prof. dr hab. inż. Yury Pauliuchuk
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
Wydział Nauk Społecznych
ORCID 0000-0002-2077-5124

prof. dr hab. Nadezhda Psareva
Akademia Pracy i Stosunków Społecznych
w Moskwie, Federacja Rosyjska

BEZPIECZEŃSTWO INFORMACYJNE

INFORMATION SECURITY

Streszczenie
W opracowaniu pod tytułem *Bezpieczeństwo informacyjne* przedstawiono jak jest bardzo ważna informacja i dlaczego tak jest bardzo ważna ochrona. Przedstawiono również jakie zagrożenia informacyjne mogą szkodzić interesom państwa. W opracowaniu zwrócono również uwagę, że każda płaszczyzna bezpieczeństwa narodowego staje się coraz bardziej zależna od swobodnego przepływu informacji i od zachowania systemów bazujących na informacjach. Każda gałąź gospodarki na przykład energetyka, media, systemy finansowe i transportowe itp. są szczególnie uzależnione od systemów informatycznych. Już dziś stanowią one kluczowe elementy procesu podejmowania decyzji w wielu organizacjach cywilnych i wojskowych. Podkreślono również, że w miarę intelektualnego rozwoju i politechnizacji życia informacje zaczęły nabierać coraz większych wartości. Ich posiadanie stało się warunkiem lepszej i bezpieczniejszej egzystencji. Na tym też tle pojawiła się konkurencja. Informacje zaczęto coraz bar-dziej chronić jako dobro materialne.

Słowa kluczowe: bezpieczeństwo, dyplomacja, gospodarka, informacja, systemy

Abstract
The study entitled Information security shows how important information is and why it is so important to protect. Information threats that may harm the interests of the state were also presented. The study also noted that each level of national security is becoming more and more dependent on the free flow of information and on the behavior of information-based systems. Every branch of the economy, for example energy, media, financial and transport systems, etc., is particularly dependent on information systems. They are already key elements of the decision-making process in many civil and military organizations today. It was also emphasized that with the intellectual development and polytechnization of life, information began to gain more and more value. Their possession has become a condition for a better and safer existence. Against this background, competition appeared. Information began to be more and more protected as a material asset.

Keywords: security, diplomacy, economy, information, systems

Wstęp

Skok rozwojowy nauki i techniki na przełomie wieków XX i XXI spowodował ukształtowanie się powszechnego obecnie przekonania, że żyjemy w czasach przełomu cywilizacyjnego. Pierwsze symptomy tego przełomu zauważono w latach 80. XX wieku, a z początkiem lat 90. pojawiły się już bardzo skonkretyzowane pojęcia i inicjatywy "globalnej infrastruktury informacyjnej" i "społeczeństwa informacyjnego". To ostatnie stało się m.in. nowym hasłem politycznym i kierunkiem rozwojowym Unii Europejskiej. Inspiruje ono obecnie rozwijane programy kształtowania badań, rozwoju gospodarki i kultury, kierunkuje liczne pochodne względem tej inicjatywy plany, projekty i przedsięwzięcia realizowane w wielu krajach rozwiniętych i rozwijających się. Bazę techniczną współczesnych rozwiniętych społeczeństw stworzyły takie nauki jak informatyka, telekomunikacja, automatyka oraz integrujące je, szerzej rozumiane techniki informacyjne, przyczyniając się do przyśpieszonych a jednocześnie głębokich przekształceń cywilizacyjnych. Stosuje się także pojęcie "społeczeństwo sieciowe", dla podkreślenia specyfiki współczesnych wielostronnych powiązań i zależności oraz roli współczesnego sposobu komunikacji między poszczególnymi osobami i instytucjami, a także ich szerokiego dostępu do źródeł informacji i wiedzy. Podkreśla się, że stało się to możliwe wskutek skokowego rozwoju sprawnych technik komunikacji elektronicznej, pozwalających na stałe doskonalenie i obniżenie kosztów komunikacji przy pomocy dźwięku i obrazu oraz transmisji danych (ale także wskutek rozwoju innych technik transportowych). Objawiła się znacząca likwidacja bariery przestrzeni i czasu. Szybka globalna multimedialna wymiana informacji umożliwiająca posługiwanie się w skali świata jednoczesnym i jednorodnym przekazem dźwiękowo-wizyjnym, pozwala m.in. ograniczyć w ekonomicznie znaczący sposób podróże związane z wykonywaniem zawodu, ale także ułatwia i upowszechnia np. dostęp do rozrywki. Aplikacje informacyjne, wykorzystujące coraz bardziej zaawansowane możliwości elektronicznego przekazu, mogą być różnorodne i obejmują różne dziedziny. Ograniczeniami w ich stosowaniu mogą być tylko koszty implementacji i użytkowania, gdyż możliwości samej techniki są niezwykle szerokie[1].

Informacja

Dotychczasowe formy rozpowszechniania informacji za pomocą druku w formie książek, gazet i czasopism są zastępowane przez oszczędniejsze w produkcji i łatwiejsze do dystrybucji odpowiedniki elektroniczne. Przekazy telewizyjne uzupełniane są o możliwości zwrotnego oddziaływania abonenta, usługi handlowe i inne mogą być realizowane środkami zdalnymi, po części nawet automatycz-

[1] K. B. Wydro, *Badania nad istotą informacji, jej właściwościami i stosowanymi technikami informacyjnymi – próba systematyzacji w obszarze wiedzy o informacji,* Państwowy Instytut Badawczy, Warszawa 2007, s. 27.

nie, procesy edukacyjne nie wymagają bezpośredniego kontaktu uczących się i uczących, a nadto są wyposażane w nowe rozwiązania ułatwiające naukę. Na tym zasadza się szczególna rola interaktywności, umożliwiającej uczestnikowi procesu komunikacyjnego kształtowanie go stosownie do swoich potrzeb. Ponadto, wszelkie nowe media charakteryzują się tym, że z jednej strony przekraczają granice między technologiami i mediami, z drugiej zaś między komunikowaniem prywatnym i publicznym, gdyż to samo medium może być używane w celach prywatnych i publicznych[2].

Ten przełom informacyjno-komunikacyjny uzyskano dzięki osiągnieciom w dziedzinie mikro- i optoelektroniki, tj. technologii półprzewodników i światłowodów, rozwojowi metod informatyki, automatyki, udoskonaleniu i upowszechnieniu telekomunikacji, w tym opracowaniu różnorodnych technik cyfrowych, metod sterowania opartych o wykorzystanie pojęcia sprzężenia zwrotnego, metod optymalizacji, metod sprawnej, niezawodnej transmisji i dystrybucji informacji. Sukcesy w tych obszarach stworzyły masę krytyczną w postaci praktycznych i tanich rozwiązań technicznych, owocującą właśnie rozległymi i przełomowymi skutkami cywilizacyjnymi. W odniesieniu do sposobów komunikacji ważną nowością, jest wprowadzanie interaktywności, tzn. umożliwienie użytkownikowi aktywnego wyboru zakresu i treści odbieranego przekazu. Dzięki tej możliwości wiele czynności wymagających dotychczas udziału osobistego, przy którym identyfikacja oraz autoryzacja osób je dokonujących była oczywista i naturalna, jest obecnie realizowanych na odległość, za pośrednictwem środków teleinformatycznych. W czynnościach realizowanych osobiście współuczestniczące strony mogą w naturalny sposób dobrać i zaakceptować stopień wymaganej poufności czy wiarogodności (choć nie zawsze znając rzeczywistą wartość tego poziomu). W systemach interaktywnych to zaufanie musi być odnoszone także do sieci komunikacyjnej jako pośrednika. Jej twórcy i operatorzy wprowadzają więc takie środki ochrony informacji, i wiedzę o nich starają się tak upowszechniać, aby uzyskać odpowiednie zaufanie społeczne co do wystarczalności poziomu poufności i zachęcenia do korzystania z ich oferty usługowej.

Można więc stwierdzić, że rozwój mikroelektroniki i optoelektroniki oraz technik przetwarzania informacji jaki objawił się w ostatnich dziesięcioleciach, spowodował daleko idące ułatwienia w operowaniu informacją i jej wymianie (dystrybucji) w skali globalnej. Powstała też niezbędna infrastruktura umożliwiająca przetwarzanie i rozpowszechnianie dużych ilości informacji. Pojawiła się tendencja, a także potrzeba, znacznie intensywniejszego i wszechstronnego wykorzystania informacji, co doprowadziło do obecnego stanu rzeczy[3]:

- Informacja staje się podstawowym i strategicznym zasobem, od którego zależy działanie gospodarki światowej. Jednocześnie pogłębione wykorzystanie informacji dynamizuje rozwój społeczny i kulturalny. Postępująca informatyzacja integruje gospodarki lokalne w połączony organizm i umoż-

[2] Tamże, s.28.
[3] Tamże, s. 25.

liwia dynamiczny rozwój i skuteczne monitorowanie relacji ekonomicznych, społecznych i politycznych.

- Nikną tradycyjne granice organizacji; powstają organizacje ponadnarodowe, postępują wspierane tendencjami liberalizacyjnymi procesy globalizacji zmieniające sposoby działalności gospodarczej, przyśpieszające dystrybucję know-how i innowacji. Rynki realne ewoluują w kierunku rynków elektronicznych wirtualnej wszechobecnej przestrzeni rynkowej umożliwiając np. handel w czasie rzeczywistym. Rozwój mediów i usług wyszukiwania informacji przekształcił operacyjnie światowy system finansowy w niezwykle sprawną i błyskawicznie działającą strukturę.
- Następuje coraz pełniejsza konwergencja technologiczna środków wymiany informacji we wszystkich obszarach jej zastosowania, dzięki stosowaniu wspólnej bazowej platformy, jaką jest technika cyfrowa. Jednocześnie można obserwować konwergencje struktur sieci wymiany informacji, usług informacyjnych, a także symptomy konwergencyjne w obszarze działań legislacyjnych i regulacyjnych, niezbędnych dla poprawnego rozwoju.
- Intensyfikują się procesy zmiany zawodów wiążące się z postępującą dematerializacją przedmiotów pracy wskutek jej wszechstronnej informatyzacji. Powstają także zawody nowe, związane z tworzeniem, budową i obsługa systemów i urządzeń techniki informacyjnej.
- Kształtują się nowe wyzwania intelektualne w związku z rewizją dotychczasowego opisu świata, nieadekwatnego wobec nowych osiągnięć wiedzy wspomaganych technikami informacyjnymi. Charakteryzuje się to odchodzeniem od ujęcia mechanistycznego w kierunku modeli chaotyczno-systemowych, silniej uwzględniających nieliniowości i niestacjonarności procesów.

Łatwość przetwarzania, replikowania, przesyłania i przechowywania informacji powoduje ogromny wzrost jej łącznego wolumenu dostępnego odbiorcom. Zwiększa to trudności w poszukiwaniu i pozyskiwaniu informacji adekwatnej do rzeczywistych potrzeb. Co więcej, kłopot sprawia fakt, że o jej przydatności rzeczywistej trudno przesądzać z góry, tj. jak długo nie zostanie ona użyta a co najmniej przeanalizowana. Dalej łatwość przekształcania prowadzi także do łatwości fałszowania lub tworzenia informacji fikcyjnej, w celu umyślnego wprowadzania w błąd odbiorcy tej informacji w większym lub mniejszym stopniu. Mówi się w tym kontekście o zagrożeniach samego środowiska informacyjnego, ale i możliwości jego szkodliwego oddziaływania na procesy rozwojowe.

Stosownie do łacińskiej etymologii, informare znaczy tyle, co nadawać kształt, formę, natomiast informatio określa już gotowe przedstawienie czegoś, pojęcie. Współcześnie termin ”informacja” jest używany w odniesieniu do wielu nowoczesnych form opisu, związanych ze sposobami komunikowania się i stąd ma wiele definicji. Definicje te są uzależnione od dziedziny w jakiej ”informacja” jest rozpatrywana, klasy problemów, bądź kontekstu użycia, ale także, w ramach tej samej dziedziny bywa różnie definiowana przez różnych autorów, co można stwierdzić studiując bogatą literaturę przedmiotu. Część definicji wywodzi się z prób identy-

fikacji tego, czym jest informacja, na podstawie obserwacji poczynionych na gruncie pojedynczej dziedziny, np. telekomunikacji (elektroniki) czy biologii. Liczne inne mają źródła i inspiracje w bardziej uniwersalnych analizach prowadzonych w obszarach interdyscyplinarnych[4].

Jest rzeczą oczywistą, że definicje bardziej uniwersalne umożliwiają i porządkują badania szersze, ogólniejsze, o charakterze ramowym czy teoretycznym, ale także jak już wspomniano skutkują możliwością przenoszenia wyników osiąganych w jednych dziedzinach na dziedziny inne. Zrozumiała jest więc tendencja poszukiwania jednoznacznej, dostatecznie ogólnej definicji, która byłaby przydatna w sposób możliwie uniwersalny. Poszukiwania te uprawnia pogląd, że w odniesieniu do nadzwyczaj szerokiego spektrum treściowego obiektów zwanych informacją można domniemywać, czy choćby zakładać intuicyjnie, że istnieje jakaś cecha wspólna dla różnie rozumianych pojęć "informacja", będąca substancją zasadniczą opisywanego tą nazwą zjawiska i, że analizy dotyczące istoty informacji w poszczególnych dziedzinach dotyczą tylko pewnych fragmentarycznych cech tej substancji. Wobec tego zasadne i celowe jest dążenie do wyodrębnienia tej substancji, tj. sedna "informacji" i stąd obserwuje się bogactwo prac w tym przedmiocie, podejmowanych w różnorodnych dziedzinach, a zmierzających do poprawnego zdefiniowania informacji[5].

Systemy Bezpieczeństwa

W Słowniku terminów z zakresu bezpieczeństwa narodowego zdefiniowano system bezpieczeństwa państwa (SBP) jako skoordynowany wewnętrznie zbiór elementów organizacyjnych, ludzkich i materiałowych, ukierunkowanych na przeciwdziałanie wszelkim zagrożeniom państwa, a w szczególności politycznym, gospodarczym, psychospołecznym, ekologicznym i militarnym1 . W definicji tej wyraźnie wskazano na warstwę podmiotową pochodzenia zagrożeń bezpieczeństwa państwa. Na uwagę zasługuje tu kolejność wymienianych zagrożeń bezpieczeństwa państwa zgodnie z postrzeganiem aspektów współczesnego bezpieczeństwa Polski – zagrożenia militarne zostały wymienione jako ostatnie, a zdecydowanie większy wymiar gatunkowy nadano aspektom politycznym, gospodarczym, psychospołecznym czy ekologicznym. Za punkt wyjścia do zdefiniowania systemu bezpieczeństwa państwa można przyjąć określony poziom zapewnienia tego bezpieczeństwa. Przy czym trzeba mieć świadomość, że o stanie idealnego bezpieczeństwa państwa można rozważać jedynie teoretycznie, gdyż pomimo nawet chwilowego uzyskania stanu braku zagrożeń nie można wykluczyć możliwości pojawienia się nowych. Ich źródłem bowiem są różnego rodzaju sprzeczności interesów między ludzkich. Zagrożenia stanowią splot destrukcyjnych zdarzeń i burzą ustalony ład oraz porządek państwa. Dlatego też te dwie kategorie: „bez-

[4] M. Grabowski, A. Zając, *Dane, informacja, wiedza – próba definicji,* [w:] Zeszyty Naukowe UE w Krakowie nr 798/2009, s.99-116.

[5] Tamże, s.101.

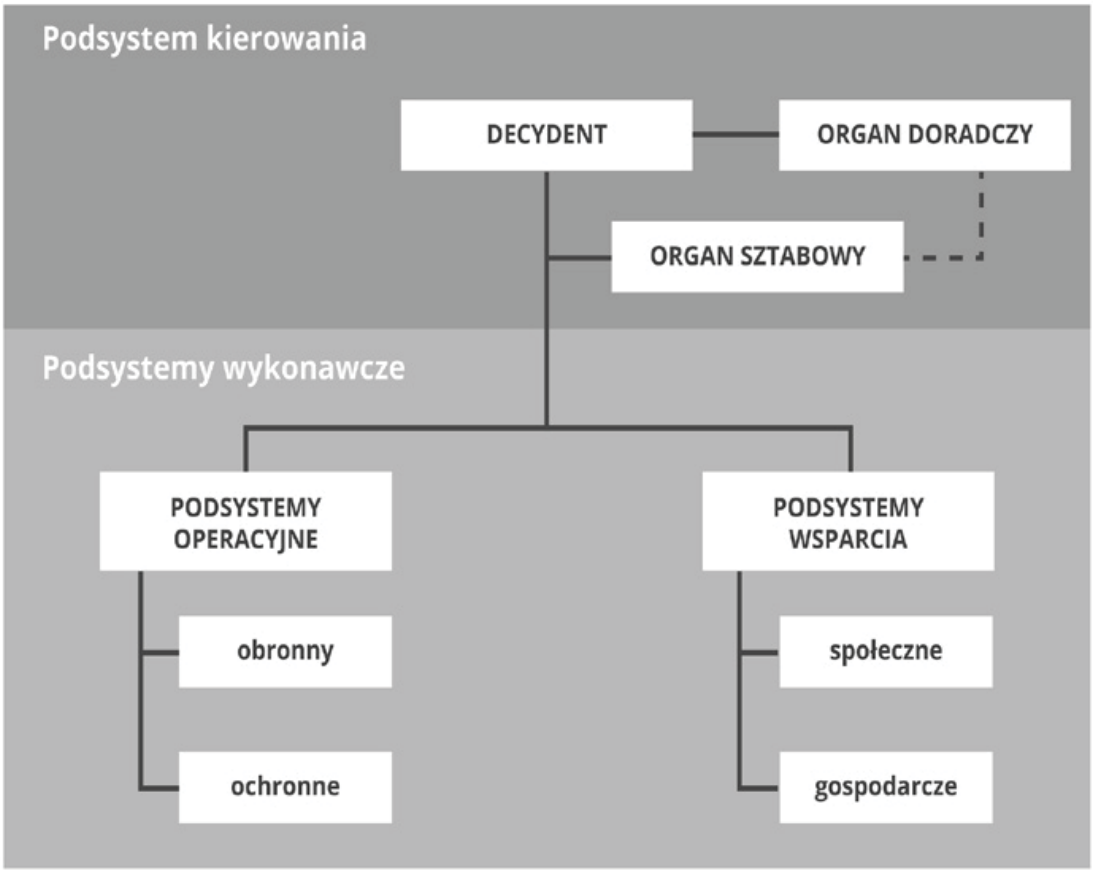
pieczeństwo" i „zagrożenie" są ze sobą ściśle skorelowane poprzez działalność ludzką, która z jednej strony, dąży do ograniczenia istniejących zagrożeń, z drugiej strony zaś wyzwala wciąż nowe. Ujmując kompleksowo problem zapewnienia bezpieczeństwa państwa, można przyjąć, że system bezpieczeństwa państwa to zbiór wzajemnie powiązanych elementów (ludzi, organizacji, urządzeń) wydzielonych w celu zapewnienia bezpieczeństwa państwa, tzn. zapewnienia nienaruszalności terytorialnej oraz stworzenia warunków do swobodnego i stabilnego rozwoju państwa we wszystkich sferach jego działalności. Tak rozumiany system bezpieczeństwa państwa ma z jednej strony gwarantować stabilność bytu narodu w trwałych granicach państwa, a z drugiej przeciw działać wszelakim zagrożeniom mogącym ograniczać lub uniemożliwiać swobodny i stabilny rozwój w dziedzinach życia społecznego. Przy czym funkcjonowanie całego systemu musi odznaczać się wysoką sprawnością (skutecznością) we wszystkich dziedzinach działania, a zatem musi być to system integrujący wszystkie siły i środki w ramach jednej, sprawnie zarządzanej struktury.

W opublikowanej w 2013 r. przez Biuro Bezpieczeństwa Narodowego (BBN) Białej księdze bezpieczeństwa narodowego Rzeczypospolitej Polskiej system bezpieczeństwa narodowego (bezpieczeństwa państwa) został zdefiniowany jako całość sił (podmiotów), środków i zasobów przeznaczonych przez państwo do realizacji zadań w dziedzinie bezpieczeństwa, odpowiednio do tych zadań zorganizowana (w podsystemy i ogniwa), utrzymywana i przygotowywana(patrz schemat nr 1.).

Podsystem kierowania jest kluczowym elementem systemu bezpieczeństwa narodowego. Stanowi on część systemu bezpieczeństwa narodowego przeznaczoną do kierowania jego funkcjonowaniem, obejmującą organy władzy publicznej i kierowników jednostek organizacyjnych, które wykonują zadania związane z bezpieczeństwem narodowym (w tym organy dowodzenia Sił Zbrojnych RP), wraz z organami doradczymi i aparatem administracyjnym (sztabowym) oraz procedurami funkcjonowania i infrastrukturą (stanowiska i centra kierowania oraz zarządzania, system łączności). Ma on żywotne znaczenie dla całego systemu bezpieczeństwa w czasie pokoju, kryzysu i wojny. Zapewnia uzyskiwanie wiedzy o zagrożeniach i ich analizę, planowanie przygotowania i działania podsystemów operacyjnych i wsparcia oraz zarządzanie (dowodzenie) nimi w trakcie działań[6].

Można wyodrębnić cztery strategiczne obszary zadaniowe podsystemu kierowania. Pierwszym jest monitorowanie zagrożeń, z uwzględnieniem ich skali, rodzaju i miejsca występowania. Drugi dotyczy zapobiegania powstawaniu zagrożeń, zarówno na terytorium kraju, jak i poza jego granicami. Trzeci obejmuje działania związane z usuwaniem skutków zagrożeń, gdy nie udało się im zapobiec. Ostatni obszar obejmuje kierowanie obroną państwa w razie bezpośredniej agresji militarnej. Dla realizacji tych zadań konieczne są odpowiednie warunki planistyczne, organizacyjne, finansowe czy techniczne. Ich zapewnieniu służą ure-

[6] http://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/system-bezpieczenstwa-n/kierowanie-bezpieczenst/5975,Kierowa nie-bezpieczenstwem-narodowym.html. [dostęp 20.10.2020]



Schemat nr 1. Uniwersalny model systemu bezpieczeństwa narodowego
Źródło: https://www.Epodreczniki.Pl/reader/c/141459/v/latest/t/student-canon/m/iizmgwteov#iizmgwteov_d5e295 [dostęp 20.10.2020]

gulowania prawne, dotyczące podwyższania gotowości obronnej państwa oraz przygotowania systemu stanowisk kierowania dla poszczególnych organów administracji publicznej, w tym Centralnego Stanowiska Kierowania Obroną Państwa.

Podsystemy (w tym ogniwa) wykonawcze systemu bezpieczeństwa narodowego (bezpieczeństwa państwa) to siły i środki przewidziane do realizacji ustawowo określonych zadań w dziedzinie bezpieczeństwa, pozostające w dyspozycji organów kierowania bezpieczeństwem. Wyróżnia się ich dwa rodzaje: operacyjne oraz wsparcia.

Podsystemy operacyjne tworzą: podsystem obronny państwa (obronności, obrony narodowej, bezpieczeństwa militarnego) – przeznaczony do wykorzystywania szans, podejmowania wyzwań, redukowania ryzyk i przeciwdziałania (zapobiegania i przeciwstawiania się) zewnętrznym zagrożeniom o charakterze polityczno-militarnym – oraz podsystemy ochronne państwa i ludności (bezpieczeństwa cywilnego, pozamilitarnego) – przeznaczone do wykorzystywania szans, podejmowania wyzwań, redukowania ryzyk i przeciwdziałania (zapobiegania i przeciwstawiania się) zewnętrznym i wewnętrznym zagrożeniom o charakterze niemilitarnym (cywilnym).

Podsystemy wsparcia to podmioty społeczne i gospodarcze przeznaczone do wykorzystywania szans, podejmowania wyzwań, redukowania ryzyk i przeciwdziałania (zapobiegania i przeciwstawiania się) zewnętrznym i wewnętrznym zagrożeniom o charakterze społecznym i gospodarczym, a także do społecznego i gospodarczego zasilania operacyjnych podsystemów bezpieczeństwa narodowego w czasie pokoju, kryzysu i wojny[7].

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. A symetryzacji 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[8].

W konflikcie tym nie występuje termin „pole walki", działania odbywają się w rozproszeniu, bez zachowania ciągłości geograficznej i chronologicznej. 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 metod14 . Kolejną cechą konfliktu asymetrycznego jest łatwość jego prowadzenia. Internet i telefonia komórkowa umożliwiają błyskawiczną komunikację oraz anonimowość . Siły prowadzące konflikt są rozproszone, dlatego atak odwetowy raczej nie odniesie skutku, ponadto druga strona powstrzymuje się przed uderze-

[7] Tamże

[8] G. Nowacki, , *Znaczenie informacji w obszarze bezpieczeństwa narodowego,* [w:] Nierówności Społeczne a Wzrost Gospodarczy nr 36/2013, Warszawa 2013, s. 107-123.

niem odwetowym, obawiając się skutków politycznych i społecznych zdecydowanej akcji militarnej[9].

Zagrożenia dla bezpieczeństwa informacyjnego RP:

Wymiar wewnętrzny zagrożeń:

1. Zagrożeniem płynącym z funkcjonowania w środowisku informacyjnym może być rozpowszechnianie i powielanie treści propagandowych mające na celu ukazanie polskiej racji stanu w negatywnym świetle, co de facto szkodzi interesowi państwa (stosowanie prowokacji, celowe manipulowanie przekazem poprzez wyrywanie z kontekstu fragmentów wypowiedzi polityków RP, nadawanie im kontrowersyjnego charakteru).
2. Do najpoważniejszych zagrożeń związanych z niedoskonałym funkcjonowaniem społeczeństwa obywatelskiego należy zaliczyć:
   a. występowanie w społeczeństwie deficytów informacyjnych, skutkujących podatnością na wrogą perswazję;
   b. potencjalna dezinformacja obywateli poprzez agresywne działania propagandowe; dywersja ideologiczna – narzucanie obcych idei niezgodnych z interesem państwa;
   c. pojawienie się i rozwój postaw antypaństwowych; nasilenie się postaw agresywnych, defetystycznych (np. islamofobia, szpiegomania);
   d. wzrost negatywnych postaw społecznych lub wystąpienie konfliktów społecznych, zgodnych z intencjami przeciwnika informacyjnego (informacyjnego napastnika);
   e. istnienie (tworzenie) agentury wpływu (inspirowanie do zakładania oraz wsparcie finansowe formacji politycznych lub organizacji społecznych wspierających i realizujących obce interesy w Polsce);
   f. wpływanie na opinię publiczną przez agentów zmiany sterowanych z zewnątrz, zwłaszcza aktywizacja wybranych grup społecznych przez inne państwo oraz realizacja interesów obcych państw, sprzecznych z interesem RP;
   g. obniżanie się morale społeczeństwa w razie agresji informacyjno-propagandowej, rzutujące negatywnie na polityczno-militarne procesy decyzyjne.
3. Do zagrożeń informacyjnych związanych z funkcjonowaniem w cyberprzestrzeni należą:
   a. dezinformacja, wroga propaganda, zakłócające realizację istotnych zadań administracji publicznej oraz sektora prywatnego;
   b. ataki powodujące zakłócenia funkcjonowania sieci teleinformatycznych w sektorach i instytucjach o podwyższonym stopniu wrażliwości, w tym tworzących infrastrukturę krytyczną;
   c. istnienie technologicznych luk, które dają szansę, także niezauważonej, ingerencji w treści portali internetowych oraz wpływania na zdolności do działania w cyberprzestrzeni.

[9] Tamże

4. Odrębnym obszarem występowania potencjalnych zagrożeń jest przestrzeń medialna:
   a. monopolizacja rynku informacyjnego i jego poszczególnych struktur oraz niekontrolowany rozwój rynku informacyjnego media masowe mogą być narzędziem dezinformacji;
   b. przejmowanie lub finansowanie mediów przez podmioty nieprzychylne lub wrogie Polsce;
   c. pojawienie się w przestrzeni informacyjnej mediów propagujących idee sprzeczne z interesem narodowym;
   d. aktywne uczestnictwo przeciwnika w polskich mediach społecznościowych – propagowanie idei sprzecznych z interesem narodowym;
   e. nieświadome, niezamierzone powielanie przekazu informacyjnego sprzecznego z interesem narodowym przez użytkowników mediów społecznościowych lub media masowe.

Wymiar zewnętrzny zagrożeń:

1. Wśród podstawowych zagrożeń w obszarze bezpieczeństwa informacyjnego państwa należy wskazać takie jak:
   a. deformowanie treści oraz wprowadzanie do systemów informacyjnych nieprawdziwych treści logicznych za pośrednictwem kanałów łączności rządowej czy wojskowych systemów dowodzenia;
   b. działalność służb specjalnych i podmiotów informacyjnych innych państw oraz aktorów niepaństwowych (w tym szpiegostwo);
   c. wroga aktywność operacyjna struktur informacyjno-propagandowych aktorów państwowych i pozapaństwowych;
   d. działania propagandowe i dezinformacyjne;
   e. dominacja potencjalnych agresorów w środowisku informacyjnym;
   f. penetracja środowiska informacyjnego RP przez wrogie struktury informacyjnopropagandowe;
   g. utrata zdolności wpływania, dystrybucji informacji w środowisku informacyjnym.
2. Poważnym zagrożeniem są niepożądane, zewnętrzne oddziaływania informacyjne, mogące dotyczyć procedur sterowania procesami decyzyjnymi państwa, na które ukierunkowany jest atak informacyjny.
3. Skutkować to może bezpośrednim przełożeniem na koncepcje doktrynalne odnoszące się do infrastruktury wojskowej, systemów kierowania państwem i dowodzenia siłami zbrojnymi, a także szeroko rozumianych operacji informacyjnych.
4. Wśród najpoważniejszych zagrożeń związanych z niedoskonałym funkcjonowaniem społeczeństwa obywatelskiego należy zaliczyć:
   a. inspirowane z zewnętrz działania informacyjne podmiotów wewnętrznych mające na celu wywoływanie i pogłębianie podziałów społecznych i politycznych;
   b. wsparcie zewnętrzne dla podmiotów realizujących politykę przeciwnika;

c. dezinformacja obywateli innych państw, w tym tworzących wspólnoty organizacyjne w kwestiach dotyczących polskiej polityki zagranicznej.

5. W związku z funkcjonowaniem RP w globalnej cyberprzestrzeni mogą pojawić się zagrożenia w postaci ataków cybernetycznych na instytucje rządowe, pozarządowe i kulturalne kształtujące świadomość narodową lub blokady rządowego przekazu informacyjnego wskutek ataków cybernetycznych.[10]

Informacyjny wymiar bezpieczeństwa

Przez praktyków, bardzo często bezpieczeństwo informacyjne rozumiane jest jako ochrona informacji przed niepożądanym (przypadkowym lub świadomym) ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania. środki bezpieczeństwa podejmowane są w celu zapewnienia poufności, integralności i dostępności informacji. Ich celem jest wyeliminowanie zagrożenia dla informacji. Wskazuje to, że przytoczona wyżej definicja bezpieczeństwa informacyjnego sformułowana została w ujęciu negatywnym. W miarę intelektualnego rozwoju i politechnizacji życia informacje zaczęły nabierać coraz większych wartości. Ich posiadanie stało się warunkiem lepszej i bezpieczniejszej egzystencji. Na tym też tle pojawiła się konkurencja. Informacje zaczęto coraz bar-dziej chronić jako dobro materialne. Chęć stworzenia sobie podobnych do innych lub lepszych Przez praktyków, bardzo często bezpieczeństwo informacyjne rozumiane jest jako ochrona informacji przed niepożądanym (przypadkowym lub świadomym) ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania. środki bezpieczeństwa podejmowane są w celu zapewnienia poufności, integralności i dostępności informacji. Ich celem jest wyeliminowanie zagrożenia dla informacji. Wskazuje to, że przytoczona wyżej definicja bezpieczeństwa informacyjnego sformułowana została w ujęciu negatywnym. W miarę intelektualnego rozwoju i politechnizacji życia informacje zaczęły nabierać coraz większych wartości. Ich posiadanie stało się warunkiem lepszej i bezpieczniejszej egzystencji. Na tym też tle pojawiła się konkurencja. Informacje zaczęto coraz bar-dziej chronić jako dobro materialne. Chęć stworzenia sobie podobnych do innych lub lepszych warunków życia stworzyła potrzebę zdobywania informacji. Zrodził się zatem swoisty rodzaj walki – jedni, możliwymi dla siebie sposobami, dążą do zdobycia informacji, a drudzy z podobnym zaangażowaniem starają się im to udaremnić. W postępowaniu takim występuje sprzeczność celów i działań, czyli najbardziej dystynktywnych cech, które kojarzą się z desygnatem pojęcia ,,walka". Można by powiedzieć, że przedmiotem tej walki stała się informacja, a narzędziami – wszelkie środki dostosowane do jej zdobywania, zakłócania i obrony. Walka taka nazywana jest walką informacyjną.[11]

[10] *Doktryna bezpieczeństwa informacyjnego RP, Biuro Bezpieczeństwa Narodowego,* 24 lipca 2015 r.
[11] http://www.liedel.pl/?p=13[dostęp 20.10.2020]

Wobec wzrostu znaczenia informacji ujęcie negatywne bezpieczeństwa informacyjnego jest niewystarczające dla zapewnienia bezpieczeństwa narodowego. Każda płaszczyzna bezpieczeństwa narodowego staje się coraz bardziej zależna od swobodnego przepływu informacji i od zachowania systemów bazujących na informacjach. Wojsko, gospodarka, energetyka, media, systemy finansowe i transportowe są szczególnie uzależnione od systemów informatycznych. Już dziś stanowią one kluczowe elementy procesu podejmowania decyzji w wielu organizacjach cywilnych i wojskowych. Ich dotychczasowy rozwój i zakresy wdrożeń pozwalają prognozować, że obszary zastosowań informatycznych będą obejmować coraz większe przestrzenie funkcjonalne. Teoretycznie został stworzony niemalże nieograniczony dostęp do ogromnych zbiorów informacji, a w tym: finansowych, przemysłowych, marketingowych, technologicznych, wojskowych i innych. Niezbędne dla bezpieczeństwa państwa staje się wprowadzenie polityki bezpieczeństwa informacyjnego zapewniającej ochronę istniejących systemów, ale również gwarantującej państwu i podmiotom, które chroni, posiadanie, przetrwanie i swobodę rozwoju „społeczeństwa informacyjnego". [12]

Takie ujęcie bezpieczeństwa informacyjnego ma charakter pozytywny. Środki polityki bezpieczeństwa informacyjnego budowane w oparciu o ujęcie pozytywne muszą uwzględniać, że:

- informacja stanowi zasób strategiczny państw i organizacji XXI wieku;
- informacja i wynikająca z niej wiedza oraz technologie informatyczne staną się podstawowym czynnikiem wytwórczym;
- większość dochodu państwa zostanie uzyskana z szeroko rozumianego sektora informacyjnego;
- procesy decyzyjne w innych sektorach gospodarki i życia społecznego uzależnione będą od systemów przetwarzania i przesyłania informacji;
- zakłócenie prawidłowości działania systemów informacyjno – sterujących nie wymaga wysokich nakładów materialnych;
- rywalizacja pomiędzy przeciwnikami przeniesie się na płaszczyznę walki informacyjnej.

Potrzebę wypracowania skutecznych środków polityki bezpieczeństwa informacyjnego wymusza wzrastająca informatyzacja sił zbrojnych, zwiększające się ciągle możliwości systemów łączności, ze wzrastającym nasyceniem wojsk nowymi technikami walki w tym szczególnie bronią precyzyjnego rażenia. Jak widać, zarówno na Zachodzie jak i Wschodzie współczesna walka informacyjna najbardziej łączona jest z walką zbrojną. Wyrażane są nawet poglądy z czym trzeba się zgodzić że w przyszłości ta forma zmagań stać się może ekwiwalentem innych rodzajów walk, w tym i walki zbrojnej. Można więc przewidywać, że obserwowany w tym zakresie wyścig może doprowadzić w przyszłości do tego, że walka informacyjna stanie się nawet substytutem wojny. Umiejętnie prowadzona jest z pew-

[12] Tamże

nością w stanie naruszać szeroko rozumiane proporcje strategiczne i kształtować sceny polityczne, tak w aspekcie międzynarodowym, jak i wewnętrznym.[13]

Współczesność wchłonęła też w sferę walki informacyjnej media, które w sposób dla siebie nieświadomy mogą być wykorzystywane przez przeciwnika jako narzędzia skutecznego zakłócania informacyjnego. Szczególnie dogodne do tego warunki istnieją w państwach demokratycznych, gdzie wolna prasa, goniąc za sensacjami dnia codziennego, jest niezwykle podatna na dezinformowanie i błyskawiczne rozprzestrzenianie wszelkich informacji, które mogą przynosić korzyści określonemu przeciwnikowi. Z tych samych powodów może stać się niepostrzeżenie źródłem upływności informacyjnej. Współczesne środki walki informacyjnej są dostosowane do zdobywania informacji przeróżnymi metodami i technikami. Nawet wśród zaprzyjaźnionych państw trwa w tym zakresie ciągła konkurencja i sądzić należy, że nigdy nie zostanie zaniechana. Uzyskana w tym zakresie przewaga spełniać może nie tylko funkcje wspomagające walkę zbrojną, ale może również spełniać funkcje odstraszania przez unaocznianie przeciwnikowi braku realnych perspektyw do osiągnięcia łatwych korzyści. Już dziś bardzo skutecznymi środkami walki informacyjnej stać się mogą wszystkie te, które dostosowane są do zdalnego wprowadzania wirusów komputerowych do sieci informacyjnych, dostosowanych programowo do samopowielania się i szybkiego rozprzestrzeniania. Ogromne znaczenie mogą mieć również tak zwane bomby logiczne, które jako odpowiednio opracowane aplikacje programowe, będą dostosowane do uaktywniania się na określone wcześniej sygnały lub według zaprogramowanych reżimów czasowych. Skutecznym przedsięwzięciem może być także blokowanie wymiany informacji i szerzenie dezinformacji w torach transmisyjnych za nieświadomym pośrednictwem środków masowego przekazu. Współczesne narzędzia walki informacyjnej stwarzają możliwości podejmowania skutecznej działalności ukierunkowanej na sterowanie procesami decyzyjnymi przeciwnika, nawet w skali państwowej. Wprowadzenie do publicznego i utajonego systemu informacyjnego danego państwa złożonych zbiorów precyzyjnie dobranych prawdziwych i sfałszowanych danych może tworzyć z góry zaplanowane nastroje społeczne i klimat polityczny, które w efekcie spowodują podejmowanie decyzji zgodnych z oczekiwaniami sprawcy tych manipulacji. Współczesne środki walki informacyjnej wskazują, jak nigdy dotąd, na konieczność uwzględniania tego problemu nie tylko w programach reformowania sił zbrojnych, ale również i w funkcjonowaniu państwa. Potrzeba taka wynika chociażby z tego, że ich użycie jest możliwe nie tylko w okresie zagrożenia i wojny. Już w okresie pokoju mogą być podejmowane w tym zakresie dobrze zamaskowane wysiłki ukierunkowane nie tylko na zdobywanie informacji, ale również na powodowanie niepokojów, zamieszek i kryzysów rządowych, co w atmosferze ciągle trwającej globalnej konkurencji wydaje się być bardzo realne. Nie można też wykluczyć, że w ramach tego mogą być stosowane różnego rodzaju akty terrorystyczne sterowane przez jakieś państwo. Ta forma przemocy może być prowadzona chociażby siłami służb specjalnych, o których

[13] Tamże

wiadomo, że są stale na całym świecie doskonalone i rozwijane. Może to nawet stanowić ekwiwalent otwartych agresji, co z coraz większą intensywnością daje się obserwować już teraz.

Podsumowanie

Wysiłki walki informacyjnej mogą być ukierunkowane na podrywanie autorytetu zaatakowanego państwa na arenie międzynarodowej, czy też podrywanie jego zaufania sojuszniczego. W szerokim zakresie może być włączana do tego dyplomacja, handel zagraniczny i media. Na oddziaływanie takie szczególnie jest podatna sfera ekonomiczna, polityczna, polityczna i społeczna. W działaniach tych mogą być również prowokowane incydenty międzypaństwowe, powodujące napięcia społeczne w stosunkach dobrosąsiedzkich. Każdy ma jakieś sekrety, skrzętnie ukrywane przed otoczeniem, i każdy też chciałby posiąść informacje o warunkach najlepszej egzystencji w określonym otoczeniu. Przy większych strukturach organizacyjnych zbiory tajemnic i zapotrzebowań na informacje rozrastają się. W przypadku państwa czy koalicji liczba elementarnych postaci tajemnic i zapotrzebowań na informacje jest przeogromna i znaczeniowo niezmiernie złożona. Z tego też względu dbałość o bezpieczne warunki egzystencji państwa wiąże się nierozerwalnie z potrzebą ciągłego rozpoznawania otoczenia i bronienia dostępu do własnych tajemnic.[14]

Literatura:

1. Koziej S., Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja
2. Ptak M., Współczesne rozumienie bezpieczeństwa, zagrożeń i obronności, Zeszyty Naukowe WSOWL, Nr I (155), 2010
3. A. Jóźwiak, Znaczenie telekomunikacji i teleinformatyki w systemie bezpieczeństwa państwa
4. G. Nowacki, Znaczenie informacji w obszarze bezpieczeństwa narodowego, Wojskowa Akademia Techniczna, Warszawa
5. L. Więcaszek-Kuczyńska, Zagrożenia bezpieczeństwa informacyjnego, Obronność zeszyty naukowe NR 2 (10) 2014
6. Doktryna bezpieczeństwa informacyjnego RP, Biuro Bezpieczeństwa Narodowego, 24 lipca 2015 r.
7. K. B. Wydro, Badania nad istotą informacji, jej właściwościami i stosowanymi technikami informacyjnymi – próba systematyzacji w obszarze wiedzy o informacji, Państwowy Instytut Badawczy, Warszawa 2009.

Netografia:

8. http://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/system-bezpieczenstwa-n/kierowanie-bezpieczenst/5975,Kierowa nie-bezpieczenstwem-narodowym.html
9. http://www.liedel.pl/?p=13

[14] http://www.liedel.pl/?p=13.[dostęp 20.10.2020]