Roczniki Kolegium Analiz Ekonomicznych
nr 29/2013

Andrzej Żebrowski

Wydział Humanistyczny
Uniwersytet Pedagogiczny w Krakowie

Bezpieczeństwo informacyjne Polski a walka informacyjna

Wstęp

Bezpieczeństwo informacyjne państwa ma ścisły związek z jego bezpieczeństwem wewnętrznym i zewnętrznym. Wszechobecna globalizacja, rozwój społeczeństwa informacyjnego i technologii teleinformatycznych zmieniły obecne środowisko bezpieczeństwa państw, w tym również Rzeczypospolitej Polskiej. W środowisku bezpieczeństwa międzynarodowego i otoczeniu wewnętrznym państwa znaczącą pozycję zajmuje walka informacyjna, która stanowi zagrożenie praktycznie dla wszystkich sfer działania zarówno państwa, jak i jednostki.

W niniejszym artykule zostały poruszone kwestie dotyczące bezpieczeństwa informacyjnego naszego państwa w aspekcie trwającej walki informacyjnej, a także konieczności wypracowania i przyjęcia doktryny bezpieczeństwa informacyjnego Rzeczypospolitej Polskiej.

Bezpieczeństwo państwa

Bezpieczeństwo państwa to taki rzeczywisty stan stabilności wewnętrznej i suwerenności państwa, który odzwierciedla brak lub występowanie jakichkolwiek zagrożeń (w sensie zaspokajania podstawowych potrzeb egzystencjalnych i behawioralnych społeczeństwa oraz traktowania państwa jako suwerennego podmiotu w stosunkach międzynarodowych)[1]. Mając na uwadze szerokie

[1] S. Dworecki, *Zagrożenia bezpieczeństwa państwa*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 1994, s. 16.

rozumienie bezpieczeństwa państwa, można przyjąć, że jest to zdolność władz i narodu do ochrony swoich wewnętrznych wartości. Do najważniejszych wartości chronionych przez państwo należą: przetrwanie państwa jako instytucji i narodu jako grupy etnicznej, biologiczne przeżycie ludności, integralność terytorialna państwa, jego niezależność polityczna i swoboda działania międzynarodowego, spokój, ochrona własności, jakość życia obywateli[2].

Należy mieć świadomość tego, że bezpieczeństwo państwa nie jest wartością stałą, ale procesem, który pod wpływem zmian występujących w jego otoczeniu zewnętrznym (bliższym i dalszym) i wewnętrznym wymaga dostosowania do pojawiających się zagrożeń i szans. Wymaga to utrzymania potencjałów militarnego i pozamilitarnego, którym należy podporządkować wiele rzeczowych i funkcjonalnych elementów państwa.

Bezpieczeństwo państwa w okresie bipolarnego podziału świata opierało się przede wszystkim na sile militarnej, a więc był to stan uzyskany w rezultacie utrzymywania odpowiednio zorganizowanych i wyposażonych sił zbrojnych oraz zawartych sojuszów wojskowych, a także posiadania koncepcji strategicznej wykorzystania będących w dyspozycji sił, stosownie do zaistniałej sytuacji[3]. Podejście takie jest dużym uproszczeniem, ponieważ siła militarna państwa zależy od jego „potencjału obronnego, przez który należy rozumieć całokształt możliwości materiałowych i moralnych, które mogą być spożytkowane w celu zapewnienia bezpieczeństwa państwa (prowadzenia wojny). Od jego wielkości zależy siła obronna państwa. W potencjale obronnym państwa wyróżnia się m.in. potencjał obronno-gospodarczy[4] i potencjał wojskowy (militarny)[5] państwa"[6].

*

Działalnością państwa w środowisku bezpieczeństwa międzynarodowego kierują dwa dążenia pierwotne, które są odzwierciedleniem jego podstawowych interesów narodowych:

---

[2] J. Zając, *Bezpieczeństwo państwa*, w: *Bezpieczeństwo państwa*, red. K.A. Wojtaszczyk, A. Materska-Sosnowska, Oficyna Wydawnicza ASPRA-JR, Warszawa 2009, s. 18.

[3] *Słownik terminów z zakresu bezpieczeństwa narodowego*, red. W. Łepkowski, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2009, s. 16.

[4] Potencjał obronno-gospodarczy – część potencjału obronnego państwa, określającego jego możliwości w zakresie gospodarczego zaspokajania potrzeb obronnych (prowadzenia wojny); ibidem, s. 103.

[5] Potencjał wojskowy – ogólna zdolność sił zbrojnych państwa (koalicji) do prowadzenia walki zbrojnej w skali wojny (w skali strategicznej) dla osiągnięcia celów nakreślonych przez politykę; ibidem, s. 105.

[6] Ibidem, s. 104.

– wola przetrwania, zachowania odrębnego istnienia i tożsamości, co w odniesieniu do bezpieczeństwa oznacza obronę suwerenności i integralności terytorialnej,
– dążenie do własnej potęgi, niekoniecznie wojskowej i nie tylko w stosunku do innych państw; podstawowym kryterium powinna być ochrona i pomnażanie dobra własnego narodu oraz budowanie jego potęgi.

Realizacja powyższych celów zależy od wielu złożonych i wzajemnie powiązanych czynników, składających się na tzw. potęgę państwa, której elementy przedstawia tabela 1.

Tabela 1. Elementy potęgi państwa

Lp.	Elementy potęgi państwa	
1.	Zajmowane terytorium	wielkość, położenie, klimat, topografia
2.	Bogactwa naturalne	różnorodność, stopień samowystarczalności, dostępność i zakres wykorzystania
3.	Źródła energii	różnorodność, stopień samowystarczalności, dostępność i zakres wykorzystania
4.	Możliwość produkcji żywności	dostępność surowców, racjonalność gospodarowania, efektywność i konkurencyjność wytwarzania
5.	Ludność	liczba, wykształcenie, stan zdrowia, procent w wieku produkcyjnym
6.	Przemysł	różnorodność, wydajność, efektywność, nowoczesność
7.	Transport i komunikacja	równomierność pokrycia obszaru kraju, zasięg, przepustowość, dostępność
8.	Stan oświaty, nauki, techniki	rzeczywiste osiągnięcia, nowoczesność metod i form, dostępność, skuteczność w praktycznych zastosowaniach, nowoczesność rozwiązań konstrukcyjnych i technologicznych
9.	Siły zbrojne	liczebność, patriotyzm, wyszkolenie taktyczne i specjalistyczne, wyposażenie w sprzęt bojowy i pomocniczy, stopień nowoczesności i skuteczności sprzętu, funkcjonalność systemu zasilania
10.	System polityczny, społeczny i gospodarczy	stabilność, akceptowalność
11.	Dyplomacja	przygotowanie fachowe, międzynarodowe uznanie, rzeczywista efektywność i skuteczność prezentowania interesów państwa na arenie międzynarodowej
12.	Charakter i morale społeczeństwa	skład narodowościowy, etniczny i wyznaniowy, poziom tolerancji, poczucie tożsamości narodowej, zaangażowanie i zdolność do poświęceń, poszanowanie prawa

Źródło: *Stosunki międzynarodowe – problemy badań i teorii*, red. A. Bodnar, W.J. Szczepański, PWN, Warszawa 1983, s. 101.

Różne sposoby podejścia do bezpieczeństwa państwa kreują to pojęcie w kategoriach wartości, procesu i stanu[7]:

1) wartość, o którą należy zabiegać w sposób permanentny i uwzględniający zmiany wewnątrz i na zewnątrz państwa,
2) proces obejmuje szereg różnorodnych przedsięwzięć skierowanych przeciw zagrożeniom uniemożliwiającym realizację wszystkich celów państwa,
3) stan, mierzony stosunkiem potencjału obronnego państwa do skali zagrożeń.

Ważne jest to, aby „bezpieczeństwo państwa nie było traktowane tylko jako stan braku zagrożeń w określonych dziedzinach działalności społeczeństwa, ale również (a może nawet – przede wszystkim) bezpieczeństwo powinno być pojmowane jako proces obejmujący szereg przedsięwzięć podejmowanych w celu przygotowania struktur państwa do hipotetycznych zagrożeń lub też eliminowania niekorzystnych zdarzeń w obszarze bezpieczeństwa (zagrożeń potencjalnych) i niedopuszczenia, by przerodziły się one w realne zagrożenia. Zatem bezpieczeństwo państwa jest efektem wynikowym szeregu działań podejmowanych w obszarze zewnętrznych i wewnętrznych uwarunkowań funkcjonowania państwa. Działania te podejmowane są przez wszystkie podmioty prawnie odpowiedzialne za bezpieczeństwo państwa, w tym głównie przez konstytucyjnie wskazane ciała odpowiedzialne za zapewnienie bezpieczeństwa państwa zarówno w wymiarze zewnętrznym, jak i wewnętrznym”[8].

Zapewnienie bezpieczeństwa państwa wymaga prowadzenia określonej polityki bezpieczeństwa, której celem jest zapewnienie: suwerenności i niepodległości; istnienia państwa; przetrwania narodu; zachowania tożsamości narodowej; niezależności gospodarczej, żywnościowej, kulturowej, naukowej, surowcowej itd.; spokoju społecznego; zrównoważonego rozwoju; stanu posiadania[9].

Bezpieczeństwo będące procesem należy budować, tzn. dostosowywać istniejący system bezpieczeństwa wewnętrznego i zewnętrznego do zmieniających się warunków w otoczeniu państwa, w tym trzeba realizować konsekwentnie określone zadania, które powinny zabezpieczać spokojny i zrównoważony rozwój w każdej sytuacji. Zadania te obejmują m.in.: przygotowanie stosownych możliwości obronnych państw; przygotowanie sprawnego i skutecznego systemu ochrony ludności; zabezpieczenie sprawnego funkcjonowania struktur państwa w sytuacji zagrożenia; przygotowanie adekwatnych do zagrożeń i wyzwań

---

[7] K.A. Wojtaszczyk, op.cit., s. 12.

[8] M. Kulisz, *Analiza bezpieczeństwa państwa na płaszczyźnie przedmiotowej*, Zakład Wydawnictw Statystycznych, Radom 2008, s. 5.

[9] J. Gołębiewski, *Bezpieczeństwo narodowe RP*, „Zeszyt Problemowy” Towarzystwa Wiedzy Obronnej, nr 1, Warszawa 1999, s. 13–14.

zasobów ludzkich, materiałowych i programów; zintegrowanie wszystkich sił politycznych do realizacji celów bezpieczeństwa[10].

Skuteczność i efektywność bezpieczeństwa państwa powinna być oparta na trwałych wartościach, które rzutują na jego potencjał bezpieczeństwa. Niektóre składniki potencjału bezpieczeństwa są typowe dla zapewnienia spokojnego i zrównoważonego rozwoju społecznego.

Tabela 2. Elementy potencjału bezpieczeństwa państwa

Lp.	Elementy potencjału bezpieczeństwa
1.	Stabilność wewnętrzna państwa
2.	Skuteczność instytucji publicznych
3.	Dojrzałość elit politycznych
4.	Profesjonalizm administracji publicznej
5.	Aktywność społeczna, polityczna i zawodowa społeczeństwa
6.	Poziom zatrudnienia i bezrobocia
7.	Poziom i zakres udziału społeczeństwa w rządzeniu i zarządzaniu
8.	Liczebność grup etnicznych i mniejszości narodowych
9.	Poszanowanie reguł demokracji i wolnego rynku
10.	Przestrzeganie praw człowieka
11.	Przyswojenie wymogów prawa międzynarodowego i standardów powszechnie akceptowanych
12.	Funkcjonowanie opieki medycznej, społecznej, socjalnej i systemów edukacyjnych
13.	Przestrzeganie praw mniejszości narodowych i grup etnicznych
14.	Poziom rozwoju gospodarczego i społecznego
15.	Poziom dobrobytu lub braku nędzy
16.	Umiejętność prowadzenia dialogu i osiągania rozumnych kompromisów i inne

Źródło: J. Gołębiewski, *Bezpieczeństwo narodowe RP*, „Zeszyt Problemowy" Towarzystwa Wiedzy Obronnej, nr 1, Warszawa 1999, s. 17.

Bezpieczeństwo państwa jest zdeterminowane zagrożeniami dla jego istnienia i narodu w wymiarze zarówno zewnętrznym, jak i wewnętrznym. Jego zakres przedmiotowy wraz z przemianami cywilizacyjnymi ulega ewolucji w kierunku jego rozszerzenia. W następstwie wszechobecnej globalizacji (ze wszystkimi pozytywnymi i negatywnymi następstwami), rewolucji naukowej

[10] Ibidem, s. 14.

i technicznej, a także innych wyzwań społeczność międzynarodowa odeszła od jednowymiarowego, nakierowanego na zagrożenie militarne bezpieczeństwa do jego obecnej, wielowymiarowej postaci.

Bezpieczeństwo państwa zawsze ma ścisły związek z jego bezpieczeństwem informacyjnym. Należy podkreślić, że bezpieczeństwo informacyjne zawsze jest obecne w polityce bezpieczeństwa i obronności państwa. Nie jest nową dziedziną bezpieczeństwa państwa, łączy procedury i narzędzia ochrony danych, informacji i systemów. Istotny jest również postęp naukowo-techniczny, który jest adaptowany na potrzeby ochrony informacji, nie tylko z punktu widzenia jego użyteczności, ale także ze względu na przeciwdziałanie zagrożeniom. Dlatego w sferze bezpieczeństwa informacji pojawia się wiele określeń, takich jak:

1) bezpieczeństwo informacji.
2) cyberbezpieczeństwo,
3) bezpieczeństwo teleinformatyczne.

Mając to na uwadze, można przyjąć, że 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 lub zniszczeniem[11].

W innym ujęciu „bezpieczeństwo informacyjne dotyczy zagwarantowania sobie przez dany podmiot (np. państwo) integralności, kompletności oraz wiarygodności posiadanych zasobów informacyjnych w każdej formie, nie tylko elektronicznej. Odnosi się więc zarówno do wszelkiego rodzaju wysiłków, służących ochronie posiadanych informacji, istotnych w kontekście bezpieczeństwa (a więc mających wpływ na sprawne funkcjonowanie struktur państwowych i społeczeństwa), jak i zapewnieniu przewagi informacyjnej przez zdobywanie nowych lub bardziej aktualnych danych oraz akcje dezinformacyjne wobec ewentualnych przeciwników (państw lub innych podmiotów). […] Z kolei bezpieczeństwo informatyczne (a precyzyjniej teleinformatyczne, ze względu na stopień integracji fizycznej sieci telefonicznych i technologii informatycznych) ma węższy zakres znaczeniowy. Kieruje ono uwagę na zmiany technologiczne w uzyskiwaniu, przechowywaniu, przetwarzaniu oraz przekazywaniu informacji, dokonujące się wraz z upowszechnianiem cyfrowych form prezentacji danych. […] Inaczej rzecz ujmując: bezpieczeństwo informatyczne (teleinformatyczne) odnosi się do faktu szybkiego upowszechniania określonych metod przetwarzania i przesyłania informacji oraz wiążących się z tym konsekwencji w sferze bezpieczeństwa, nie zaś zwięk-

[11] P. Potejko, *Bezpieczeństwo informacyjne*, w: *Bezpieczeństwo państwa…*, op.cit., s. 194.

szenia rangi informacji (niezależnie od sposobu i medium jej przechowywania, przetwarzania i przesyłania) we współczesnym świecie"[12].

Postęp w teleinformatyce sprawił, że piąty wymiar konfrontacji, którym jest cyberprzestrzeń, nie tylko przyczynia się do rozwoju podmiotów państwowych (pozapaństwowych) czy jednostki, ale jest również źródłem poważnych zagrożeń dla ich bezpieczeństwa.

Należy zaznaczyć, że bezpieczeństwa informacyjnego państwa nie można odnosić wyłącznie do bezpieczeństwa w przestrzeni technicznej, pomijając przestrzeń osobową. Podejście takie stanowi duże uproszczenie i jest źródłem rzeczywistych zagrożeń dla informacji. Zbudowanie bezpiecznego systemu ochrony informacji jest praktycznie niemożliwe, najsłabszym ogniwem w każdym systemie jest bowiem człowiek. W związku z tym utrzymanie bezpieczeństwa państwa w aspekcie informacyjnym powinno opierać się na następujących przesłankach[13]:

1) zwiększanie ochrony własnych systemów informacyjnych,
2) stała ocena słabości systemów informacyjnych potencjalnych przeciwników, w tym takie działania, jak możliwości wtargnięcia do ich systemów,
3) przygotowanie możliwych form odpowiedzi na atak, w tym z wykorzystaniem zarówno informacyjnych, jak i konwencjonalnych (wojskowych) środków rażenia,
4) rozwijanie metod szacowania poniesionych i/lub zadanych zniszczeń (strat informacyjnych).

Dlatego właściwe skonstruowany system ochrony, wsparty rozwiązaniami prawno-organizacyjnymi, przestrzeganiem zasad określonych przez politykę bezpieczeństwa informacyjnego, pozwala na realizację funkcji wewnętrznej i zewnętrznej przez państwo.

„Bezpieczeństwo narodowe państw jest coraz bardziej uzależnione od sprawności funkcjonowania infrastruktury informacyjnej (w tym infrastruktury teleinformatycznej). Jej załamanie może spowodować katastrofę, której rozmiar jest z każdym rokiem coraz większy. Groźbę takiego rozwoju wydarzeń stwarzają zarówno skomplikowany charakter powiązań funkcjonalnych i sprzężeń wewnętrznych infrastruktury informacyjnej państwa, jak i lawinowy rozwój teleinformatyki. W ocenie wielu specjalistów, załamanie się funkcjonowania infrastruktury informacyjnej (w tym infrastruktury teleinformatycznej) państwa

[12] M. Madej, *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, w: *Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, Wydawnictwo PISM, Warszawa 2009, s. 18–19.

[13] *Zagrożenia dla bezpieczeństwa informacyjnego państwa (identyfikacja, analiza zagrożeń i ryzyka). Raport z badań*, t. 2, Akademia Obrony Narodowej, Warszawa 2004, s. 109.

doprowadziłoby do dezorganizacji funkcjonowania państwa i zagrożenia jego interesów na świecie"[14].

Walka informacyjna

Wiele problemów dotyczących sfery wewnętrznej państwa wynika z negatywnych oddziaływań zewnętrznych i wewnętrznych w ramach tzw. walki informacyjnej, która jeśli jest umiejętnie prowadzona, może zagrozić zarówno bezpieczeństwu pojedynczych państw, jak i bezpieczeństwu światowemu[15].

Tabela 3. Walka informacyjna

Lp.	Walka informacyjna	
	Państwo	Pojęcie
1.	Stany Zjednoczone	Walka informacyjna to działania podejmowane w celu uzyskania przewagi w tym zakresie przez kształtowanie procesów i systemów informacyjnych oraz sieci komputerowych przeciwnika, przy jednoczesnej ochronie własnych zasobów informacyjnych
2.	RFN	Walka informacyjna jest rozumiana jako wszechstronne wykorzystywanie informacji i technik łączności, jak również technik przeznaczonych do zakłócania i niszczenia wrogich ośrodków informacji i systemów łączności w czasie kryzysu i konfliktu celem osiągnięcia przewagi strategicznej i taktycznej
3.	Wielka Brytania	Walka informacyjna to dążenie do obezwładniania przeciwnika przez zniszczenie jego systemów komputerowych, finansowych, telekomunikacyjnych czy kontroli ruchu
4.	Federacja Rosyjska	Walka informacyjna to kompleks przedsięwzięć obejmujących wsparcie, przeciwdziałanie i obronę informacyjną, prowadzonych według jednolitej koncepcji i planu, w celu wywalczenia i utrzymania panowania nad przeciwnikiem w dziedzinie informacyjnej podczas przygotowania operacji wojskowych oraz prowadzonych działań bojowych

[14] J.L., *Bezpieczeństwo Stanów Zjednoczonych w świetle walki informacyjnej*, „Wojskowy Przegląd Zagraniczny" 1999, nr 3, s. 5.

[15] L. Ciborowski, *Potencjalne zagrożenia – identyfikacja i charakterystyka*, „Myśl Wojskowa" 2000, nr 4, s. 86.

5.	Polska	Walka informacyjna to zorganizowana w formie przemocy aktywność zewnętrzna państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na niszczenie lub modyfikowanie systemów informacyjnego komunikowania się przeciwnika lub przepływających przez nie informacji oraz aktywność zapewniająca ochronę własnych systemów informacyjnego komunikowania i przesyłania przez nie informacji przed podobnym działaniem przeciwnika
		Walka informacyjna to kooperacja negatywnie wzajemna, przynajmniej dwupodmiotowa, realizowana w sferach: zdobywania informacji, zakłócania informacyjnego i obrony informacyjnej, gdy każdemu działaniu jednej strony przyporządkowane jest działanie antagonistyczne strony drugiej
6.	Sojusz Północnoatlantycki	Walka informacyjna to działania informacyjne prowadzone w okresie kryzysu i/lub konfliktu zbrojnego z zamiarem promowania określonego celu politycznego lub wojskowego w odniesieniu do wskazanego przeciwnika lub przeciwników

Źródło: D.E. Denning, *Walka informacyjna i bezpieczeństwo informacyjne*, Wydawnictwo Naukowo-Techniczne, Warszawa 2002, s. 11; R. Szpyra, *Operacje informacyjne państwa w działaniach sił powietrznych*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2002, s. 146; L. Ciborowski, *Walka informacyjna*, Wydawnictwo ECT, Toruń 1999, s. 187; P. Gawliczek, J. Pawłowski, *Zagrożenia symetryczne*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2003, s. 42.

Z przedstawionych definicji wynika, że zakres walki informacyjnej jest znacznie szerszy i łączy się ze sferą nie tylko militarną, ale także pozamilitarną[16]. Jesteśmy bowiem świadkami świadomej dezinformacji i manipulacji, którą prowadzi się w sposób oficjalny i niejawny zarówno w czasie pokoju, jak i w czasie kryzysu oraz wojny, co jest jej cechą charakterystyczną. Należy podkreślić, że walka informacyjna wykracza poza tradycyjne postrzeganie pola walki, jej potencjalni sprawcy (atakujący) i ofiary (atakowani) nie muszą bowiem być związani tylko z siłami zbrojnymi. Działania polegające na zdobywaniu informacji, zakłócaniu informacyjnym, a także obronie informacyjnej nie zostały odkryte pod koniec XX wieku. Zaadaptowane przez podmioty: wojskowe, polityczne, gospodarcze, służby specjalne i policyjne czy przestępcze były wykorzystywane zawsze, choć nie używano terminu „walka informacyjna", którą zalicza się do walki niezbrojnej, co w skrajnych przypadkach prowadzi do fizycznej destrukcji obiektu ataku. „Prowadzona jest wespół z innymi formami – nigdy nie może

[16] A. Żebrowski, *Ewolucja polskich służb specjalnych. Wybrane obszary walki informacyjnej. (Wywiad i kontrwywiad w latach 1989–2003*), Wydawnictwo Abrys, Kraków 2005, s. 30.

występować w oderwaniu, bo nigdy też sama dla siebie nie może stanowić celu. Jej cel wynika zawsze z charakteru i celu walki wspieranej"[17].

„Współcześnie walka informacyjna jest dominującą formą walki w zbiorze walk (zbrojnych i niezbrojnych), ponieważ we wszystkich obszarach działania państwa, a także prywatnym, wykorzystywane są systemy informacyjnego komunikowania. Suma ich funkcjonowania (niezakłóconego) składa się na bezpieczeństwo informacyjne państwa"[18]. Walka informacyjna ma charakter uniwersalny, ponieważ jest prowadzona we wszystkich sferach działania państwa, nie tylko przez komponenty sił zbrojnych, służby specjalne i policyjne, ale również przez konkurencyjne korporacje (czy firmy), wówczas strategie marketingowe, reklamowe, konsumpcyjne i współpraca są podstawowymi obszarami zainteresowania zantagonizowanych stron. Walka ta jest również prowadzona przez państwa w wymiarze zarówno zewnętrznym, jak i wewnętrznym.

Prowadzone działania bez względu na sferę zainteresowania nadają walce informacyjnej nową jakość, mającą ścisły związek z rozwojem teleinformatyki, która jest wszechobecna w naszym codziennym życiu. Stwarza ona warunki (przy braku właściwej ochrony) nieograniczonego dostępu do zasobów informacyjnych podmiotów gospodarczych, naukowych, technologicznych, marketingowych i innych, które realizują zadania w sferze wewnętrznego i zewnętrznego bezpieczeństwa państwa.

Walka informacyjna wpisuje się w formę nie tylko nacisku politycznego, wojskowego czy gospodarczego, ale także zastraszania. Właściwie wypracowane i wdrażane środki oddziaływania informacyjnego stanowią potężne narzędzie walki w znaczeniu ogólnym. W sferze negatywnych wpływów mogą znaleźć się zarówno jednostki, jak i podmioty o kluczowym znaczeniu dla bezpieczeństwa wewnętrznego i zewnętrznego państwa. Istotne jest to, że walka informacyjna pełni funkcję uniwersalną, co pozwala na osiągnięcie zamierzonych efektów w czasie rzeczywistym. „Umiejętne prowadzenie walki informacyjnej może doprowadzić do bardzo szybkiego zerwaniu wielu żywotnych funkcji współczesnej infrastruktury cywilnej i wojskowej. […] Paraliżuje głównie jej funkcjonowanie i w ten sposób znacznie ogranicza egzystencję państw objętych światową konkurencją"[19].

[17] L. Ciborowski, *Mechanizmy i przestrzenie walki informacyjnej*, w: *Informacja w walce zbrojnej*, red. G. Nowacki, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2002, s. 45.

[18] A. Żebrowski, op.cit., s. 30.

[19] L. Ciborowski, *Potencjalne zagrożenia…*, op.cit., s. 86.

Tabela 4. Ukierunkowanie walki informacyjnej

Lp.	Ukierunkowanie walki informacyjnej
1.	Zdalne wprowadzanie do sieci informatycznych wirusów komputerowych, dostosowanych programowo do samopowielania i szybkiego rozprzestrzeniania
2.	Lokowanie w systemach informatycznych tzw. bomb logicznych, które jako odpowiednio opracowane aplikacje programowe będą dostosowane do uaktywniania się na określone wcześniej sygnały lub według zaprogramowanych wcześniej reżimów czasowych
3.	Blokowanie wymiany danych w torach transmisyjnych, deformowanie treści oraz wprowadzanie do systemów informacyjnych nieprawdziwych treści logicznych za pośrednictwem środków masowego przekazu, kanałów łączności rządowej i wojskowych systemów dowodzenia
4.	Wprowadzanie wirusów komputerowych do rządowych oraz komercyjnych sieci i systemów informatycznych, jak również układów zdalnego sterowania tymi systemami
5.	Wytwarzanie impulsów wielkiej mocy, zaprogramowanych na niszczenie urządzeń elektronicznych, a także środków biologicznych – specjalnych mikrobów – do niszczenia obwodów elektronicznych i materiałów izolacyjnych
6.	Stosowanie broni elektronicznej przeciwko wybranym elementom infrastruktury i przemysłu, powodujące np. paraliżowanie łączności, transportu, dopływu energii elektronicznej, czyli paraliżowanie życia w danym regionie

Źródło: L. Ciborowski, *Potencjalne zagrożenia – identyfikacja i charakterystyka*, „Myśl Wojskowa" 2000, nr 4, s. 86–87.

„Na szczególną uwagę zasługują zewnętrzne oddziaływania informacyjne, którymi mogą być objęte procedury sterowania procesami decyzyjnymi państwa, na które ukierunkowany jest atak informacyjny. Może to być realizowane poprzez wprowadzanie do jawnego i niejawnego systemu informacyjnego danego państwa złożonych zbiorów precyzyjnie dobranych prawdziwych i fałszywych danych z zamysłem osiągnięcia z góry zaplanowanego celu, jakim może być np. tworzenie określonych nastrojów politycznych czy społecznych"[20]. Do realizacji tych złożonych i wzajemnie powiązanych przedsięwzięć, obok wyspecjalizowanych podmiotów, angażowane są media, które w sposób dla siebie nieświadomy, w pogoni za sensacją, jako elementy podatne na dezinformowanie stanowią skuteczne narzędzie w procesie prowadzonej walki informacyjnej. Walka informacyjna to podejmowanie wielu złożonych działań, których podstawowym celem było i jest zdobycie przewagi informacyjnej nad przeciwnikiem.

[20] Ibidem, s. 87.

Doktryna bezpieczeństwa informacyjnego

Bezpieczeństwo narodowe (państwa) rozumiane jest szeroko, jako stan uzyskany w rezultacie odpowiednio zorganizowanej obrony i ochrony przed wszelkimi zagrożeniami militarnymi i niemlitarnymi, tak zewnętrznymi, jak i wewnętrznymi, przy użyciu sił i środków pochodzących z różnych dziedzin działalności państwa[21]. Jedną z podstawowych dziedzin tej działalności, co należy wyraźnie podkreślić, jest bezpieczeństwo informacyjne państwa.

Można przyjąć, że dogmat „siła ognia jest potęgą" powoli jest zastępowany stwierdzeniem, że potęgą jest informacja. Jesteśmy świadkami gwałtownego rozwoju potencjałów informacyjnych, co oznacza konieczność poszukiwania odpowiedzi na pytanie: jak skutecznie oddziaływać informacyjnie na przeciwnika, dezorganizować jego systemy informacyjne, przy jednoczesnym zapewnianiu sprawności własnych systemów informacyjnych?

W aspekcie prowadzonych rozważań i trwającej rewolucji w technice teleinformatycznej państwo powinno zająć się problematyką walki informacyjnej prowadzonej w przestrzeni zarówno osobowej, jak i technicznej, mając na uwadze wypracowanie i przyjęcie doktryny (a może strategii) bezpieczeństwa informacyjnego Rzeczypospolitej Polskiej. W tym miejscu rozważań warto wskazać na przyczyny zainteresowania się walką informacyjną, która ma charakter złożony i wielowymiarowy. Można do nich zaliczyć m.in.:

1) upadek bipolarnego podziału świata (systemu państw socjalistycznych) to m.in. wynik długofalowej walki informacyjnej,
2) przebieg, charakter i wyniki wojny antyirackiej w rejonie Zatoki Perskiej, która została określona przez Amerykanów jako pierwsza w historii wojskowości wojna informacyjna; walka informacyjna, stanowiąca istotne uzupełnienie tradycyjnych metod walki, w formie uderzeń ogniowych na systemy informacyjne Iraku (stacje radiolokacyjne, stanowiska dowodzenia, węzły linii wysokiego napięcia, węzły systemów telekomunikacyjnych itp.) przyniosła zwielokrotnienie skutków uderzeń ogniowych na wojska irackie,
3) poszukiwanie nowych metod i środków odstraszania, mogących stworzyć wystarczającą barierę ochronną dla interesów Polski,
4) nieprzewidywalne i przypadkowe dotychczas wyniki operowania informacją mogą obecnie przyjąć formę działań zinstytucjonalizowanych i przewidywalnych (oczywiście tylko w pewnym zakresie),

[21] *Słownik terminów z zakresu bezpieczeństwa…*, op.cit., s. 169.

5) powszechne wykorzystywanie techniki teleinformatycznej we wszystkich sferach działania państwa, ze szczególnym wskazaniem na podmioty właściwe w sferze bezpieczeństwa wewnętrznego i zewnętrznego państwa,
6) rosnące uzależnienie Sił Zbrojnych Rzeczypospolitej Polskiej od cywilnej infrastruktury łączności naziemnej i satelitarnej oraz komercyjnej techniki teleinformatycznej,
7) rosnącą zależność środków ogniowych od systemów łączności, rozpoznania i techniki teleinformatycznej, w których podejmowane są działania mające na celu utworzenie systemów rozpoznawczo-uderzeniowych na szczeblu operacyjnym,
8) powstanie i rozwijanie się światowej sieci informatycznej,
9) rosnącą liczbę przypadków penetracji sieci i systemów teleinformatycznych przez podmioty (osoby) nieuprawnione.

Osoby będące we władzy wykonawczej i ustawodawczej powinny mieć świadomość, że walka informacyjna stanowi kluczowy element bezpieczeństwa wewnętrznego i zewnętrznego państwa. „Ważne jest również i to, że walka informacyjna może zaistnieć w formie walki sieci informatycznych i walki cybernetycznej, łączącej najnowsze zdobycze techniki [podwójnego zastosowania – A.Ż.] w wielowiekową ideą zwycięstwa bez zniszczeń fizycznych. W tym wypadku informacja jest zarówno bronią, jak i celem, nie jest postrzegana jako mnożnik potencjału bojowego własnych siła zbrojnych. Obiektem ataku będzie treść informacji zawartych w sieciach łączności i w sieciach informatycznych. Celem walki informacyjnej w omawianej sferze jest infrastruktura polityczna, społeczna, gospodarcza i wojskowa przeciwnika”[22].

Istotne jest również to, że ta forma walki informacyjnej z wykorzystaniem techniki teleinformatycznej (nieniszczącej) nie wymaga formalnej deklaracji wojny, przynajmniej w jej historycznym rozumieniu. Ponadto umiejętne stosowanie tej formy walki sprawia, że nie jest ona wykrywalna, a w przypadku jej wykrycia atakujący najczęściej pozostaje anonimowy. Powszechny dostęp do technik teleinformatycznych i niskie koszty pozwalają na podjęcie walki informacyjnej zarówno przez podmioty państwowe, pozapaństwowe, jak i zwykłych ciekawskich.

Mając na uwadze specyfikę walki informacyjnej, należy stwierdzić, że w aspekcie strategicznym konieczne jest zainteresowanie się (nadzorowanie) tego rodzaju działalnością z pozycji uprawnionych podmiotów politycznych

[22] J.L., *Amerykańska koncepcja walki informacyjnej*, „Wojskowy Przegląd Zagraniczny” 1998, nr 4, s. 18.

władzy państwowej, ponieważ nie istnieją w tej dziedzinie jakichkolwiek ramy prawne, a tym bardziej etyczne, mogące ukierunkować działalność obejmującą swobodną grę w sferze bezpieczeństwa wewnętrznego i zewnętrznego państwa.

Warunkiem zapewniającym ciągłe utrzymywanie inicjatywy na poziomie strategicznym zarządzania bezpieczeństwem państwa jest przewaga informacyjna, która ma bezpośrednie przełożenie na koncepcje doktrynalne odnoszące się do infrastruktury cywilnej i wojskowej systemów kierowania państwem i dowodzenia siłami zbrojnymi, a także szeroko rozumianych operacji informacyjnych.

Wypracowana i przyjęta doktryna bezpieczeństwa informacyjnego Rzeczypospolitej Polskiej powinna wspierać inicjatywę egzekutywy w tworzeniu nowych aktów prawnych w przedmiotowej sprawie, a także poddawać analizie i ocenie wewnętrzne i zewnętrzne źródła konfliktów w cyberprzestrzeni. Niniejszy dokument powinien definiować interes narodowy Rzeczypospolitej Polskiej w sferze informacyjnej i telekomunikacyjnej. Powinien on być realizowany na trzech podstawowych poziomach: państwa, społeczeństwa i jednostki. Doktryna powinna wskazywać obszary interesów narodowych Rzeczypospolitej Polskiej w sferze informacji:

1) utrzymanie zasady konstytucyjnego prawa obywateli do wiarygodnych informacji,
2) zaplecze informacyjne polityki zagranicznej Rzeczypospolitej Polskiej (zagraniczna propaganda państwa, kontrola nad modernizacją systemów informacyjnych ukierunkowanych na kształtowanie pozytywnego wizerunku zewnętrznego państwa),
3) rozwój technologii, w tym zaplecza przemysłu informacyjnego, telekomunikacji,
4) ochrona danych i zasobów prywatnych oraz zasobów publicznych przed nieuprawnionym dostępem, działaniami przestępczymi i terrorystycznymi (cyberterrorystycznymi).

Doktryna bezpieczeństwa informacyjnego związana z walką informacyjną powinna uwzględniać szerokie spektrum zagrożeń dla: wolności konstytucyjnych i praw człowieka, bezpieczeństwa informacyjnego państwa, infrastruktury krytycznej państwa. Ponadto powinna wskazywać zagrożenia dla bezpieczeństwa informacyjnego państwa w wymiarze wewnętrznym i zewnętrznym:

1) zagrożenia wewnętrzne to bezprawne przechwytywanie danych (w tym niekontrolowany ulot informacji), zmiany treści danych w systemach informacyjnych, wykorzystywanie niecertyfikowanych technologii (teleinformatycznych) zagranicznych, naruszanie prawa w zakresie rozprzestrzeniania danych o charakterze niejawnym itp.,

2) zagrożenia zewnętrzne to: działalność służb specjalnych i podmiotów informacyjnych państw trzecich, działalność państw trzecich ograniczająca interesy państwa w światowym obrocie informacyjnym, ograniczanie aktywności państwa na informacyjnych rynkach wewnętrznych i zewnętrznych, restrykcyjna polityka dotycząca eksportu technologii i produktów informacyjnych, działalność cyberterrorystyczna.

Doktryna powinna również wskazywać priorytety dotyczące kształtowania polityki naukowej i technicznej związanej z teleinformatyką, a także wspierać badania na poziomie strategicznym rozwoju sektora naukowego i technicznego, technologicznego, ekonomicznego oraz odkrycia, nieopatentowane technologie, kadry naukowo-techniczne i ich kształcenie, ochronę przemysłu jądrowego.

Kolejny problem wymagający uregulowania to bezpieczeństwo wewnętrzne i obronność państwa, co wiąże się m.in. z ochroną infrastruktury informacyjnej Sił Zbrojnych Rzeczypospolitej Polskiej i podmiotów realizujących zadania w tym obszarze. Za zewnętrzne zagrożenia dla systemu obronnego Rzeczypospolitej Polskiej należy uznać: działalność rozpoznawczą obcych służb specjalnych ukierunkowaną na komponenty rodzajów sił zbrojnych, działalność dywersyjną metodami informatycznymi, cyberterroryzm. Analogiczne zagrożenia odnosi się do wewnętrznych grup terrorystycznych i przestępczych.

Wspomniany dokument powinien również określać odpowiedzialność państwa za koordynację i kontrolę procesu budowania jego bezpieczeństwa informacyjnego. Ponadto należy wskazać podmioty państwowe i pozapaństwe odpowiedzialne za realizację zasad doktryny bezpieczeństwa informacyjnego Rzeczypospolitej Polskiej. Dokument ten powinien być aktualizowany z uwzględnieniem postępu naukowego i technicznego, a także pojawiających się zagrożeń związanych z prowadzoną walką informacyjną.

Zakończenie

Zagrożenia dla infrastruktury państwa, których źródłem jest wszechobecna walka informacyjna, wymagają od podmiotów państwowych, pozapaństwowych i jednostek zaangażowania w proces budowania bezpieczeństwa informacyjnego państwa. W tym złożonym procesie ważne jednak jest wsparcie ze strony legislatywy i egzekutywy, m.in. w postaci przyjęcia i praktycznego wdrożenia doktryny bezpieczeństwa informacyjnego Rzeczypospolitej Polskiej, która wraz

ze zmianami zachodzącymi w otoczeniu zewnętrznym i wewnętrznym państwa powinna być aktualizowana.

Bibliografia

1. Ciborowski L., *Mechanizmy i przestrzenie walki informacyjnej*, w: *Informacja w walce zbrojnej*, red. G. Nowacki, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2002.
2. Ciborowski L., *Potencjalne zagrożenia – identyfikacja i charakterystyka*, „Myśl Wojskowa" 2000, nr 4.
3. Ciborowski L., *Walka informacyjna*, Wydawnictwo ECT, Toruń 1999.
4. Denning D.E., *Walka informacyjna i bezpieczeństwo informacyjne*, Wydawnictwo Naukowo-Techniczne, Warszawa 2002.
5. Dworecki S., *Zagrożenia bezpieczeństwa państwa*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 1994.
6. Gawliczek P., Pawłowski J., *Zagrożenia symetryczne*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2003.
7. Gołębiewski J., *Bezpieczeństwo narodowe RP*, „Zeszyt Problemowy" Towarzystwa Wiedzy Obronnej, nr 1, Warszawa 1999.
8. J.L., *Amerykańska koncepcja walki informacyjnej*, „Wojskowy Przegląd Zagraniczny" 1998, nr 4.
9. J.L., *Bezpieczeństwo Stanów Zjednoczonych w świetle walki informacyjnej*, „Wojskowy Przegląd Zagraniczny" 1999, nr 3.
10. Kulisz M., *Analiza bezpieczeństwa państwa na płaszczyźnie przedmiotowej*, Zakład Wydawnictw Statystycznych, Radom 2008.
11. Madej M., *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, w: *Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, Wydawnictwo PISM, Warszawa 2009.
12. Potejko P., *Bezpieczeństwo informacyjne*, w: *Bezpieczeństwo państwa*, red. K.A. Wojtaszczyk, A. Materska-Sosnowska, Oficyna Wydawnicza ASPRA-JR, Warszawa 2009.
13. *Słownik terminów z zakresu bezpieczeństwa narodowego*, red. W. Łepkowski, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2009.
14. *Stosunki międzynarodowe – problemy badań i teorii*, red. A. Bodnar, W.J. Szczepański, PWN, Warszawa 1983.
15. Szpyra R., *Operacje informacyjne państwa w działaniach sił powietrznych*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2002.

16. Wojtaszczyk K.A., *Bezpieczeństwo państwa – konceptualizacja pojęć*, w: *Bezpieczeństwo państwa*, red. K.A. Wojtaszczyk, A. Materska-Sosnowska, Oficyna Wydawnicza ASPRA-JR, Warszawa 2009.
17. *Zagrożenia dla bezpieczeństwa informacyjnego państwa (identyfikacja, analiza zagrożeń i ryzyka). Raport z badań*, t. 2, Wydawnictwo Akademia Obrony Narodowej, Warszawa 2004.
18. Zając J., *Bezpieczeństwo państwa*, w: *Bezpieczeństwo państwa*, red. K.A. Wojtaszczyk, A. Materska-Sosnowska, Oficyna Wydawnicza ASPRA-JR, Warszawa 2009.
19. Żebrowski A., *Ewolucja polskich służb specjalnych. Wybrane obszary walki informacyjnej. (Wywiad i kontrwywiad w latach 1989–2003*), Wydawnictwo Abrys, Kraków 2005.

* * *

Polish information security and information warfare

Summary

The acquisition of information, the protection of information and its use has always accompanied human operations. Since the nineties of the last century this process is referred to as the information warfare, which is supported by information technology infrastructure. The information warfare is carried out in all areas of the state operations, and its participants are state actors, non-state actors, as well as individuals. Their main aim is to obtain information superiority over the enemy, disrupt his perception and protect one's own information assets against corresponding actions of the opposing party. The effective information warfare requires many complex legal and organisational projects where the information security doctrine constitutes, among others, the basis for the effective operation of the authorised entities in the complex challenge of information security.

Keywords: national security, the state's information security, information warfare, doctrine