wyjść układu".

Według C.L. Shannona[7], „informacją jest to wszystko, co nie jest ani energią, ani masą, czyli zasilaniem – jest to każde rozpoznanie stanu układu, odróżnialnego od innego stanu tego układu".

---

[2] W. Kopaliński, *Słownik wyrazów obcych i zwrotów obcojęzycznych*, Wiedza Powszechna, Warszawa 1980, s. 429.

[3] N. Wiener, *Cybernetics or Control and Communication in the Animal and the Machine*, New York, Hermann & Cie, The Technology Press, and John Wiley & Sons, 1948, s. 67–69.

[4] L. Couffignal, *Cybernetyka*, Paryż 1965, s. 36.

[5] W. Głuszkow, *Wstęp do cybernetyki*, Naukowa Dumka, Kijów 1963, s. 21–29.

[6] H. Greniewski, *Cybernetyka niematematyczna*, PWN, Warszawa 1982, s. 43.

[7] C.E. Shannon, W. Warren, *The Mathematical Theory of Communication*, The University of Illinois Press, Urbana 1949, s. 41–48.

J. Seidler[8] stwierdza, że „informacją można nazywać to wszystko, co jest użytkowane do bardziej sprawnego wyboru działań prowadzących do realizacji pewnego celu". Wyjaśnia przy tym, że mówiąc o sprawności działania należy mieć na myśli to, iż mając i użytkując właściwie informację można realizować celowe działania lepiej, bez istotnego zwiększania czy to środków materialnych, czy zużywanej energii. Na podstawie dokonanej analizy przyjęto, że desygnat pojęcia „informacja", w rozumieniu rzeczowym, należy utożsamiać z nazwą treści percepcji zmysłowej bodźca, a w rozumieniu czynnościowym (funkcjonalnym) – z procesem informowania.

Informacja, w rozumieniu rzeczowym, służy również do tworzenia wiedzy o otoczeniu człowieka i o nim samym. Procedurę tę w najprostszym ujęciu odzwierciedla pętla poznania indukcyjno-dedukcyjnego, w której zespoły myślowe poznawczych funkcji mózgu (umysł) spełniają rolę centralną. Wiedza tworzona w umyśle ludzkim nie jest związana tylko z poznaniem indukcyjnym. Związana jest również z poznaniem dedukcyjnym. Istota tego procesu polega na tym, że na bazie racji indukcyjnych wyprowadzane są nowe racje dedukcyjne, które uzupełniają i rozszerzają wiedzę uzyskaną drogą indukcyjną. Te obydwie metody poznania umysłowego przeplatają się, a przewaga jednej nad drugą zależna jest tylko od skłonności umysłowych konkretnego człowieka i poznawanego przez niego obiektu.

Związki informacji z umysłem ludzkim nie pozwalają jeszcze wyjaśnić relacji występujących w infrastrukturze informacyjnej. Powodem takiego stanu rzeczy jest fakt, że systemy informacyjne znajdujące się w otoczeniu człowieka nie mają i mieć nie mogą uniwersalnego wnętrza strukturalnego, dostosowanego funkcjonalnie do wszelkich sytuacji. Ich struktura jest zawsze następstwem konkretnych potrzeb człowieka, zespołów ludzkich, organizacji oraz możliwości technicznych i technologicznych.

**Przekaz informacyjny jako sposób oddziaływania na człowieka**

W XXI wieku w potencjalnych konfliktach, sytuacjach kryzysowych oraz w konkurencji na szeroką skalę mogą być wykorzystywane nowe technologie informacyjne oraz nowe techniki wpływania na postawy i zachowania ludzi.

W oddziaływaniu na ludzi można wyodrębnić trzy zasadnicze mechanizmy, wykorzystywane do kształtowania pożądanych postaw i zachowań:

- mechanizm internalizacji lub introjekcji polegający na przekazywaniu treści odpowiednio dobranych i spreparowanych, przy założeniu jednego tylko kryterium,
- mechanizm przymusu – gdzie jednostka przyjmuje pewną postawę ze względu na obiecaną nagrodę lub ze strachu przed karą, jaka ją może spotkać,
- mechanizm identyfikacji stanowiący o tym, że każdy człowiek posiada swe wzorce osobowe, do których chciałby się upodobnić.

[8] J. Seidler, *Nauka o informacji*, WNT, Warszawa 1983, s. 69.

Mechanizmy te wpływają na dobór odpowiednich metod oddziaływania na postawy i zachowania ludzi. Współcześnie zmierza się w stronę środków komunikacji opartych na kombinacji wszystkich elementów: tekstu, obrazu, bezpośredniej rozmowy, listu, muzyki – możliwości takie dają współczesne media: telewizja, Internet. Związane jest to także z możliwościami odbioru treści informacyjnych przez mózg człowieka[9]:
– wzrok – 83%,
– słuch – 11%,
– węch – 3,5%,
– dotyk – 1,5%,
– smak – 1%.

Internet konkuruje z telewizją jako środek dotarcia do masowego audytorium i wpływania na opinie i decyzje. Podobnie jak audycje telewizyjne, Internet także stwarza możliwości nadawania i przekazywania wydarzeń na bieżąco. Jest środkiem dającym jednostkom i małym grupom takie same możliwości wypowiedzi, jakie mają rządy i wielkie korporacje. W Internecie stwierdzono manipulację przez odpowiednie preparowanie informacji tekstowej, obrazu oraz równoczesne wykorzystanie obydwu kanałów informacji. Manipulacja może być skierowana do całego społeczeństwa lub jego części.

Media zajmują ważne miejsce w kształtowaniu opinii publicznej. A właśnie opinia publiczna jest ważnym czynnikiem rozwoju społeczeństwa, aktywną formą ustosunkowania się do zjawisk społecznej rzeczywistości. Manipulacja w mediach jest formą wywierania wpływu na członków widowni w celu realizowania przez nią działań, zaspokajających potrzeby manipulatora, przy czym odbiorcy nie zdają sobie z tego sprawy. Manipulator nie interesuje się tym, czy działania podejmowane przez odbiorcę przynoszą korzyści odbiorcy informacji medialnej, interesuje go wyłącznie, aby manipulowani byli przekonani, że działania te wykonują z własnej woli, a skutki tych działań są dla nich pozytywne. To właśnie sprawia, że osoba poddawana manipulacji najczęściej nie zdaje sobie z tego sprawy, a poinformowana o tym gwałtownie zaprzecza, że działa w sposób niekontrolowany. Zachowanie u odbiorcy przekonania o samodzielności podejmowania działań powoduje, że jest on niesłychanie odporny na perswazję i próby pokazania faktycznej sytuacji, w jakiej się znajduje. Z tego względu koniecznością staje się wyposażenie różnych instytucji w niezbędne instrumenty oraz kształcenie obywateli, umożliwiające obronę przed manipulacją.

**Charakterystyka systemu informacyjnego**

Niezbędnym atrybutem każdej organizacji jest system informacyjny, który umożliwia wymianę informacji pomiędzy poszczególnymi użytkownikami. Istotnym warunkiem sprawnego działania organizacji jest właściwe podejmowanie decyzji. Każda decyzja jest podejmowana w pewnym przesunięciu czaso-

[9] K. Piątkowski, *Wojna nowego typu?*, „Polska w Europie" nr 1, marzec 2002.

wym w stosunku do odniesienia wykonawczego. Jest wypracowywana i podejmowana w stosunku do stanu otoczenia prawdopodobnego, który w rozumieniu dosłownym zwykle nie zaistnieje.

Oznacza to, że w praktyce wszelkie decyzje podejmowane są zawsze w stosunku do odniesień prospektywnych, z natury rzeczy mogą być tylko przybliżonym odzwierciedleniem stanu rzeczywistego, który może zaistnieć w przyszłości – mogą być odzwierciedleniem tylko prawdopodobnym. Dlatego też w trakcie ich realizacji musi się odbywać ciągłe monitorowanie umożliwiające korygowanie bądź potwierdzanie kształtu i treści wcześniej stworzonego obrazu tego odniesienia. To z kolei wskazuje na potrzebę wprowadzania określonych korekt do podjętej wcześniej decyzji bądź też utwierdza w przekonaniu o jej trafności. Do tego jednak potrzebna jest decydentowi odpowiednia wiedza o stanie odniesienia i obiekcie oddziaływania, często utożsamiana z informacjami[10].

W otoczeniu człowieka istnieją dwa podstawowe rodzaje systemów informacyjnych. Pierwszą grupę tworzą systemy naturalne, a drugą – sztuczne.

Systemy naturalne stworzyła sama natura i funkcjonują poza wpływem i wolą człowieka. W szerokim rozumieniu tego słowa są również odporne na wszelkie jego oddziaływania – człowiek nie jest w stanie zmienić ani ich struktury, ani zasad funkcjonowania.

Sztuczne systemy informacyjne są zawsze wytworem ludzkiej działalności. Stosowane w nich rozwiązania strukturalne i organizacyjne – hierarchiczne, funkcjonalne, informacyjne i techniczne – tworzone są zawsze tylko w aspekcie dających się przewidywać potrzeb ich twórców i tylko na miarę zdobytej przez nich na ten temat wiedzy oraz fizycznych możliwości jej materializowania w konkretnych rozwiązaniach.

Sztuczne systemy informacyjne tworzone są przez człowieka w aspekcie spełniania konkretnych potrzeb wynikających z zamiaru jakiegoś działania celowego. Tworzone są z zamysłem poznawania lub identyfikowania zdarzeń w przestrzeni pola operacyjnego, na którego materii zamierzone jest jakieś działanie. Służą również do ustalania stanu i możliwości operacyjnych aparatu narzędziowego, przeznaczonego do realizacji tego zamierzenia, oraz monitorowania efektów podejmowanej działalności.

W strukturze systemu informacyjnego występują elementy kierowania określonymi procesami. W organach, takich jak centra, węzły, szeroko stosuje się dzisiaj technologie informacyjne i różnego rodzaju urządzenia elektroniczne. Wykorzystuje się je do rejestrowania i gromadzenia danych, ich analizowania, segregowania i przechowywania oraz do wypracowywania decyzji i przekazywania tych decyzji wykonawcom. Tym samym są to najbardziej newralgiczne

[10] Wynika to z logiki działania celowego, a spełnianie pożądanych w tym zakresie potrzeb wiąże się ściśle z wykorzystaniem zasobów informacyjnych. Różnica pomiędzy wiedzą a informacją zostanie wyjaśniona w dalszej części procedury dowodowej.

punkty w strukturze każdego systemu informacyjnego. Dlatego też elementy te jako przedmioty oddziaływania są szczególnym obiektem zainteresowania struktur bezpieczeństwa narodowego.

## OPERACJE INFORMACYJNE W XXI WIEKU

**Informacja w działaniu celowym**

Realizacja każdego działania celowego odbywa się zawsze w jednym z trzech rodzajów otoczenia. Może przebiegać w zupełnym wyizolowaniu, może się odbywać w ramach współpracy lub w ramach rywalizacji.

W warunkach wyizolowania organizator i realizator działania celowego zdany jest tylko na własne siły i własną pomysłowość w osiąganiu danego celu. Nikt mu w sposób zamierzony ani nie pomaga, ani nie przeszkadza. Jest po prostu wyizolowany z otoczenia. Co najwyżej może się natknąć na pewne zdarzenia losowe, które bądź pozytywnie, bądź negatywnie wpłyną na realizację podjętego wysiłku.

W ramach współpracy organizator i realizator działania celowego wspomagany jest w swych wysiłkach działaniami innego lub innych, którzy pomagają mu osiągnąć zamierzony cel. Ten z kolei, dążąc do osiągnięcia własnego celu, wspiera działania elementów współpracujących z nim. W tych warunkach, podobnie jak poprzednio, nikt nikomu nie przeszkadza w realizacji podjętych działań. Co najwyżej mogą wystąpić pewne zdarzenia losowe, które bądź ułatwią, bądź też utrudnią ich realizację.

Zupełnie inaczej przebiega proces działania celowego w warunkach rywalizacji (kooperacji negatywnej). Według T. Kotarbińskiego, także z punktu widzenia cybernetyki, kooperacja ta utożsamiana jest z walką. „Walka to wszelkie działania przynajmniej dwupodmiotowe (zakładając, że zespół może być podmiotem), gdzie przynajmniej jeden z podmiotów przeszkadza drugiemu”[11]. W szczególnym, najzwyklejszym i najciekawszym przypadku oba podmioty nie tylko dążą obiektywnie do celów niezgodnych, lecz nadto wiedzą o tym i liczą się w budowaniu swoich planów też z działaniami strony przeciwnej.

T. Kotarbiński wyróżnił cele permutacyjne (zmieniające) i perseweracyjne (niezmieniające). W takim kontekście do rywalizacji może dojść wtedy i tylko wtedy, gdy przynajmniej jedna ze stron dążyć będzie do zmiany istniejącego stanu rzeczy.

Po pierwsze, może zaistnieć stan, w którym zarówno strona A, jak i B mogą mieć cele permutacyjne, to znaczy, że obie rywalizujące strony pragną zmienić istniejący stan rzeczy. Obydwie strony będą więc prowadzić działania po to, by zmienić ten stan.

[11] T. Kotarbiński, *Traktat o dobrej robocie*, Wrocław, 1982, s. 221.

Po drugie, może zaistnieć stan, w którym strona A pragnie zmienić istniejący stan rzeczy, strona B zaś utrzymać go. Wówczas A atakuje, B zaś broni się.

Po trzecie, może zaistnieć stan przeciwstawny drugiemu, to znaczy, że strona B stawia sobie cele permutacyjne, zaś strona A perseweracyjne.

W walce skutecznej, niejako w uzupełnieniu teorii czynu skutecznego, zawsze jedna ze stron osiągnie cel, czyli w rezultacie zwycięży. Warunkiem zaś koniecznym do osiągnięcia celu jest uzyskanie przewagi. W przewadze nie chodzi o posiadanie większych zasobów od strony przeciwnej, lecz o sprawne ich wykorzystanie, a zatem o stałą możliwość wykorzystania potencjału w określonym, rozstrzygającym miejscu i czasie. Takie sprawne wykorzystanie potencjału zapewniają systemy i technologie informacyjne, które muszą być chronione przed oddziaływaniem strony przeciwnej.

Zwycięstwo nad potencjalnym przeciwnikiem (agresorem) będzie odnosił ten, kto potrafi wpłynąć na decyzje strony przeciwnej, aby były one dla niego korzystne. Będzie to polegało na wprowadzaniu decydentów w błąd co do realnej sytuacji, czyli na stwarzaniu sytuacji utrudniających kooperantowi negatywnemu podejmowanie trafnych decyzji, wykonywanie sprawnych działań z jednoczesną obroną własnych systemów informacyjnych.

Każda rywalizacja wymaga dogodnej sytuacji. Ważne dla osiągnięcia sukcesu będzie więc postawienie potencjalnego przeciwnika w sytuacji, w której będzie zmuszony dążyć do zmiany pozycji i sytuacji, czyli tracić część potencjału na działania przygotowawcze. W każdym przypadku do osiągnięcia sukcesu przyczyni się działanie, w którym doprowadzimy do stanu przeciwstawnego oczekiwaniom strony przeciwnej, tak aby strona ta musiała odrabiać wytworzony stan rzeczy, niezgodny z jej celem.

**Przestrzeń operacji informacyjnych**

Wszelkie konflikty, szczególnie w ostatnich latach, świadczą jednoznacznie, iż w każdej organizacji istnieją takie elementy, od których zależy jej sprawność. Jeśli przyjmie się tezę, że wszystkie sztuczne systemy informacyjne tworzone są przez człowieka w aspekcie spełniania konkretnych potrzeb, wynikających z realizacji jakiegoś działania celowego, to można również stwierdzić, że są one nierozerwalnie związane z każdym działaniem celowym, realizowanym w warunkach kooperacji negatywnej wzajemnej. Każdy z zaangażowanych podmiotów dąży do wypracowania takich decyzji, aby po ich wdrożeniu odnieść sukces w rywalizacji. Dąży zatem do wypracowywania decyzji możliwie najtrafniejszych w danej sytuacji. Do osiągnięcia tego niezbędna jest jednak wiedza o stanie, usytuowaniu oraz możliwościach i zamiarach wykorzystywania narzędzi strony przeciwnej i o panującej u niego sytuacji.

Tak samo niezbędna jest wiedza o własnych siłach i środkach. Posiadanie tych danych stanowi podstawę do świadomego wypracowywania poprawnych decyzji. Luki w zasobach wiedzy powodują podejmowanie decyzji ryzykownych, o nieprzewidywalnych skutkach.

Dlatego też należy zapewnić sprawne funkcjonowanie własnych systemów informacyjnych, gdyż ich zakłócenie stanowi często zasadniczy czynnik determinujący powodzenie (osiągnięcie celu). Stąd też we współczesnych konfliktach, sytuacjach kryzysowych, obezwładnienie systemów informacyjnych pociągnąć może destrukcję funkcjonalną całej organizacji. O powodzeniu wszelkich działań będzie więc decydować wyeliminowanie tych decydujących elementów w systemach informacyjnych strony przeciwnej, które stanowią o jego sprawności działania.

Realizację powyższych celów można uzyskać przez prowadzenie operacji informacyjnych, które należy interpretować jako kompleks planowych przedsięwzięć, polegający na wpływaniu na postawy decydentów, zakłócaniu systemów informacyjnych strony przeciwnej z jednoczesną ochroną własnych systemów informacyjnych. Operacje informacyjne będą prowadzone w określonej przestrzeni (środowisku informacyjnym).

Przestrzeń operacji informacyjnych to zbiór skoordynowanych elementów (przynajmniej dwóch przeciwstawnych stron), których istota, ze względu na relację porządkującą celu, skupiona jest w podprzestrzeniach: zdobywania informacji (rozpoznania), zakłócania informacyjnego i ochrony informacyjnej.

Podprzestrzeń zdobywania informacji (rozpoznania) to układ skoordynowanych elementów dostosowanych do spełniania swej roli w środowisku elektromagnetycznym, akustycznym, magnetycznym i chemicznym, przez których pryzmat możliwe jest identyfikowanie aktualnego stanu otoczenia.

Podprzestrzeń zakłócania informacyjnego to układ skoordynowanych elementów dostosowanych do wnoszenia entropii informacyjnej do komunikatów i powodowania destrukcji fizycznej nośników tych komunikatów i nośników danych.

Podprzestrzeń ochrony informacyjnej to układ skoordynowanych elementów, których celem jest uniemożliwienie i utrudnienie zdobywania danych o fizycznej naturze aktualnego i planowanego stanu rzeczy i zjawisk we własnej przestrzeni funkcjonowania oraz uniemożliwienie i utrudnienie wnoszenia entropii informacyjnej do komunikatów i destrukcji fizycznej do ich nośników.

Przestrzeń osobową operacji informacyjnych tworzą narzędzia i procesy dostosowane do oddziaływania w sferze środowiska informacyjnego, które jest bezpośrednio postrzegalne zmysłami ludzkimi.

Przestrzeń techniczną operacji informacyjnych tworzą wszelkie narzędzia i procesy dostosowane do oddziaływania w sferze środowiska informacyjnego, które jest bezpośrednio niepostrzegalne zmysłami ludzkimi.

Typowym elementem występującym wewnątrz systemu informacyjnego jest podsystem zdobywania informacji. Tworzą go profesjonalnie wyspecjalizowane narzędzia rozpoznawcze, których zadaniem jest zdobycie prawdziwych danych o stanie, usytuowaniu, możliwościach oraz planach i zamiarach strony przeciwnej. W podsystemie tym przedmiotem kooperacji negatywnej jest zbiór możli-

wych postaci danych o stronie przeciwnej. Każda ze stron stara się rywalizować z systemem rozpoznania swojego kooperanta negatywnego przez stosowanie odpowiedniej ochrony danych i zakłócanie podsystemów strony przeciwnej.

W podsystemie zbierania danych o własnym potencjale walka ma nieco inny charakter niż w torze zdobywania danych o przeciwniku. Skupiona jest głównie na problematyce zachowywania i dezorganizowania jego sprawności funkcjonalnej. Wynika to z tego, że sukces w kooperacji negatywnej wzajemnej warunkowany jest sprawnością kierowania. Jakość tego procesu odzwierciedla się w trafności podejmowanych decyzji. Dlatego też do osiągnięcia tego nie wystarcza tylko znajomość przeciwnika. Konieczna jest jeszcze dobra znajomość chwilowych stanów własnego potencjału. Z tego też względu organy kierujące (sterujące) walką starają się wszelkimi sposobami zapewniać sobie ciągły napływ wiarygodnych i precyzyjnych danych o rzeczywistym stanie, usytuowaniu i rezultatach prowadzonej walki.

Ochrona zbioru postaci danych może być realizowana różnymi sposobami i narzędziami. Istota tej ochrony sprowadza się do stwarzania warunków uniemożliwiających stronie przeciwnej przechwytywanie danych, szczególnie tych ich postaci, które zawierają największy potencjał informacyjny o ważnych sytuacjach rzeczywistych. Nie zawsze jednak jest to możliwe. Nie zawsze też pewne postacie danych można ukryć. Dlatego w ramach ochrony informacyjnej, oprócz ukrywania, stosowane jest jeszcze maskowanie danych. Jego istota sprowadza się do stosowania takich rozwiązań, które powodują tylko zmianę wartości potencjału informacyjnego określonych postaci danych.

Zakłócanie zdobywania danych może być prowadzone różnymi sposobami z wykorzystaniem różnych narzędzi. Podsystem zakłócania jest bardziej złożony niż podsystem ochrony informacyjnej. System ten spełnia dwie podstawowe funkcje. Chociaż służy tylko do zwiększania entropii informacyjnej w torze zdobywania danych, to jednak funkcję tę realizuje drogą stosowania szeroko rozumianej pozoracji i drogą fizycznej destrukcji jego elementów technicznych. Procedura destrukcyjnego oddziaływania na podsystem zdobywania danych (system rozpoznania) realizowana jest z zamysłem uniemożliwiania stronie przeciwnej wykorzystywania tych postaci danych, do których udało się mu zdobyć dostęp, mimo stosowania ochrony informacyjnej. Ma to na celu generowanie i udostępnianie stronie przeciwnej zbiorów postaci danych, które stwarzać będą dezinformacyjne obrazy sytuacyjne i zarysy rozwiązań koncepcyjnych. Dlatego też podejmowane w tym zakresie przedsięwzięcia muszą być dostatecznie: scentralizowane, kompleksowe, spójne, wiarygodne, nieszablonowe, skryte, terminowe, ciągłe i elastyczne.

Efektywność operacji informacyjnych zależy od wielu czynników. Jednym z najważniejszych jest trafność doboru narzędzi i form ich wykorzystywania w procesie oddziaływania na systemy informacyjne. Struktury operacji informacyjnych mają przedstawić stronie przeciwnej fałszywy obraz rzeczywistości

w przestrzeni planowanej przez niego operacji i przez to ukierunkować jego wysiłki na planowanie i prowadzenie działań w stosunku do nieistniejących lub nieistotnych dla sukcesu odniesień. Osiągnięcie tego w sposób nieświadomy dla strony przeciwnej jest przedsięwzięciem niezmiernie trudnym i złożonym. Wiąże się przede wszystkim ze spójnością dozowanej mu specjalnie upływności informacyjnej, której szczegóły, w całej swej masie, muszą się składać na jednolicie logiczny obraz.

Każdy podmiot zdaje sobie sprawę, że działająca negatywnie strona czynić będzie takie wysiłki. Dlatego też każda zdobyta postać danych będzie wielokrotnie sprawdzana, gruntownie analizowana i potwierdzana w innym obszarze. Z tego też względu wszystkie przedsięwzięcia powinny być prowadzone kompleksowo i jednolicie. Niższy szczebel, nie znając rzeczywistych zamiarów i planów, może zdemaskować i tym samym zniweczyć całość przedsięwzięcia, podejmując określone działania z własnej inicjatywy. Z analizy faktów wynika, że nigdy w historii nie zdarzyło się, aby tego typu przedsięwzięcia – podjęte z inicjatywy niższych szczebli kierowania i bez zgody organu centralnego – były skuteczne. Zawsze były demaskowane, a jeśli nawet nie, to i tak przynosiły odwrotne do zamierzonych rezultaty.

Z punktu widzenia potrzeb prowadzenia operacji informacyjnych ważna jest wcześniejsza i bieżąca wiedza o przedmiotach oddziaływania i ich otoczeniu. Tylko taki stan informacyjny może stanowić podstawę do trafnego doboru narzędzi i form oddziaływania, a co za tym idzie – przeprowadzenia skutecznego działania. Każda reakcja celowa musi być zawsze poprzedzona rozpoznaniem przedmiotu, na który będzie skierowana i rozpoznaniem warunków jego usytuowania. Przedsięwzięcia realizowane w ramach operacji informacyjnych (np. walka elektroniczna, działania psychologiczne, ochrona danych) w znaczny sposób przyczyniają się do uzyskania przewagi informacyjnej, a tym samym do odniesienia sukcesu. Z powyższych założeń wynika, że przewaga informacyjna jest logicznym następstwem skutecznego prowadzenia operacji informacyjnych.

Chcąc odnieść sukces, należy jak najdłużej utrzymywać swój potencjał w pełnej zdolności do działań. Utracenie możliwości reakcji na działania strony przeciwnej pozbawia możliwości realizacji celu. Dlatego duże znaczenie w tym zakresie będzie odgrywać zdobywanie informacji, ważne w tym zakresie jest aby posiadać pewne, sprawdzone informacje o stronie przeciwnej, a strona przeciwna aby nie miała o nas informacji lub miała błędne.

Nie mniej ważny od wypracowywania decyzji jest również proces jej wdrażania do realizacji. Pod tym względem szczególną rolę odgrywa terminowość i skrytość realizacji poszczególnych przedsięwzięć. Można zatem powiedzieć, że w kooperacji negatywnej wzajemnej, oprócz działań zasadniczych, toczy się jeszcze walka o szybkość reakcji i trafność działania (walka o „czas" i o precyzję działania). W tej właśnie sferze działania mieści się funkcjonalna rola operacji informacyjnych. Jako że ich przedmiotem są systemy informacyjne, ich efek-

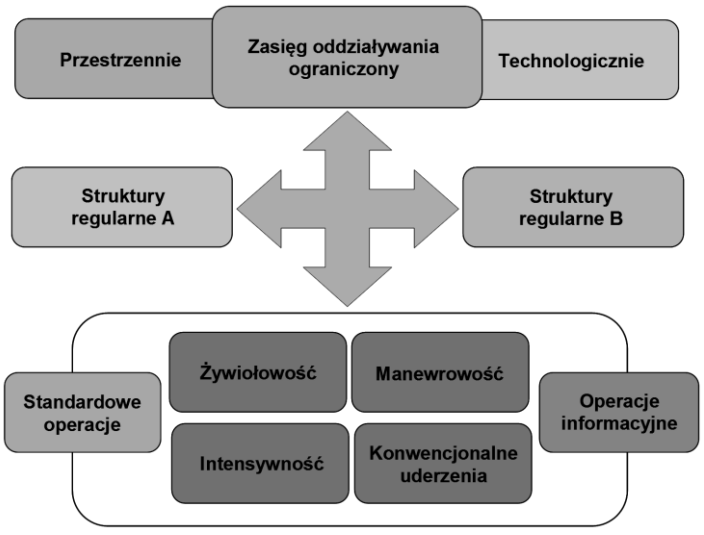
ty będą się materializować w sprawności i skuteczności funkcjonowania tych systemów.

**Zagrożenia informacyjne dla bezpieczeństwa narodowego**

Rozwój cywilizacyjny, postęp naukowo-techniczny oraz nowa sytuacja geopolityczna na świecie powodują, że zmieniają się formy i środki zagrożeń. Nowe zagrożenia dla bezpieczeństwa międzynarodowego to przede wszystkim zorganizowany terroryzm międzynarodowy, niekontrolowana proliferacja broni masowego rażenia oraz środków ich przenoszenia, zorganizowana przestępczość międzynarodowa, konflikty spowodowane rozkładem państw czy bloków (np. była Jugosławia, ZSRR).

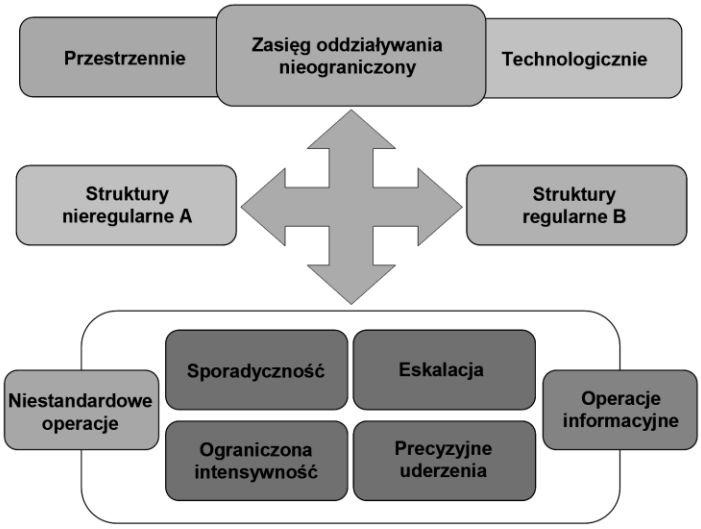
Zmienia się charakter współczesnych konfliktów na świecie z symetrycznego na asymetryczny. Konflikt asymetryczny ma miejsce jeśli strony posiadają różny status prawno-międzynarodowy oraz występuje sytuacja, w której walczą ze sobą nierówni przeciwnicy. Jej cechą jest uznanie za nadrzędne technik przemocy[12] (rysunki 1, 2). Asymetryzacji towarzyszy wzrost popularności taktyk partyzanckich (form defensywnych) oraz taktyk terrorystycznych (form ofensywnych).

W przypadku konfliktu zbrojnego będzie miał on charakter asymetryczny, kiedy państwo i jego siły zbrojne konfrontowane są z przeciwnikiem, którego cele, organizacja, środki i metody walki nie mieszczą się w kategoriach konwencjonalnych.




**Rysunek 1. Cechy charakterystyczne konfliktu symetrycznego**

[12] T. Ciszewski, *Zarządzanie sytuacją kryzysową w środowisku zagrożonym IED*, „Zeszyty Naukowe WSOWLąd", nr 3 (157), Wrocław, 2010, s. 205–224.




**Rysunek 2. Cechy charakterystyczne konfliktu asymetrycznego**

W konflikcie tym nie występuje termin „pole walki", działania odbywają się w rozproszeniu, bez zachowania ciągłości geograficznej i chronologicznej[13]. Kluczowymi elementami konfliktu są: skrytość, zmienność i zaskoczenie. Przeciwnik w tym konflikcie unika bezpośredniej konfrontacji, posługuje się głównie terroryzmem oraz narzędziami operacji informacyjnych, w tym działań psychologicznych. W konflikcie asymetrycznym uwydatnia się przewaga słabszej strony, która może osiągnąć znaczące korzyści (propagandowe, psychologiczne), angażując minimalne siły i środki. Siły zbrojne wielu państw nie spełniają wymagań do działań asymetrycznych. Trudno jest walczyć z przeciwnikiem, który nie stanowi widocznego zagrożenia, atakuje cele niewojskowe przy użyciu niekonwencjonalnych metod[14].

Kolejną cechą konfliktu asymetrycznego jest łatwość jego prowadzenia. Internet i telefonia komórkowa umożliwiają błyskawiczną komunikację oraz anonimowość[15].

Siły prowadzące konflikt są rozproszone, dlatego atak odwetowy raczej nie odniesie skutku, ponadto druga strona powstrzymuje się przed uderzeniem odwetowym, obawiając się skutków politycznych i społecznych zdecydowanej akcji militarnej[16].

[13] K. Piątkowski, *Wojna nowego typu?*, „Polska w Europie" nr 1 z marca 2002 r.

[14] A. Wejkszner, *Wojny XXI wieku. Istota konfliktów asymetrycznych* [w:] *Zagrożenia asymetryczne współczesnego świata*, red. S. Wojciechowski, R. Fiedler, Poznań 2009.

[15] K. Piątkowski, *Wojna nowego typu?*…

[16] M. Madej, *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*, Warszawa 2007.

Celem podmiotu prowadzącego walkę asymetryczną jest maksymalizacja efektów przy minimalizacji kosztów poprzez spektakularne akcje terrorystyczne mające wywołać skutki psychologiczne w społeczeństwie. Podmiot ten stanowią zakonspirowane grupy, które łączy więź ideologiczno-etniczna. Cechą podmiotów asymetrycznych jest niekonwencjonalne wykorzystanie dostępnych środków destrukcyjnego oddziaływania. Obok najtańszego uzbrojenia i amunicji, mogą one wykorzystać inny rodzaj środków oddziaływania[17], niekoniecznie militarne.

Oprócz znacznego rozwoju środków elektronicznych (mikroprocesory, generatory impulsu elektromagnetycznego, bomby „logiczne", wirusy komputerowe) oraz mass mediów (Internet, telewizja, radio, prasa) pojawiły się nowe możliwości oddziaływania, jak chociażby broń wiązkowa (energii kierowanej), światła stroboskopowe wywołujące nudności czy infradźwięki powodujące depresje, napięcia, strach, sztuczną wesołość, spowolnienie reakcji, dolegliwości sercowe i zaburzenia równowagi. Ponadto mogą być wykorzystane różne techniki psychotroniczne, które wywołują subiektywne i obiektywne zachowania ludzi pod wpływem sugestii lub autosugestii.

Ugrupowania terrorystyczne, obce służby specjalne, a także ekstremistyczne oraz zorganizowane grupy przestępcze mogą podejmować próby uzyskania nieuprawnionego dostępu do treści informacyjnych, w tym wymienianych w ramach współpracy sojuszniczej.

Coraz bardziej realne stają się dla Polski zagrożenia w sferze informacyjnej takie, jak: dezorganizacja kluczowych systemów informacyjnych, penetracja baz danych, prowadzenie działań dezinformacyjnych, których celem będzie sparaliżowanie systemu bezpieczeństwa państwa. Dlatego też organizacja i wyposażenie organów administracji publicznej, sił zbrojnych, organizacji pozamilitarnych powinny być stale dostosowywane do potrzeb bezpieczeństwa narodowego, konieczności wypełniania zobowiązań sojuszniczych i międzynarodowych oraz możliwości społeczno-ekonomicznych państwa.

Ze względu na ewolucję charakteru zagrożeń bezpieczeństwa regularne siły zbrojne będą stopniowo zastępowane przez nowoczesne, mobilne, wyspecjalizowane, bliżej nieokreślone struktury. Z charakteru nowych zagrożeń wynika konieczność rozwoju współpracy sił zbrojnych ze strukturami cywilnymi w zakresie reagowania na zagrożenia pozamilitarne oraz podejmowania operacji ratowniczych i antyterrorystycznych w kraju i poza jego granicami.

Siły Zbrojne RP służą zapewnieniu bezpieczeństwa Polski i niosą pomoc sojuszniczą zgodnie z art. 5 Traktatu Północnoatlantyckiego, ich celem jest także ochrona polskich interesów oraz budowa pozycji Polski w NATO i Unii Europejskiej.

---

[17] A. Bujak, *Możliwe kierunki zmian w reagowaniu kryzysowym (cz. I)*, „Zeszyty Naukowe WSOWLąd" nr 2/2005, Wrocław 2005.

Ważnym zadaniem sił zbrojnych jest zapewnienie należytej ochrony infrastruktury informacyjnej. Wyznaczone służby podejmują działania wspólnie z sojusznikami, a także producentami i dostawcami urządzeń oraz oprogramowania komputerowego, krajowymi operatorami telekomunikacyjnymi i dostawcami usług internetowych, ośrodkami badawczymi i szkoleniowymi.

Ogniwa informacyjne, zarówno cywilne, jak i wojskowe realizują zadania związane z ochroną i propagowaniem polskich interesów na arenie międzynarodowej, informacyjnym osłabianiem przeciwnika oraz umacnianiem morale, determinacji obronnej i wytrwałości własnego społeczeństwa.

Do czynników, które należy brać pod uwagę, można zaliczyć: tworzenie środowiska informacyjnego, dotychczasowy rozwój państwa i jego przyszłość, prawo, nowe technologie (w tym szczególnie informacyjne), sytuację polityczną i ekonomiczną na świecie.

Infrastruktura informacyjna powinna zapewnić bezpieczny obieg danych w czasie niemal rzeczywistym, co przyczyni się do wzmocnienia własnego potencjału oddziaływania. Infrastrukturę powinny tworzyć systemy sensorowe (np. podsystemy zdobywania informacji źródłowych, zarządzania oraz sterowania urządzeniami elektronicznymi).

Działania wymagane do tworzenia strategicznej infrastruktury informacyjnej są kompleksowe. Ważną rolę w tym zakresie odgrywa planowanie systemów informacyjnych oraz zarządzanie nimi, niemniej jednak należy brać pod uwagę adaptowanie systemów do zmieniających się warunków otoczenia oraz wdrażanie nowych technologii. Technologia informacyjna musi być całkowicie wykorzystana we wszystkich obszarach, ale także musi łatwo się przystosowywać do zmieniających się potrzeb.

**Rola struktur operacji informacyjnych w systemie bezpieczeństwa narodowego**

Realizacja polityki RP, m.in. wspieranie polityki ONZ, NATO, UE w obszarze zarządzania kryzysowego i w działaniach stabilizacyjnych, wiązać się będzie z potrzebą uwzględnienia w planowaniu strategicznym rozszerzonego spektrum zagrożeń, zwłaszcza o charakterze asymetrycznym oraz nowego kontekstu technologicznego. Warunkami powodzenia operacji wojskowych oraz pozamilitarnych będą przede wszystkim: uzyskanie przewagi informacyjnej; użycie struktur zadaniowych, wyposażonych w nowocześniejszy sprzęt techniczny od sprzętu przeciwnika; zastosowanie zaawansowanych technologii informacyjnych w zakresie dowodzenia; posiadanie możliwości skutecznego rażenia, dokonywania manewru i ochrony przed rażeniem przeciwnika; umiejętne stosowanie symetrycznej strategii wobec działań przeciwnika, pełne wykorzystanie zasobów informacyjnych kraju oraz realizacja współpracy cywilno-wojskowej.

Przewaga informacyjna jest celem, który można uzyskać przez prowadzenie operacji informacyjnych. Przewaga informacyjna jest także środkiem do uzyskania innych celów, np. politycznych, ekonomicznych na poziomie strategicz-

nym lub operacyjnym. Operacje informacyjne są prowadzone z intencją uzyskania sukcesu (przewagi informacyjnej), ale także są prowadzone w celu uniemożliwienia uzyskania przewagi informacyjnej.

Przedsięwzięcia dotyczące uzyskania przewagi informacyjnej wchodzą w skład szerszego kompleksu działań właściwych dla operacji informacyjnych, obejmują m.in. tworzenie infosfery, zarządzanie systemami i zasobami informacyjnymi oraz akcje prowadzone w ramach dezinformacji. Wszelkie działania w tym zakresie są wspomagane przez technologię informacyjną.

Zdobywanie użytecznych informacji jest „kluczowym" czynnikiem uzyskania przewagi informacyjnej. Dlatego zarówno źródła zdobywania danych, jak i realizowane przedsięwzięcia muszą odpowiadać światowym standardom, w innym wypadku mogą wystąpić przeszkody w uzyskaniu przewagi informacyjnej. Dlatego też należy prowadzić badania dotyczące nowych technologii informacyjnych i wdrażać w życie nowe sposoby. Ponadto tylko użyteczne dane powinny być odbierane i przekazywane, gdyż niepożądane dane (nieprawdziwe) mogą opóźnić proces decyzyjny oraz przyczynić się do niewykonania misji. Zdobywanie użytecznych danych jest ważne nie tylko dla uzyskania przewagi informacyjnej, ale także dla procesu decyzyjnego.

Z perspektywy użyteczności (osiąganych celów) przewaga informacyjna i proces decyzyjny są ściśle ze sobą powiązane. Możliwość opóźnienia przekazu danych u strony przeciwnej, obrazujących położenie strategiczne, zwiększa skuteczność wpływu na podejmowanie przez niego decyzji[18]. Informacja jest ważnym elementem w procesie decyzyjnym, natomiast technologia znacznie przyspiesza cykl decyzyjny, jeśli oczywiście wykorzystywana ona jest w ramach prowadzenia operacji informacyjnych, których rezultaty wspomagają proces decyzyjny w operacjach militarnych. Ważną rolę odgrywa tu bieżąca i użyteczna informacja, gdy napływ bieżących danych zostanie zakłócony, proces decyzyjny może zakończyć się fiaskiem.

Technologia informacyjna może być nieużyteczna dla uzyskania przewagi informacyjnej, dopóki nie jest dostosowana do prowadzonych działań. Zdobywanie, przetwarzanie, dystrybucja i wykorzystanie danych są częścią szerszego kompleksu działań prowadzonych w ramach operacji informacyjnych. Działania te przyczyniają się do uzyskania przewagi informacyjnej i wymagają stosowania technologii informacyjnej oraz posiadania aktualnych i użytecznych danych. W dzisiejszym globalnym środowisku informacyjnym (satelity, komputery) uzyskanie przewagi informacyjnej bez wykorzystania technologii informacyjnej jest niemożliwe.

[18] D.J. Dishong, *On Studying the Effect of Information Warfare on C2 Decision Making*, Naval Postgraduate School, 1994. Autor przeprowadził eksperyment, do którego wykorzystał program symulacji komputerowej nazwany „Tactical Tic-Tac-Toe". Eksperyment udowodnił, że opóźnienie w tworzeniu obrazu pola walki na poziomie taktycznym u przeciwnika zwiększa możliwość odniesienia sukcesu w walce oraz w znaczny sposób zmniejsza straty własne.

Przewaga w infosferze wymaga mistrzowskiego zdobywania informacji, jej wykorzystania oraz manipulacji nią. Przewaga informacyjna może się przyczynić do osiągnięcia sukcesu w walce. Przewaga informacyjna jest kamieniem węgielnym umożliwiającym decydentom podjęcie właściwej decyzji. Struktury operacji informacyjnych mają zastosowanie zarówno podczas sytuacji kryzysowych, stanach wyjątkowych, czy wojennych.

## WNIOSKI

W wieku informacji zapotrzebowanie na użyteczną informację staje się jednym z najważniejszych zadań działalności w sferze cywilnej i militarnej. Aktualnie informacja jest traktowana jako zasób strategiczny. To wskazuje, że informacja i technologie informacyjne powinny zostać włączone w proces decyzyjny. Uzyskiwana w tym zakresie przewaga staje się nie tylko gwarantem, ale wręcz warunkiem bezpiecznej egzystencji i to nie tylko w skali pojedynczego człowieka czy instytucji, ale w odniesieniu do państwa czy koalicji.

Najistotniejsze staje się zapewnienie sprawności i bezpieczeństwa systemów informacyjnych, zwalczanie przestępczości komputerowej wymierzonej w infrastrukturę informacyjną i przede wszystkim uzyskanie przewagi informacyjnej. Uzyskanie przewagi informacyjnej wymagać będzie mistrzowskiego zdobywania informacji, jej wykorzystania oraz manipulowania nią, aby osiągnąć cele polityczne i wojskowe. Dlatego też wiele krajów na świecie opracowuje koncepcje operacji informacyjnych oraz tworzy struktury do ich realizacji. W wieku industrialnym zwycięstwo nad państwem uprzemysłowionym oznaczało zniszczenie nie tylko poważnej części jego armii, ale także pozbawienie bogactw naturalnych i bazy przemysłowej. Natomiast zwycięstwo nad państwem wieku informacji wymaga pozbawienia go możliwości wykorzystania jego systemów informacyjnych. Tę możliwość zapewniają właśnie operacje informacyjne, które mogą być prowadzone zarówno przez siły zbrojne, jak i organy pozamilitarne.

Na podstawie literatury przedmiotu należy sądzić, że w przyszłych konfliktach oraz sytuacjach kryzysowych, dążenie do uzyskania przewagi informacyjnej nad potencjalnym przeciwnikiem (konkurentem) przez prowadzenie operacji informacyjnych stanie się regułą postępowania.

## LITERATURA

Bujak A., *Możliwe kierunki zmian w reagowaniu kryzysowym (cz. I)*, „Zeszyty Naukowe WSOWLąd" nr 2/2005, Wrocław 2005.

Ciszewski T., *Zarządzanie sytuacją kryzysową w środowisku zagrożonym IED*, „Zeszyty Naukowe WSOWLąd", nr 3 (157), Wrocław 2010.

Couffignal L., *Cybernetyka*, Paryż 1965.

Dishong D.J., *On Studying the Effect of Information Warfare on C2 Decision Making*, Naval Postgraduate School, 1994.

Głuszkow W., *Wstęp do cybernetyki*, Naukowa Dumka, Kijów 1963.

Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania.* Wydaw. Fundacji Postępu i Telekomunikacji, Kraków 1999.

Greniewski H., *Cybernetyka niematematyczna*, PWN, Warszawa 1982.

Kopaliński W., *Słownik wyrazów obcych i zwrotów obcojęzycznych*, Wiedza Powszechna, Warszawa 1980.

Kotarbiński T., *Traktat o dobrej robocie*, Wrocław 1982.

Madej M., *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*, Warszawa 2007.

Piątkowski K., *Wojna nowego typu?*, „Polska w Europie" nr 1 z marca 2002.

Seidler J., *Nauka o informacji*, WNT, Warszawa 1983.

Shannon C.E., Warren W., *The Mathematical Theory of Communication*, The University of Illinois Press, Urbana 1949.

Wejkszner A., *Wojny XXI wieku. Istota konfliktów asymetrycznych* [w:] *Zagrożenia asymetryczne współczesnego świata*, red. S. Wojciechowski, R. Fiedlera, Poznań 2009.

Wiener N., *Cybernetics or Control and Communication in the Animal and the Machine*, New York, Hermann & Cie, The Technology Press, and John Wiley & Sons, 1948.

Wooldridge, D.E., *Sensory Processing in the Brain: An Exercise in Neuroconnective Modeling*. Wiley, New York 1979.

*Streszczenie*

W artykule wyjaśniono termin „informacja" oraz przedstawiono znaczenie informacji w systemie informacyjnym oraz działaniu celowym. Potencjalny agresor dokonując destrukcji systemów informacyjnych może sparaliżować funkcjonowanie organizacji lub całego państwa. Świadczy to o tym, że zagrożenia w sferze informacyjnej stają się realnym zagrożeniem dla bezpieczeństwa narodowego. Aby się przed tym uchronić, potrzebna jest wiedza o stanie otoczenia i rodzących się przesłankach zagrożeń. Elementem kluczowym w tym zakresie staje się posiadanie przewagi informacyjnej, którą można uzyskać przez prowadzenie operacji informacyjnych.

**The importance of information in National Security area**

*Summary*

The paper refers to term of information and the importance of information in information systems and purpose action. Potential aggressor causing destruction of information systems can cripple functioning of organization or all over the nation. It means, that threats of information sphere are getting real threats for National Security. The knowledge of surrounding area situation and the occurrence of the threats is required to defend. The key element in mentioned range is got information dominance, that can be given by realization of information operations.