dr Radosław Chodkowski
Akademia Sztuki Wojennej, Warszawa
ORCID: 0000-0003-2425-8295

https://doi.org/10.29316/9788368103243_4

MILITARNE ASPEKTY BEZPIECZEŃSTWA INFORMACYJNEGO

MILITARY ASPECTS OF INFORMATION SECURITY

Streszczenie

Zapewnienie bezpieczeństwa informacyjnego to niezwykle złożony, wielowymiarowy proces, który opiera się na różnorodnych mechanizmach zarówno społecznych, psychicznych, jak i technicznych. Ta złożoność czyni go podatnym na zakłócenia. Wielość zagrożeń występujących w infosferze powoduje, że zapewnienie bezpieczeństwa informacyjnego na zadowalającym poziome jest wielkim wyzwaniem. Wyzwanie to staje się jeszcze większe, kiedy zapewnienie bezpieczeństwa informacyjnego dotyczy sił zbrojnych. Wynika to z faktu, że ich, tak bardzo zależne od informacji, działanie bardzo często ma wpływ na sprawy najwyższej wagi dla państwa, społeczeństwa, ale także bezpośredni wpływ na utratę bądź zachowanie życia ludzi. Doświadczenia konfliktów zbrojnych, które w ostatnich latach toczyły się, bądź ciągle się toczą, pokazują, że informacja, jak nigdy dotąd, nie tylko jest niezbędna do skutecznego prowadzenia walki, ale stanowi bardzo istotne narzędzie oddziaływania zarówno na przeciwnika, jak i na środowiska nie będące bezpośrednio stroną konfliktu, ale mające na niego realny wpływ. W poniższym opracowaniu autor, wykorzystując analizę dostępnego materiału źródłowego, dążył będzie do uzyskania odpowiedzi na pytania: 1) Jak, w kontekście współczesnych warunków środowiskowych, można zdefiniować bezpieczeństwo informacyjne? 2) Jakie czynniki determinują bezpieczeństwo informacyjne w siłach zbrojnych?

Słowa kluczowe: bezpieczeństwo informacyjne, walka informacyjna, potrzeby informacyjne, infosferera

Abstract

Ensuring information security is an extremely complex, multidimensional process that relies on diverse social, psychological, and technical mechanisms. This complexity makes it vulnerable to disruption. The multitude of threats present in the infosphere renders the assurance of information security at a satisfactory level a major challenge. This challenge becomes even greater when information security concerns the armed forces. This stems from the fact that their activities, so heavily dependent on information, often affect matters of the utmost importance to the state and society, as well as having a direct impact on the loss or preservation of human life. The experiences of armed conflicts that have taken place in recent years, or are still ongoing, demonstrate that information, more than ever before, is not only indispensable for the effective conduct of combat but also constitutes a highly significant tool of influence, both on the adversary and on environments not directly engaged in the conflict yet exerting a real impact on its course. In this study, the author, through an analysis of the available source material, seeks to provide answers to the following questions: 1) How, in the context of contemporary environmental conditions, can information security be defined? 2) What factors determine information security within the armed forces?

Keywords: information security, information warfare, information needs, infosphere

Wstęp

Jak wielką rolę odgrywa informacja w życiu codziennym pokazuje poniższy cytat: „Pojęcie informacji jest jednym z podstawowych terminów, jakimi stykamy się w trakcie codziennego funkcjonowania, zarówno w sferze osobistej, jak i zawodowej. Informacja towarzyszy nam właściwie zawsze – w każdym miejscu, w każdej sytuacji. Trudno sobie we współczesnym świecie wyobrazić funkcjonowanie bez swobodnego dostępu do informacji. Obecnie nie ma dziedziny życia, w której można byłoby pozwolić sobie na zignorowanie jej znaczenia. Należy pamiętać, że im więcej źródeł danych jest dla nas ogólnie dostępnych (…) tym większą uzyskujemy przewagę zarówno na poziomie intelektualnym, jak i np. zawodowym”[1]. Jak wynika z powyższego, zarówno

[1] M. Jakubowska, *Informacja i jej bezpieczeństwo – wybrane zagadnienia*, [w:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, red. M. Górka, Difin, Warszawa 2014, s. 15.

jednostki jak i organizacje potrzebują informacji do sprawnego funkcjonowania. Szczególnym rodzajem organizacji, której funkcjonowanie zależne jest od informacji są siły zbrojne. Wyjątkowość ta wynika z faktu, iż sukces lub porażka sił zbrojnych decyduje nie tylko o osiągnięciu lub nie celów biznesowych czy politycznych, ale także niejednokrotnie o zachowaniu lub utracie ludzkiego życia. W takim kontekście zapewnienie bezpieczeństwa informacyjnego a w nim zaspokojenie potrzeb informacyjnych jawi się jako kluczowe.

Należy rozważyć także jakie warunki muszą zostać spełnione, aby można było stwierdzić, że potrzeba taka jest zaspokajana. „Zaspokajana", a nie „zaspokojona", ponieważ zaspokajanie potrzeb informacyjnych nie jest aktem jednorazowym. Jest to raczej nieprzerwany proces, który ma na celu zapewnienie nieprzerwanego dostępu do informacji. Tym samym pojawia się tu jeden z warunków zapewnienia bezpieczeństwa informacyjnego – niezakłócony dostęp: do informacji. Nie może to być dostęp: do jakiejkolwiek informacji, bo w takim przypadku nieograniczony dostęp: do Internetu, biblioteki czy jakiegokolwiek innego źródła informacji można by uznać za zapewnienie bezpieczeństwa informacyjnego. Oczywiście nie jest to prawdą, ponieważ nie każda informacja zaspokaja potrzeby informacyjne. Żeby informacja mogła służyć do zapewnienia potrzeb informacyjnych powinna spełniać kilka warunków. Taka informacja powinna być przede wszystkim w odpowiedniej formie, tak aby można było ją wykorzystać. Informacja podana w formie niemożliwej do odczytania np. z uwagi na nieznajomość języka, brak odpowiednich urządzeń do jej odczytania (odkodowania) itd. powoduje, że pomimo posiadania informacji będzie ona nieczytelna, a zatem bezużyteczna z punktu widzenia zaspokajania potrzeb informacyjnych.

Bezpieczeństwo informacyjne

Zdefiniowanie bezpieczeństwa informacyjnego nie jest zadaniem łatwym, choćby z uwagi na fakt, że wraz z rozwojem społeczeństwa informacyjnego zmianom ulegały zarówno technologie informacyjne jak również ilość i zakres przetwarzanych informacji.

Niemniej jednak, niezależnie od obserwowanych zmian, można wyróżnić kilka obszarów wspólnych i uniwersalnych dla zapewnienia bezpieczeństwa informacyjnego, niezależnie od charakterystyki podmiotu, którego ono dotyczy.

Zbieżności te można zauważyć w prezentowanych poniżej poglądach różnych autorów. Wynika z nich, np. że bezpieczeństwo informacyjne dotyczy szerokiego zakresu elementów, daleko wykraczających poza zapewnienie tylko bezpieczeństwa posiadanej już informacji.

W ujęciu prezentowanym przez J. Antczaka i A. Nowaka „(…) bezpieczeństwo informacyjne dotyczy:

- samej informacji, jej specyficznej postaci, często nieuchwytnej dla wielu osób (można zostać okradzionym nie będąc tego świadomym!),
- systemów, w których jest ona wytwarzana, przetwarzana, przechowywana i przekazywana,
- środowiska, w którym systemy działają (każdy szczegół dotyczący pomieszczenia, kablowania czy zasilania może okazać się decydujący w skutkach),
- personelu, który korzysta z tych systemów i który często bywa niedouczony, nieobliczalny w swoich działaniach i trudny do skontrolowania,
- całego otocznia prawnego, które dopiero się kształtuje, próbując iść krok w krok za rozwojem technologii z różnym skutkiem”[2].

Podobnie bezpieczeństwo informacyjne przedstawia K. Liderman, którego zdaniem ww. bezpieczeństwo „(…) obejmuje wszystkie formy (także werbalne) wymiany, przechowywania i przetwarzania informacji (…)”[3] i dotyczy „(…) podmiotu (człowieka lun organizacji), który może być zagrożony utratą zasobów informacyjnych lub otrzymaniem informacji złej jakości. Zatem bezpieczeństwo informacyjne oznacza uzasadnione zaufanie podmiotu do jakości i dostępności pozyskanej oraz wykorzystanej informacji”[4]. Daje się tu zauważyć, iż w prezentowanym podejściu do bezpieczeństwa informacyjnego został dodany element związany z zagrożeniem otrzymywania informacji złej jakości. W kontekście zabezpieczenia potrzeb informacyjnych sił zbrojnych powyższe pokazuje, że mogą one zostać narażone na otrzymywanie informacji, która celowo została zmieniona (pozbawiona jakości) tak, aby wywrzeć zamierzony przez podmiot celowo wpływający na jakość informacji, efekt. Zbliżony do powyższego pogląd prezentuje również P. Dela. Opisując bezpieczeństwo

[2] J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne. Wybrane problemy*, Akademia Obrony Narodowej, Warszawa 2013, s. 19.

[3] K. Liderman, *Bezpieczeństwo informacyjne. Nowe wyzwania*, Wydawnictwo Naukowe PWN, Warszawa 2012, s. 22.

[4] Tamże.

informacyjne zaznacza on, że wykracza ono „(…) poza ramy obowiązujących norm. Informacja, funkcjonująca w przestrzeni informacyjnej stała się narzędziem i środkiem realizacji przyjętych celów działania. W bezpieczeństwie informacyjnym, oprócz zapewnienia bezpieczeństwa informacji, niezwykle istotne jest stosowanie elementów walki informacyjnej z elementami dezinformacji i propagandy. Jej umiejętne wykorzystanie pozwala nie tylko na działanie z pozycji dodatniej w stosunku do potencjalnych adwersarzy, ale także pozwala kreować rzeczywistość stawiającą dowolny podmiot bezpieczeństwa zarówno w korzystnym, jak i niekorzystnym świetle. Co więcej, każdy podmiot bezpieczeństwa musi być równocześnie świadomy, że także on może być (a nawet jest) celem oddziaływania informacyjnego, celem propagandy ukierunkowanej na dyskredytację, zmniejszenie wpływów, poniesienie wymiernych strat. Zdolność skutecznego przeciwstawienia się wrogiej kampanii informacyjnej i identyfikacji, kto za nią stoi staje się newralgicznym elementem funkcjonowania każdego państwa i najważniejszym czynnikiem skutecznego działania. Spłaszczanie problemu tylko i wyłącznie do ochrony zasobów informacyjnych nie gwarantuje działania z pozycji dodatniej w XXI wieku. Bezpieczeństwo informacyjne to transsektorowy obszar bezpieczeństwa, który odnosi się do środowiska informacyjnego (przestrzeni informacyjnej). Jest to proces, którego celem jest zapewnienie prawidłowego i zarazem bezpiecznego funkcjonowania podmiotu bezpieczeństwa w przestrzeni informacyjnej poprzez panowanie we własnej infosferze w celu zabezpieczenia własnych interesów (…)”[5].

Wspominane powyżej zagrożenia w środowisku informacyjnym są zjawiskiem powszechnym. Kluczowe jest jednak prawidłowe ich zidentyfikowanie, ponieważ „(…) powstają one na gruncie sytuacji, w ramach których mamy do czynienia z występującymi w pojedynkę lub w różnych konfiguracjach zjawiskami:

- braku informacji,
- ograniczenia dostępu do informacji,
- nadmiaru informacji,
- manipulacji informacyjnej,
- fałszerstw informacyjnych,
- napływu informacji nierzetelnej,
- utraty informacji chronionej,

[5] P. Dela, *Elementy propagandy w życiu publicznym*, Studia politologiczne, t. 54, 2019, s. 77.

– prezentowania informacji zdezaktualizowanej itp."[6]

Rozwój społeczeństwa informacyjnego powoduje pojawianie się coraz to nowszych zagrożeń o charakterze informacyjnym, są one „(…) efektem przyspieszonego rozwoju cyberprzestrzeni (inforsfery). Są one skutkiem społecznej dyfuzji technologii informacyjnych, globalizacji systemów informacyjnych, co przyniosło wzrost interakcji społecznych, lecz także nadprodukcję informacji o często wątpliwej wartości („smog informacyjny"), parainformowanie, dezinformowanie, wirtualizację faktów i zdarzeń (tabloidyzacja mediów). (…) skutecznym środkiem prowadzącym do osiągania celów politycznych (i militarnych), a także ekonomicznych, stają się strategie walki informacyjnej (cybernetycznej, sieciowej). Zasoby informacyjne (wiedzy) stały się zasobami strategicznymi wymagającymi złożonych (i wielce kosztownych) systemów zabezpieczeń przed obcą ingerencją"[7]. W powyższym opisie znajduje potwierdzenie faktu, że rola informacji, jako środka walki znacznie wzrosła, a skuteczność jej wykorzystania nie budzi, żadnych wątpliwości. Biorąc pod uwagę relatywnie niskie koszty związane z prowadzaniem działań informacyjnych należy liczyć się z dalszym wzrostem liczby tego typu działań w przyszłości.

Z uwagi na fakt, iż znacząca część informacji pozyskiwanych w życiu codziennym, ale również w działalności służbowej, pochodzi z Internetu bardzo istotne jest zdanie T. Grabowskiego, który uważa, iż „przeciętny internauta ma prawdopodobnie bardzo wysokie mniemanie na temat własnych umiejętności wyszukiwania i weryfikacji informacji, ale wyniki badań są jednoznaczne. W ich świetle trudno nawet mówić o czytaniu tekstów w Internecie, gdyż zwykle jest to ich pobieżne przeglądanie.

Tak zwane *eyetracking*, czyli badania śledzące ruch gałki ocznej na ekranie komputera, wskazują, że uwaga internauty skupia się na początkowej partii treści (w głównej mierze na lewym górnym rogu ekranu). Zatem czytanie w przypadku stron internetowych polega na zapoznaniu się z pierwszymi linijkami tekstu (głównie tytułem), następnie skanowaniu tekstu wzdłuż lewej krawędzi ekranu (czyli czytaniu pierwszych wyrazów w każdej linijce), ponownym

[6] W. Fehler, *O pojęciu bezpieczeństwa informacyjnego*, [w:] *Bezpieczeństwo informacyjne w XXI wieku*, red. M. Kubiak, S. Topolewski, Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Siedlce 2016, s. 36.

[7] P. Sienkiewicz, *Cybernetyczne aspekty rozwoju społeczeństwa informacyjnego*, [w:] *Bezpieczny rozwój społeczeństwa informacyjnego*, red. E. Szczepaniuk, M. Gawlik-Kobylińska, J. Werner, Wydawnictwo Akademia Sztuki Wojennej, Warszawa 2016, s. 38.

przeczytaniu kilku pełnych linijek w okolicach środka artykułu i wreszcie coraz mniej uważnym skanowaniu lewej części tekstu aż do końca artykułu”[8].

Mając na uwadze powyższe spostrzeżenia nasuwa się wniosek, iż znaczna część informacji pochodzących z Internetu pozyskiwana może być na podstawie łatwości jej odnalezienia. Może to powodować niebezpieczeństwo doboru informacji ze względu na jej pozycjonowanie w przeglądarce internetowej a nie w oparciu o jej merytoryczną wartość. Dalsze wykorzystanie takiej informacji, bez jej poprawnej weryfikacji, może doprowadzić do wyciągania wadliwych wniosków czy podejmowania błędnych decyzji. Konsekwencje takiego działania mogą mieć destrukcyjny wpływ na bezpieczeństwo informacyjne podmiotu lub instytucji, w funkcjonowaniu której jest wykorzystywana. Nasuwa się również wniosek, iż umiejętność wyszukiwania i weryfikacji informacji, aby dawała gwarancję pozyskania informacji dobrej jakości, powinna być oparta o solidne przygotowanie, a nie o wewnętrzne przekonanie internauty.

Zapewnienie bezpieczeństwa informacyjnego wymaga spełnienia kilku warunków. Poniżej zostały omówione te, które zdaniem autora są najważniejsze.

Pierwszym i podstawowym elementem, który należy rozważyć w kontekście zapewnienia bezpieczeństwa informacyjnego jest sama informacja. Już na etapie ustalania czym jest informacja można spotkać w literaturze przedmiotu wiele rozważań i propozycji jej zdefiniowania. Z punktu widzenia bezpieczeństwa informacyjnego takie rozważania nie są konieczne. Dużo ważniejsze jest to jakie cechy powinna ona posiadać, aby można ją było wykorzystać do zaspokajania potrzeb informacyjnych, czyli powinna to być informacja dobrej jakości.

Do takich cech informacji zaliczyć można m.in.:

- aktualność,
- kompletność,
- spójność,
- użyteczność z punktu widzenia konkretnych potrzeb informacyjnych.

W niektórych opracowaniach znaleźć można również wskazanie, aby informacja była wiarygodna[9]. Zdaniem autora cecha ta bardziej dotyczy źródła

[8] T. W. Grabowski, *Postprawda a bezpieczeństwo. Wprowadzenie*, [w:] *Bezpieczeństwo informacyjne w dobie postprawdy*, red. T. W. Grabowski, M. Lakomy, K. Oświęcimski, Wydawnictwo Naukowe Akademii Ignatianum, Kraków 2018, s. 17.

[9] Porównaj: K. Liderman, *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2017, s. 17.

informacji, ponieważ to czy informacja jest wiarygodna czy nie wynika z jej treści, ale oparte jest raczej na zaufaniu do źródła i okoliczności jej pozyskania.

Źródło informacji stanowi niezwykle istotny element bezpieczeństwa informacyjnego. Również ono powinno charakteryzować się kilkoma cechami decydującymi o jego przydatności w zaspokajaniu potrzeb informacyjnych. Zaliczyć do nich można m.in.:

- dostępność,
- wiarygodność.

Źródło informacji niespełniające powyższych kryteriów będzie powodowało przerwy w dostępie do informacji w przypadku braku dostępności lub konieczność angażowania dodatkowego potencjału i utratę czasu na potwierdzenie użyteczności danych w przypadku braku wiarygodności.

Zdobycie lub posiadanie informacji dobrej jakości generuje, z kolei, potrzebę odpowiedniego jej zabezpieczenia. Potrzeba ta dotyczy kilku poziomów. Po pierwsze posiadana informacja, o ile nie jest jawna, wymaga stworzenia warunków zabezpieczających przed jej utratą. Co więcej, w szczególnych przypadkach nie tylko sama informacja, ale również sam fakt jej posiadania powinien podlegać ochronie przed ujawnieniem. Po drugie posiadana informacja musi zostać zabezpieczona przed utratą integralności, a co za tym idzie utratą użyteczności w zaspokajaniu potrzeb informacyjnych. Po trzecie posiadana informacja musi zostać zabezpieczona przez utratą dostępności do niej. Problematykę dotyczącą ochrony informacji niejawnych szczegółowo normalizuje Ustawa o ochronie informacji niejawnych z 5 sierpnia 2010 roku[10]. Na uwagę zasługuje fakt, że w ustawie mowa jest o ochronie informacji niejawnej pod różnymi postaciami, tj. w formie dokumentu lub materiału. Powyższa ustawa wprowadza również klasyfikację informacji wprowadzając cztery klauzule informacji niejawnych:

- ściśle tajne,
- tajne,
- poufne,
- zastrzeżone[11].

[10] *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (Dz. U. z 2010 r. Nr 182, poz. 1228).

[11] Tamże, s. 5.

Nadanie odpowiedniej klauzuli informacji niejawnej powiązane zostało ściśle ze szkodami jakie może przynieść Rzeczypospolitej Polskiej ujawnienie takiej informacji.

Szczególnie ważna z punktu widzenia zapewnienia bezpieczeństwa informacyjnego jest identyfikacja potrzeb informacyjnych i dlatego nie może być procesem realizowanym „na wyczucie". Jest to w zasadzie czynnik, bez którego mówienie o bezpieczeństwie informacyjnym nie może mieć miejsca, gdyż, jeżeli podmiot, którego bezpieczeństwo informacyjne ma zostać zapewnione, nie posiada świadomości swoich niedoborów informacyjnych, to w takiej sytuacji albo nie będzie wykazywał działań w kierunku pozyskania informacji, ponieważ nie będzie „odczuwał" potrzeby ich posiadania, albo wręcz przeciwnie będzie wykazywał „nadaktywność" i dążył do posiadania jak największej ich ilości, a z uwagi na fakt, że nie posiadając precyzyjnie zdefiniowanych potrzeb, będą to informacje pozyskiwane „na wszelki wypadek" czy „na zapas". W ten sposób, na zdobywanie niepotrzebnych informacji, marnotrawione będą posiadane zasoby, potencjał i czas.

Posiadanie właściwej informacji oraz jej właściwe zabezpieczenie nie gwarantuje jeszcze bezpieczeństwa informacyjnego, ponieważ najcenniejsza nawet informacja nie będzie użyteczna, jeżeli nie zostanie prawidłowo udostępniona. Udostępnianie informacji jest bardzo często pomijanym elementem bezpieczeństwa informacyjnego, czasami wręcz bagatelizowanym. Tymczasem źle udostępniona informacja może nie tylko być niemożliwa do wykorzystania, ale również przyczynić się do powstania znaczących szkód.

Prawidłowe udostępnienie informacji wymaga spełnienia kilku warunków. Pierwszy z nich dotyczy informacji, która ma być udostępniona. Powinna to być informacja starannie wyselekcjonowana z całego zbioru informacji posiadanych, tak aby w pełni zaspokajała potrzeby informacyjne, ale nie występowała w nadmiarze. Dotyczy to zwłaszcza informacji niejawnych, gdzie należy stosować zasadę „informacji niezbędnej", czyli ograniczenia ilości udostępnianej informacji do ilości niezbędnej do wykonania zadania. Ma to również zastosowanie w odniesieniu do informacji jawnych, które udostępniane w nadmiernej ilości mogą po prostu zablokować kanały przekazywania informacji oraz powodować sytuację, w której informacja istotna, niezbędna do wykonania zadania, ginie w wielości informacji zbędnej.

Z drugiej zaś strony ilość ta nie może być nadmiernie ograniczona, aby nie powodować powstawania niedoborów informacyjnych, bądź też tworzyć

przestrzeni na dopowiedzenia, domysły czy celowe „dopełnianie" luk informacyjnych informacją fałszywą.

Kolejnym krokiem jest dobór adresata udostępnianej informacji. Tu również znajduje zastosowanie zasada „informacji niezbędnej", z tym, że tyczy się doboru nie zakresu udostępnianych informacji, ale zbioru adresatów. W tym kroku wyselekcjonowani powinni być odbiorcy, którym udostępniana informacja jest niezbędna do realizacji zadań. Zbyt szeroki zbiór odbiorców oznacza, że udostępniana informacja trafi nie tylko do odbiorców, którym jest potrzebna, ale również do takich, którzy jej nie potrzebują, przez co utrudni im pracę. W skrajnym przypadku może zostać udostępniona osobom nieuprawnionym do jej posiadania. Bardzo dobrym przykładem takiego, zbyt szerokiego, udostępniania jest stosowanie tzw. „okólnika", czyli zdefiniowanej listy obejmującej najczęściej wszystkich albo prawie wszystkich odbiorców w danej organizacji. Jeżeli taki „okólnik" wykorzystywany jest niewłaściwie dochodzi do sytuacji, w której wszystkie informacje są kierowane do wszystkich.

Przeciwieństwem powyższej opisanej sytuacji jest ograniczanie ilości odbiorców lub w skrajnych przypadkach, całkowite zatrzymanie przekazywania informacji do kolejnych odbiorców. W takiej sytuacji istnieje ryzyko, że informacja niezbędna do wykonania zadania nie zostanie dostarczona do właściwych odbiorców, a potrzeby informacyjne nie zostaną zaspokojone.

Ostatnim warunkiem skutecznego i bezpiecznego udostępniania informacji jest dobór odpowiedniego kanału przekazywana informacji od nadawcy do odbiorcy. Kanał taki również powinien spełniać kilka warunków. Przede wszystkim powinien gwarantować zachowanie bezpieczeństwa przekazywanej informacji, co oznacza, że przekazywana nim informacja powinna być zabezpieczona przed:

- dostępem osób niepowołanych,
- utratą integralności,
- utratą dostępu.

Kanał wybrany do udostępniania informacji powinien gwarantować również odpowiedni sposób kodowania, taki który będzie dostępny zarówno dla nadawcy jak i dla odbiorcy. W innym przypadku, pomimo posiadania teoretycznej możliwości udostępnienia informacji, w praktyce może to być zupełnie niemożliwe np. z uwagi na różnice językowe albo wykorzystywanie przez nadawcę i odbiorcę niekompatybilnych systemów informatycznych.

Niezmiernie ważne dla zapewniania bezpieczeństwa informacyjnego jest posiadanie kompetentnego personelu zajmującego się przetwarzaniem informacji. Nawet najbardziej zaawansowane systemy zabezpieczeń czy przetwarzania informacji będą nieprzydatne w sytuacji, kiedy ludzie je obsługujący nie będą umieli lub nie będą chcieli się mini posługiwać. W takiej sytuacji systemy te albo będą wykorzystywane w sposób najbardziej prosty, podstawowy, bez wykorzystania ich zaawansowanych możliwości albo z uwagi na trudności w obsłudze, niewyszkolony personel unikał będzie ich wykorzystania.

Wyszkolenie personelu obejmować powinno również podnoszenie świadomości w zakresie konieczności zachowania odpowiednich procedur i stosowania się do obowiązujących zasad.

Niezwykle ważne jest również posiadanie odpowiednio wyszkolonego personelu odpowiedzialnego za organizację i implementację systemów zabezpieczeń. Jest to warunek konieczny do właściwego zidentyfikowania zagrożeń, określenia możliwości przeciwdziałania im, a w konsekwencji wyboru i implementacji adekwatnych narzędzi i rozwiązań organizacyjnych. Jest to szczególnie ważne ponieważ niedoszacowane zagrożenia lub nieodpowiednio dobrane zabezpieczenia nie będą skuteczne, natomiast „przeszacowane" zagrożenia lub zbyt rygorystyczne narzędzia, choć w teorii będą zabezpieczały bardziej niż to jest potrzebne, to w praktyce jednak mogą się okazać czynnikiem uniemożliwiającym normalne funkcjonowanie z uwagi na swoją uciążliwość w stosowaniu, co w konsekwencji może prowadzić do szukania przez personel „dróg na skróty" w celu ułatwienia lub w skrajnych przypadkach w ogóle umożliwienia wykonywania zadań. Taka sytuacja w sposób oczywisty prowadzi do powstawania luk w zabezpieczeniach i osłabienia całego systemu zabezpieczeń czyniąc go nieskutecznym.

Jednym z najmniej oczywistych elementów umożliwiających zapewnienie bezpieczeństwa informacyjnego jest wypracowanie odporności na oddziaływanie informacyjne strony przeciwnej. Wynika to z faktu, że nie wiąże się on z zapewnieniem dostępu do informacji i jej właściwego przetwarzania, ale polega na wypracowaniu odporności przed wykorzystaniem, przez stronę przeciwną, informacji jako środka oddziaływania. Uzyskanie takiej odporności jest niezwykle ważne dla prawidłowego funkcjonowania sił zbrojnych. Wynika to z faktu, że oddziaływanie informacyjne realizowane może być na wielu płaszczyznach i może być wykorzystywane zarówno do oddziaływania ośrodki

decyzyjne/dowódców, jak również na pododdziały bezpośrednio zaangażowane w walkę.

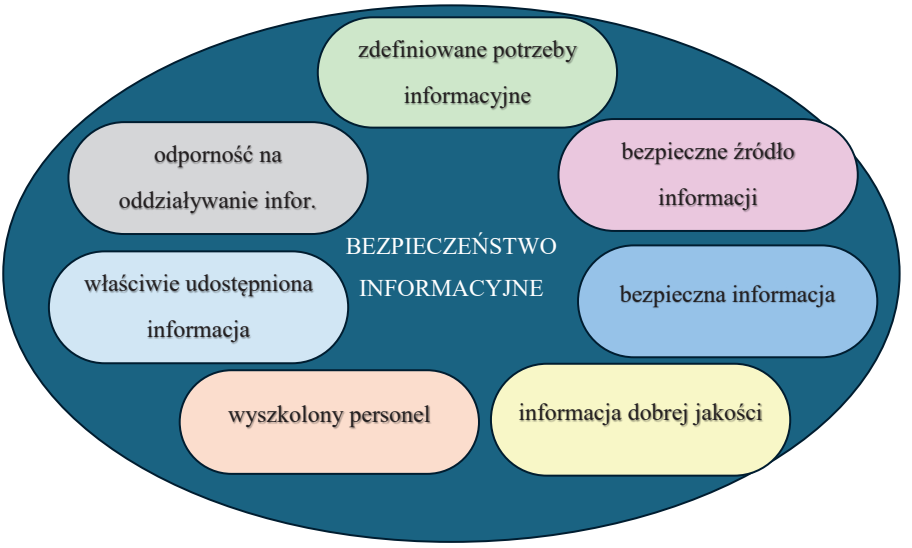
Uzyskanie odporności na oddziaływanie informacyjne wymaga szczególnych rozwiązań systemowych, które zapewnią ochronę przed przenikaniem niepożądanych informacji, zabezpieczą wykorzystywane kanały przekazywania informacji przez zakłóceniami, a także zapewnią uzyskanie odpowiednio wysokiego poziomu wyszkolenia i świadomości zagrożeń mogących wystąpić w infosferze całemu zaangażowanemu w działania personelowi.

Na podstawie powyższych rozważań można podjąć próbę określenia czym jest bezpieczeństwo informacyjne sił zbrojnych. Bezpieczeństwo informacyjne jako pewien stan, którego osiągniecie możliwe jest jedynie w sytuacji, w której wiele elementów i systemów sił zbrojnych znajduje się w określonym poziome funkcjonowania. Z dużym prawdopodobieństwem można przyjąć, że o bezpieczeństwie informacyjnym można mówić w sytuacji jednoczesnego zaistnienia wszystkich wymienionych powyżej elementów jednocześnie.

Omówione powyżej elementy organizowane i realizowane są na różnych płaszczyznach funkcjonowania sił zbrojnych. Wzajemnie się jednak przenikają przez co wzajemnie się uzupełniają i wzmacniają. Dodatkowo w wielu obszarach ich wzajemne oddziaływanie zapewnia redundancję na wypadek dysfunkcji, któregoś z elementów.

Można zatem stwierdzić, że bezpieczeństwo informacyjne stanowi swoisty „konglomerat" elementów, do których należy zaliczyć (rysunek 1):

- zdefiniowane potrzeby informacyjne,
- bezpieczne źródło informacji,
- bezpieczna informacja,
- informacja dobrej jakości,
- odporność na oddziaływanie informacyjne,
- właściwie udostępniana informacja,
- wyszkolony personel.



Rysunek 1. Elementy składowe bezpieczeństwa informacyjnego
Źródło: opracowanie własne.

Zebrane materiały pozwalają na sformułowanie wniosku, że o bezpieczeństwie informacyjnym można mówić jedynie w sytuacji, kiedy jednocześnie występują wszystkie wymienione powyżej elementy. Poszczególne składowe bezpieczeństwa informacyjnego mogą zatem być traktowane jako specyficznie rozumiane elementy zabezpieczające, których prawidłowa implementacja zapewnia bezpieczeństwo informacyjne na akceptowalnym poziomie. Żaden z nich występujący osobno nie gwarantuje osiągnięcia bezpieczeństwa informacyjnego na satysfakcjonującym poziomie. Dopiero ich połączenie i wzajemne oddziaływanie dają możliwość stworzenia warunków do zapewnienia bezpieczeństwa informacyjnego.

Czynniki determinujące bezpieczeństwo informacyjne sił zbrojnych

Z uwagi na wielość procesów jednocześnie realizowanych w siłach zbrojnych, które są wzajemnie powiązane i wzajemnie zależne, informacja jest dla tej organizacji zasobem kluczowym. Zwłaszcza, że niejednokrotnie żołnierze są zmuszeni do funkcjonowania w okolicznościach niedoboru informacji lub wręcz w sytuacji, w której strona przeciwna celowo dostarcza informacje nieprawdziwe.

Dla stworzenia lepszego kontekstu wykorzystania informacji, należy wyróżnić co najmniej dwa warianty funkcjonowania sił zbrojnych, ponieważ, z uwagi na swoją specyfikę funkcjonują one niejako w dwóch skrajnie odmiennych stanach. Pierwszy to pokojowe funkcjonowanie, które charakteryzuje się realizacją procesów niezbędnych do wykonania zadań w czasie nie będącym wojną, gdzie jednostki wojskowe stacjonują w koszarach lub na poligonach, najczęściej w niepełnym ukompletowaniu, które pozwala jedynie na: zabezpieczenie bieżącego funkcjonowania, zapewnienie możliwości szkoleniowych, a także realizację samego szkolenia, które to z kolei jest niczym innym jak przygotowaniem do prowadzenia walki. Każdy z tych obszarów pokojowego funkcjonowania wymaga przetwarzania odmiennych informacji, pochodzących z różnych źródeł, np. w trakcie szkolenia jedną z kluczowych informacji jest ta, która dostarcza danych na temat potencjalnego przeciwnika oraz warunków ewentualnej przyszłej walki. Pozwala to siłom zbrojnym na przygotowanie się do działań „w przyszłości", a nie do walki wg reguł z wojny poprzedniej. Taką informacją będzie ta dotycząca wyposażenia i taktyki walki potencjalnego przeciwnika. Znane w środowisku wojskowym powiedzenie, że wojsko przygotowuje się do wojny, która już się obyła doskonale obrazuje ten problem, ponieważ dużo łatwiej jest zdobyć informacje na temat walk, które już zostały stoczone niż skutecznie prognozować sposoby prowadzenia walki w przyszłych wojnach.

W przypadku braku aktualnych informacji, np. na temat możliwości przyszłego przeciwnika oraz środowiska przyszłych działań siły zbrojne zmuszone są do działania zgodnie z posiadanymi informacjami, a te z reguły pochodzą z konfliktów zbrojnych, które już się zakończyły lub ewentualnie właśnie trwających. Niezwykle trudno pozyskać informację nt. planowanych konfliktów zbrojnych z uwagi na oczywisty fakt ukrywania kluczowych informacji przez agresora. Nawet pozyskanie takich informacji przez wyspecjalizowane organizacje nie gwarantuje odpowiedniego zaspokojenia, na potrzeby szkoleniowe, niedoborów informacyjnych, dotyczących przyszłej wojny, z co najmniej dwóch powodów. Po pierwsze ujawnienie posiadania takich informacji może spowodować zmianę w sposobie działania potencjalnego przeciwnika, z drugiej zaś doświadczenia wielu wojen pokazuję, że początkowe założenia, co do sposobu prowadzenia wojny, rzadko kiedy nie ulegają zmianie tuż po jej rozpoczęciu z uwagi na bardzo szybko zmieniające się okoliczności jej prowadzenia zarówno te organizacyjne jak i techniczne.

Drugi stan funkcjonowania sił zbrojnych to stan wojny. Stan, w którym siły zbrojne realizują zadania chrakteryzujące się dużą dynamiką. Ponadto wykonywane są one pod presją czasu, niejednokrotnie także pod dużą presją ze strony przeciwnika oraz presją ze strony przełożonych. Dodatkowo, w odróżnieniu od funkcjonowania w czasie pokoju, zadania te niejednokrotnie wymagają od żołnierzy działania zagrożonego utratą życia. W takich okolicznościach nietrafne, spóźnione czy zaniechane decyzje i/lub działania mogą skutkować nie tylko utratą potencjału czy terytorium, ale także życia żołnierzy.

Funkcjonujące w stanie wojny siły zbrojne zmuszone są do przetwarzania informacji na wielu płaszczyznach. Z jednej strony potrzebują sprawnego systemu pozyskiwania i dystrybucji informacji o przeciwniku, jego potencjale, położeniu prawdopodobnych zamiarach, a także, o ile to tylko jest możliwe, o stanie jego wiedzy na temat naszych sił zbrojnych, z uwzględnieniem wszystkich wspominanych powyżej obszarów.

Z drugiej strony niezbędny jest sprawny system wymiany informacji nt. własnych możliwości, planów i działań. Taki system powinien zapewnić sprawną wymianę informacji niezbędnych do skutecznego prowadzenia walki. Wiąże się to z koniecznością skutecznego przekazywania informacji planistycznych i rozkazodawczych oraz wymiany informacji w trakcie prowadzonej walki, w celu synchronizacji działań oraz reagowania na sytuacje nieprzewidziane.

Dodatkowo niezbędne jest utrzymanie sprawnego systemu wymiany informacji koniecznych do skutecznego zaopatrywania i uzupełniania sił zbrojnych w celu odbudowania kurczących się zasobów jednostek w takcie prowadzenia działań. Bez takich informacji niemożliwe jest utrzymanie prawidłowego poziomu zdolności pododdziałów do prowadzenia walki. Zaspokojenie potrzeb informacyjnych w opisanych powyżej stanach funkcjonowania sił zbrojnych jest warunkiem niezbędnym do zapewnienia bezpieczeństwa informacyjnego.

W każdym z powyżej opisanych stanów spełnienie warunków niezbędnych do zapewnienia bezpieczeństwa informacyjnego wymagało będzie odmiennych działań, co wynika ze złożoności całej sytuacji, ponieważ wymaga od sił zbrojnych opracowania systemów zapewniających bezpieczeństwo informacyjne z jednej strony ściśle dostosowanych do aktualnych potrzeb, z drugiej zaś na tyle elastycznych, że będą w stanie sprawnie i bez zakłóceń zmienić swój sposób funkcjonowania w przypadku zmiany stanu funkcjonowania z pokojowego na wojenny.

Zrozumienie złożoności tego problemu możliwe jest dopiero po zrozumieniu jak złożone i wielowymiarowe jest bezpieczeństwo informacyjne samo w sobie.

Podsumowanie

Uzyskanie odpowiedzi na postawione we wstępie pytania wymagało dogłębnego rozważenia i analizy dostępnych treści w wielu wymiarach. Różnorodność podejść reprezentowanych przez wielu autorów oraz ciągle zmieniające się warunki w inforsferze powodują, że niezwykle trudno jest jednoznacznie zdefiniować czym jest bezpieczeństwa informacyjne. Poczyniona przez autora analiza dostępnego materiału źródłowego pozwoliła sformułowanie wniosku, że o bezpieczeństwie informacyjnym można mówić jedynie w sytuacji, kiedy jednocześnie występują elementy takie jak:

- zdefiniowane potrzeby informacyjne,
- bezpieczne źródło informacji,
- bezpieczna informacja,
- informacja dobrej jakości,
- odporność na oddziaływanie informacyjne,
- właściwie udostępniana informacja,
- wyszkolony personel.

Zaistnienie każdego z tych elementów samodzielnie nie stanowi o osiągnięciu bezpieczeństwa informacyjnego. Dopiero ich połączenie i wzajemne oddziaływanie dają możliwość stworzenia warunków do zapewnienia bezpieczeństwa informacyjnego.

Niezwykła złożoność bezpieczeństwa informacyjnego, połączona ze złożonością sił zbrojnych, realizujących nieustanie zmienne zadania w ewoluujących okolicznościach powoduje, że jego zapewnienie jest niezwykłym wyzwaniem. Kluczowym elementem wydaje się być przede wszystkim posiadanie świadomości konieczności jego zapewnienia, a następnie zrozumienie jego złożoności. Kolejnym elementem jest stworzenie na tyle elastycznych struktur, odpowiedzialnych za bezpieczeństwo informacyjne, aby były w stanie skutecznie realizować swoje zadania we wszystkich wymienionych powyżej obszarach oraz we wszystkich okolicznościach (pokojowe funkcjonowanie, wojna) w jakich przyjdzie siłom zbrojnym funkcjonować.

Zadanie to jest trudne, ale jednocześnie niezwykle istotne, tak jak istotne są cele, dla których osiągnięcia wykorzystywane są siły zbrojne.

Literatura

1. *AJP-01 Allied Joint Doctrine, Edition F Version 1,* NATO Standardization Office (NSO), Grudzień 2022.
2. *AJP-10.1 Allied Joint Doctrine For Information Operations, Edition A, Version 1*, NATO Standardization Office (NSO), Styczeń 2023.
3. Dela P., *Elementy propagandy w życiu publicznym*, Studia politologiczne, t. 54, 2019, s. 77.
4. Fehler W., *O pojęciu bezpieczeństwa informacyjnego,* [w:] *Bezpieczeństwo informacyjne w XXI wieku*, red. M. Kubiak, S. Topolewski, Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Siedlce 2016*,* s. 36.
5. Grabowski T. W., *Postprawda a bezpieczeństwo. Wprowadzenie,* [w:] *Bezpieczeństwo informacyjne w dobie postprawdy*, red. T. W. Grabowski, M. Lakomy, K. Oświęcimski, Wydawnictwo Naukowe Akademii Ignatianum, Kraków 2018, s. 17.
6. Jakubowska M., *Informacja i jej bezpieczeństwo – wybrane zagadnienia*, [w*:*] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku,* red. M. Górka, Difin, Warszawa 2014, s. 15.
7. Janczak J., Nowak A., *Bezpieczeństwo informacyjne. Wybrane problemy*, Akademia Obrony Narodowej, Warszawa 2013, s. 19.
8. Liderman, K., *Bezpieczeństwo informacyjne*, Wydawnictwo naukowe PWN, Warszawa 2012.
9. Liderman, K., *Bezpieczeństwo informacyjne. Nowe wyzwania*, Wydawnictwo Naukowe PWN, Warszawa 2017.
10. Sienkiewicz P., *Cybernetyczne aspekty rozwoju społeczeństwa informacyjnego,* [w:] *Bezpieczny rozwój społeczeństwa informacyjnego*, red. E. Szczepaniuk, M. Gawlik-Kobylińska, J. Werner, Wydawnictwo Akademia Sztuki Wojennej, Warszawa 2016, s. 38.
11. *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (Dz. U. z 2010 r. Nr 182, poz. 1228).