Tomasz R. Aleksandrowicz

Bezpieczeństwo informacyjne państwa

Słowa kluczowe:
bezpieczeństwo państwa, informacja, bezpieczeństwo informacyjne

Wprowadzenie

Jedną z istotnych konsekwencji powstania i dynamicznego rozwoju społeczeństwa informacyjnego jest rozszerzenie zakresu przedmiotowego bezpieczeństwa państwa o kategorię bezpieczeństwa informacyjnego. Konstytutywną cechą społeczeństwa informacyjnego jest traktowanie informacji w kategoriach zasobu strategicznego przy równoczesnym upowszechnieniu dostępu do informacji. Przetwarzanie informacji staje się podstawą tworzenia dochodu narodowego i źródłem utrzymania coraz znaczniejszej części społeczeństwa. Dostęp do informacji, zdolność do jej przetwarzania, zabezpieczenia, przekazywania i przechowywania staje się również kluczowa dla bezpieczeństwa narodowego. Informacja stała się zasobem strategicznym[1], nastąpił wyraźny wzrost jej znaczenia, nie-

[1] Stwierdzenie to odnosi się nie tylko do państw, lecz także do innych podmiotów. Leszek F. Korzeniowski, *Podstawy nauk o bezpieczeństwie*, Warszawa 2012, s. 144, podaje, że „udział zasobów informacyjnych w strukturze wartości wszystkich zasobów firmy może osiągać nawet 80%. Badania grupy 500 największych firm amerykańskich w 2000 roku wykazały, że w każdych 6 dolarach wartości rynkowej tych firm, 5 dolarów reprezentowało zasoby niewidzialne, nie wycenione w majątku, czyli zasoby informacyjne, a tylko 1 dolar to wartość zasobów rzeczowych i finansowych. Z tego wynika, że zasoby informacyjne stały się czynnikiem najważniejszym w osiąganiu celów każdej organizacji

zależnie od formy jej przedstawienia czy przechowywania w funkcjonowaniu społeczeństw, wytwarzania dóbr i dochodu narodowego oraz – *last not least* – składnika potęgi państwa[2]. „W tym sensie pojęcie rewolucji informacyjnej odnosi się do swego rodzaju megatrendu społecznego we współczesnym świecie, przejawiającego się m.in. w rosnących możliwościach oddziaływania mediów, zwłaszcza masowych, na przebieg procesów politycznych i społecznych, nie zaś samych zmianach technologicznych, umożliwiających wzrost znaczenia informacji"[3]. Należy także zwrócić uwagę na ilość dostępnych informacji, których liczba zbliża się do tzw. *attention crash* – momentu, w którym informacje, jakie chcemy przyswoić, przekraczają zdolność skupienia uwagi.

Jeśli zatem informacja stanowi – z punktu widzenia podmiotu bezpieczeństwa – jego zasób strategiczny, a więc jest elementem krytycznym dla jego funkcjonowania, musi być odpowiednio chroniona na każdym etapie przetwarzania: od pozyskania informacji, poprzez jej przekazywanie, przechowywanie, analizę i wykorzystanie, aż po zachowanie w poufności.

Termin bezpieczeństwo informacyjne państwa (podmiotu) został wprowadzony dopiero w drugiej połowie XX wieku. Nie oznacza to jednak, że informacja – jako czynnik bezpieczeństwa – nie miała wcześniej znaczenia i że nie było ono dostrzegane. Przeciwnie – problemy związane z informacją zawsze pozostawały w centrum uwagi władców, wodzów, aparatu państwowego. Wiarygodna, rzetelna, dokładna i aktualna informacja zawsze bowiem była istotna przy podejmowaniu decyzji państwowych, w szczególności w dziedzinie bezpieczeństwa – tak zewnętrznego, jak i wewnętrznego.

Śledząc pod tym kątem historię można stwierdzić, iż tradycyjnie bezpieczeństwo informacyjne rozumiano jako konglomerat kilku elementów. Po pierwsze, było to zapewnienie sobie dostępu do informacji o otoczeniu, środowisku, potencjalnych przeciwnikach i sojusznikach. Po wtóre – to ochrona informacji własnych, takich, których ujawnienie naruszałoby interesy danego podmiotu. Widoczna była pewna symetria:

---

gospodarczej. Są niezbędne we wszystkich funkcjach zarządzania: w planowaniu, organizowaniu, motywowaniu i kontrolowaniu". Zob.: T. Aleksandrowicz, *Świat w sieci. Państwa – społeczeństwa – ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*, Warszawa 2014, s. 62 i n.

[2] Zob. na ten temat: P. Levinson, *Miękkie ostrze, czyli historia i przyszłość rewolucji informacyjnej*, Warszawa 2006, passim.

[3] M. Madej, *Rewolucja informacyjna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, [w:] M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009, s. 18.

najcenniejszymi informacjami o przeciwniku zawsze były te, które starał się on zachować w tajemnicy; w sposób niejako naturalny ukształtowała się zasada zdobywania informacji chronionych przez przeciwnika przy jednoczesnej ochronie własnych tajemnic, które przeciwnik chce zdobyć. Po trzecie wreszcie, to zdobywanie przez rządzących informacji na temat rządzonych. Było to, rzecz jasna, ściśle związane z bezpieczeństwem władzy: pozyskiwano informacje o niezadowolonych, skłonnych do buntu, spiskujących przeciwko władcy, podburzających do oporu przeciw władzy etc.[4].

Funkcje i atrybuty informacji

Tak szerokie ujęcie wynika bezpośrednio z definicji pojęcia informacji, funkcji jakie informacja pełni we współczesnym państwie i społeczeństwie oraz z jej atrybutów.

Zdefiniowanie pojęcia „informacja" jest zadaniem stosunkowo trudnym i wymagającym zagłębienia się w tajniki teorii poznania. Najprościej można przyjąć, że informację stanowi każdy opis rzeczywistości, niezależnie od tego, czy jest on zgodny z prawdą, czy też nie. Takie rozumienie pojęcia informacji wynika poniekąd z łacińskiego źródłosłowu: *informatio* oznacza wizerunek, zarys, pojęcie, zaś czasownik *informo* – kształtować, tworzyć, wyobrażać sobie, przedstawiać, opisywać, kreślić, kształcić, uczyć[5]. Już samo wyliczenie tych znaczeń pozwala wskazać na funkcje informacji i jej znaczenie dla funkcjonowania człowieka i społeczeństwa.

Informacja ma wymiar niematerialny i należy odróżnić ją (jej treść) od nośnika, na którym została utrwalona (np. zapis na papierze czy plik komputerowy), jej źródła bezpośredniego (wypowiedź polityka) czy pośredniego (cytat tej wypowiedzi w mass mediach). Niekiedy informacja może funkcjonować wyłącznie w postaci niematerialnej, choćby jako plotka powtarzana z ust do ust. Możliwa jest także sytuacja, w której informacja ma wymiar wyłącznie materialny – np. nowy procesor komputerowy czy lufa czołgowa[6].

Syntetycznego przeglądu definicji pojęcia informacji dokonał w literaturze przedmiotu Krzysztof Liedel[7], którego zdaniem podejmowane

[4] Zob. T. Aleksandrowicz, *Podstawy walki informacyjnej*, Warszawa 2016, s. 53 i n.

[5] *Słownik łacińsko-polski w opracowaniu Kazimierza Kumanieckiego*, Warszawa 1975, s. 260.

[6] Zob. T. Aleksandrowicz, *Komentarz do ustawy o dostępie do informacji publicznej*, wyd. 4, Warszawa 2008, s. 95 i n.

[7] Zob. K. Liedel, *Zarządzanie informacją w walce z terroryzmem*, Warszawa 2010, s. 42–45.

przez poszczególnych badaczy próby definicyjne nie przyniosły zadowalających rezultatów, bowiem dotykają one jedynie wybranych aspektów informacji[8]. Przywołany autor przytacza następujące definicje:

- informacja to zbiór faktów, zdarzeń, cech itp. określonych obiektów (rzeczy, procesów, systemów) zawarty w wiadomości (komunikacie), ujęty i podany w takiej postaci (formie), że pozwala odbiorcy ustosunkować się do zaistniałej sytuacji i podjąć odpowiednie działania umysłowe lub fizyczne (Piotr Sienkiewicz);
- informacja jest transformacją jednego komunikatu asocjacji informacyjnej w drugi komunikat tej asocjacji; informowanie jest to transformowanie informacji zawartych w łańcuchu oryginałów w informacje zawarte w łańcuchu obrazów (Marian Mazur);
- informacja to wiedza przekazywana przez innych ludzi bądź uzyskiwana przez studia, obserwacje i badania (Andrew Webster);
- informacja to czynnik sterujący strumieniami zasileń, wykorzystywany w organizmach żywych lub maszynach do bardziej sprawnego, efektywnego i celowego działania (Edward Kowalczyk);
- informacja – bodziec oddziaływujący na układ recepcyjny człowieka, powodujący wytwarzanie w jego wyobraźni przedmiotu myślowego, odzwierciedlającego obraz rzeczy materialnej lub abstrakcyjnej, który w jego przekonaniu (świadomości) kojarzy się jakoś z tym bodźcem; oznacza to, że informacje to nie tylko te doznania, które inspirują umysł ludzki do pewnej wyobraźni; jej istnienie jest relatywnie związane z istnieniem człowieka i jego umysłem (Leopold Ciborowski);
- informacją jest nie tylko wiadomość o czymś, ale także każda decyzja, sugestia czy polecenie (Norbert Wiener);
- informacja to wiadomość uzyskana przez człowieka poprzez obserwację lub czynność umysłową, podlegającą przekazowi w układzie nadawca – odbiorca (Henryk Greniewski).

Ten krótki przegląd definicji warto uzupełnić o rozważania Czesława Bermana, który pojęcie informacji rozpatrywał w czterech kategoriach: jako rzecz, wielkość mierzalną, potencjał i zmianę. Informację jako rzecz Berman zdefiniował jako produkt określonego procesu, mającego wykonawcę, czyli źródło informacji i użytkownika – odbiorcę. Informacja rozumiana jako rzecz może być zatem wytwarzana, magazynowana, przesyłana, przetwarzana, sprzedawana etc. Informacji można przypisać szereg właściwości: treść, formę, wielkość, użyteczność czy wartość. Tak rozumiana informacja przybiera postać znaku o określonej strukturze

[8] Tamże, s. 44.

fizycznej. Istnieje zatem tworzywo, w jakim została ona utrwalona. Informacja jest także wielkością mierzalną (np. jako zapis w postaci konkretnej liczby znaków). Rozpatrywana jako potencjał, informacja ma zdolność do zmiany określonego stanu rzeczy na skutek zmniejszenia lub eliminacji niepewności odbiorcy w odniesieniu do rozważanych przez niego stanów, wybranych ze zbioru stanów możliwych[9].

Podsumowując przegląd definicji pojęcia informacja K. Liedel konstatuje, że:

- informacja może istnieć obiektywnie, niezależnie od woli i świadomości ludzi;
- informacja może występować w systemie jako czynnik sprawczy, odnosząc się do zjawisk, które nie występują w chwili obecnej, ani nie występowały w przeszłości, lecz pojawią się w przyszłości;
- informacja może dotyczyć procesów i zjawisk nierealnych, które w danym systemie nigdy nie zaistniały i nie zaistnieją w przyszłości;
- zbiór informacji jest zbiorem niewyczerpanym – informacja w przeciwieństwie do innych zasobów nie zużywa się w procesie jej wykorzystania;
- informacja może być przetwarzana, powielana i transportowana w czasie i przestrzeni, szczególnie za pomocą technik informacyjno-telekomunikacyjnych. Inny autor, Krzysztof Liderman precyzuje, iż informacja może być przenoszona w czasie i przestrzeni. Przenoszenie w czasie nazywa się magazynowaniem lub zapamiętywaniem, a przenoszenie w przestrzeni – transmisją lub komunikowaniem. Przenoszenie informacji odbywa się za pośrednictwem obiektów (nośników informacji), z wykorzystaniem zjawisk fizycznych. Magazynowanie związane jest najczęściej ze stanami wyróżnionymi obiektu fizycznego (tzw. podłoża zapisu), a transmisja ze stanami wyróżnionymi określonego zjawiska fizycznego (sygnałami)[10];
- specyficzną cechą informacji jest konieczność jej aktualizacji;
- cechą informacji jest jej różnorodność;
- informacje mogą podlegać deformacji, zniekształceniom lub zafałszowaniu na skutek świadomego działania człowieka lub zdarzeń przypadkowych;
- informacja musi być wyrażona komunikatem (wiadomością) za pośrednictwem nośnika[11].

[9] Tamże, s. 44, 45.

[10] K. Liderman, *Bezpieczeństwo informacyjne*, Warszawa 2012, s. 17.

[11] K. Liedel, *Zarządzanie informacją…*, s. 45.

Zdaniem K. Lidermana, informacja jest przede wszystkim towarem o znaczeniu strategicznym dla każdego podmiotu (państwa, firmy, osoby fizycznej) i podstawowym elementem procesów zarządzania, bowiem trudno sobie wyobrazić funkcjonowanie jakiegokolwiek podmiotu bez poprawnego obiegu informacji. Jego przerwanie lub zafałszowanie informacji – podkreśla Liderman – powoduje straty dla firmy mogące skończyć się bankructwem, a dla państwa niepokojami społecznymi, zaburzeniami w gospodarce, osłabieniem pozycji na arenie międzynarodowej etc.[12].

Informacja jest zatem traktowana jako zasób strategiczny – posiada ona swoją wartość, jej zdobycie i wykorzystanie pociąga za sobą określone koszty, zaś jej brak oznacza brak skuteczności w działaniu. Wynika to bezpośrednio z funkcji, jakie informacja spełnia we współczesnej rzeczywistości. Nawet przyjmując stosunkowo uproszczoną definicję informacji rozumianą jako opis rzeczywistości można wskazać na cały szereg funkcji:

- funkcja modelowania (opisu) – informacja stanowi obraz rzeczywistości, jest miarą złożoności i różnorodności badanego wycinka rzeczywistości;
- funkcja decyzyjna – informacja może motywować do działania, osiągania określonych celów;
- funkcja sterująca – znajdująca zastosowanie w różnego rodzaju bazach wiedzy i bazach danych, które stanowią podstawę planowania i podejmowania decyzji. W szczególności informacja służy do sterowania procesami w zautomatyzowanych procesach wytwórczych i usługowych o kluczowym znaczeniu dla gospodarki i społeczeństwa;
- funkcja rozwoju wiedzy (cywilizacji);
- funkcja kapitałotwórcza (obok ziemi, kapitału i pracy);
- funkcja konsumpcyjna, zakładająca traktowanie informacji jako towaru[13];
- funkcja kulturotwórcza[14].

Informacja, aby móc wypełniać te funkcje musi charakteryzować się określonymi cechami, które określają jej jakość. W literaturze przedmiotu za kryteria jakości informacji uznaje się:

- relewantność, tj. istotność informacji dla odbiorcy;

---

[12] K. Liderman, *Bezpieczeństwo informacyjne*, s. 17.

[13] Zob. T. Jemioło, P. Sienkiewicz (red.), *Zagrożenia dla bezpieczeństwa informacyjnego państwa. Identyfikacja, analiza zagrożeń i ryzyka. Tom I – Raport z badań*, Warszawa 2004, s. 162. Zob. też K. Liedel, T. Serafin, *Otwarte źródła informacji w działalności wywiadowczej*, Warszawa 2011, s. 38 i n. Por. K. Liedel, *Zarządzanie informacją…*, s. 42, 44–45.

[14] Zob. K. Liedel, *Zarządzanie informacją…*, s. 45; K. Liedel, T. Serafin, *Otwarte źródła informacji…*, s. 39.

- dokładność, tj. precyzyjność (stopień uwzględnienia szczegółów w treści informacji) oraz zaprezentowanie jej w sposób odpowiedni do poziomu wiedzy odbiorcy;
- jednoznaczność – stosowanie jednoznacznie określonego języka oraz precyzyjnie określonych pojęć;
- komunikatywność mierzona ilością pracy niezbędnej dla nadania jej przez odbiorcę formy umożliwiającej wnioskowanie i podjęcie decyzji;
- spójność, czyli wewnętrzna niesprzeczność (poszczególne elementy informacji są wzajemnie niesprzeczne, dotyczą zadanego tematu i są przekazane w jednolitej formie);
- odpowiedniość formy – prezentowanie informacji w sposób, który minimalizuje możliwość jej błędnej interpretacji;
- agregacja, czyli poziom syntezy informacji;
- aktualność, oznaczająca zgodność informacji ze stanem rzeczywistym, a więc sytuację, w której informacja zmieniana jest bez opóźnień, odpowiednio do zmian przedmiotu opisu;
- kompletność, oznaczająca dostępność w ilości i stopniu szczegółowości zgodnym z wymaganiami odbiorcy/użytkownika;
- celowość, rozumiana jako zdolność do wyznaczania norm w procesie sterowania;
- wartość – spowodowanie zmiany wartości sytuacji decyzyjnej;
- decyzyjność, a więc stopień wpływu na przebieg procesu decyzyjnego;
- pełność, mierzona stopniem likwidacji niepewności decydenta w procesie zarządzania;
- porównywalność, rozumiana jako możliwość porównania danej informacji z innymi informacjami;
- prawdziwość – zgodność treści informacji z opisywaną rzeczywistością;
- wiarygodność, a więc brak deformacji informacji; innymi słowy – elementy zawarte w informacji upewniają, co do rzetelności niesionego przez nią przekazu;
- wierność – informacja w zbiorze oryginałów jest taka sama, jak w zbiorze obrazów;
- źródłowość – pochodzenie informacji z bezpośredniej lub pośredniej obserwacji[15].

O jakości informacji, konkluduje przywołany Krzysztof Liedel, świadczy stopień, w jakim spełnia ona wymagania stawiane przez sys-

[15] Zob. K. Liedel, *Zarządzanie informacją…*, s. 48–49; K. Liderman, *Bezpieczeństwo informacyjne*, s. 18.

tem decyzyjny w zakresie aktualności, pełności i niezawodności. W tym kontekście aktualność (terminowość) informacji oznacza fakt otrzymania przez decydenta informacji w pożądanym (wymaganym) czasie, pełność (kompletność) to zawarcie rzeczywistych informacji o stanie rzeczy, zaś niezawodność (prawidłowość) określa stopień wpływu zniekształceń i zakłóceń na informacje dostarczane przez system informacyjny ich odbiorcom (decydentom)[16].

Informacja posiada także atrybuty bezpieczeństwa, odnoszące się do jej ochrony – a więc takie cechy, które pozwalają na jej ocenę pod kątem jej przesyłania, przechowywania i przetwarzania. Najczęściej wymieniane są:

- tajność, określająca wymagany poziom ochrony przed nieuprawnionym dostępem;
- integralność, a zatem określenie, czy informacje są poprawne, nienaruszone, nie poddane manipulacji;
- dostępność, określająca czy informacje są dostępne zgodnie z wymaganiami użytkownika;
- rozliczalność – określenie możliwości identyfikacji użytkownika;
- niezaprzeczalność, czyli brak możliwości ukrycia (wyparcia się) dostępu do informacji przez użytkownika;
- autentyczność, określająca możliwość stwierdzenia, jaki podmiot przekazał informacje[17].

Do kompleksowej oceny jakości informacji niezbędne są także metainformacje, czyli informacje na temat informacji. Przywołany powyżej Krzysztof Liderman wskazuje na 5 kategorii tego typu danych:

- informacje o interesariuszach – dane identyfikacyjne dostawców treści, administratorów stron internetowych, sponsorów, wydawców, reklamodawców, grupy docelowej etc;
- informacje uwierzytelniające prezentowane treści – status wykorzystanych źródeł informacji, dane i rekomendacje dotyczące podmiotów opracowujących treści, daty ich dostarczania;
- informacje o polityce stosowania prywatności i ochronie danych, wskazanie polityki zabezpieczania własności intelektualnej i prywatności oraz zgodności z obowiązującymi przepisami prawa;
- informacje o aktualności treści, daty wprowadzania zmian; uaktualnienia;

[16] K. Liedel, *Zarządzanie informacją…*, s. 48–49.

[17] K. Liderman, *Bezpieczeństwo informacyjne*, s. 19.

- informacje umożliwiające rozliczalność – dane identyfikacyjne i kontaktowe osób przygotowujących informacje, zasady edycji i doboru materiałów[18].

Zakres przedmiotowy bezpieczeństwa informacyjnego

Konotacja pojęcia bezpieczeństwo informacyjne jest bardzo szeroka[19]. W literaturze przedmiotu wskazuje się, że bezpieczeństwo informacyjne oznacza stan wolny od zagrożeń, rozumianych jako przekazywanie informacji nieuprawnionym podmiotom, szpiegostwo, działalność dywersyjna lub sabotażowa. Terminem tym określa się także wszelkie działania, systemy oraz metody zmierzające do zabezpieczenia zasobów informacyjnych gromadzonych, przetwarzanych, przechowywanych w pamięciach komputerów oraz sieciach teleinformatycznych, a także organizację przepływu informacji pomiędzy organami władzy[20].

W literaturze przedmiotu brak jest powszechnie akceptowanej definicji bezpieczeństwa informacyjnego podmiotu; w większości przypadków akcentowane są jedynie poszczególne aspekty tego pojęcia.

Piotr Sienkiewicz podejmując próbę konceptualizacji problematyki walki informacyjnej, za punkt wyjścia przyjmuje pojęcie bezpieczeństwa informacyjnego państwa jako integralnej części bezpieczeństwa narodowego, a następnie zagrożeń informacyjnych[21]. W ramach takiego podejścia należy uwzględnić szereg uwarunkowań bezpieczeństwa informacyjnego, a przede wszystkim to, że:

- informacja stanowi zasób strategiczny państwa;
- informacja i wynikająca z niej wiedza oraz technologie informatyczne stają się podstawowym czynnikiem wytwórczym;
- szeroko rozumiany sektor informacyjny generuje znaczną część dochodu narodowego[22];

---

[18] Tamże, s. 18, 19. Na temat atrybutów i funkcji informacji T. Aleksandrowicz, *Podstawy…*, s. 53 i n.

[19] Zob. L. Więcaszek-Kuczyńska, *Zagrożenia bezpieczeństwa informacyjnego*, „Obronność. Zeszyty Naukowe" 2014, nr 2(10).

[20] Zob. P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń 2005, s. 71, 73.

[21] P. Sienkiewicz, *Wizje i modele wojny informacyjnej*, s. 373, 374, http://winntbg.bg.agh.edu.pl/skrypty2/0095/373-378.pdf, dostęp: 5.04.2012.

[22] Technologie informatyczne i komunikacyjne stanowią silny czynnik wzrostu gospodarczego. W Unii Europejskiej sektor ten generuje 25% wzrostu PKB i 40% wzrostu pro-

- procesy decyzyjne w innych sektorach gospodarki i życia społecznego są w znacznej mierze uzależnione 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[23];
- technologie informatyczne stały się istotnym elementem funkcjonowania sił zbrojnych[24];
- media masowe mogą być wykorzystywane jako narzędzia skutecznego zakłócania informacyjnego, np. na drodze dezinformacji[25].

Część badaczy wiąże bezpieczeństwo informacyjne z ograniczeniami dostępu do informacji dla obywateli oraz naruszaniem prawa do prywatności poprzez rozwinięte systemy inwigilacji. Włodzimierz Fehler zwraca uwagę m.in. na słabości systemu ochrony danych osobowych i kwestie przestępczości w sferze informacyjnej[26]. Jego zdaniem, bezpieczeństwo informacyjne to „stan, w którym zapewniona jest swoboda przepływu informacji połączona z racjonalnym i prawnym wyodrębnieniem takich ich kategorii, które podlegają ochronie ze względu na bezpieczeństwo podmiotów, których dotyczą"[27]. Z drugiej strony, bezpieczeństwo informacyjne wiąże się z ochroną informacji przed niepożądanym ujawnieniem, modyfikacją lub zniszczeniem[28]. Ciekawy punkt widzenia prezentuje Krzysztof Liederman stwierdzając, iż bezpieczeństwo informacyjne

---

duktywności. Takie dane podaje Komisja Europejska w dokumencie *i2010 – Europejskie społeczeństwo informacyjne na rzecz wzrostu i zatrudnienia*, Komunikat Komisji Wspólnot Europejskich do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów. Bruksela, dnia 1.6.2005 COM(2005) 229 końcowy, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:PL:PDF (dostęp: 5.04.2012).

23 Zob. K. Liedel, *Bezpieczeństwo informacyjne państwa*, [w:] K. Liedel (red. nauk), *Transsektorowe obszary bezpieczeństwa narodowego*, Warszawa 2011, s. 57.

24 B. Balcerowicz, *Siły zbrojne w czasie pokoju, kryzysu i wojny*, Warszawa 2010, s. 219.

25 K. Liedel, *Bezpieczeństwo informacyjne…*, s. 57–58.

26 W. Fehler, *Informacyjny wymiar zagrożeń dla współczesnej Polski*, „Przegląd Strategiczny" 2015, nr 8, s. 83, 96.

27 Tenże, *Bezpieczeństwo współczesnej Polski. Aspekty teoretyczne i praktyczne*, Warszawa 2012, s. 13, 14.

28 Tak np. K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń dla bezpieczeństwa narodowego*, Toruń 2008, s. 19; P. Potejko, *Bezpieczeństwo informacyjne*, [w:] K.A. Wojtaszczyk, A. Materska-Sosnowska (red.), *Bezpieczeństwo państwa*, Warszawa 2009, s. 194; A. Żebrowski, *Bezpieczeństwo informacyjne Polski a walka informacyjna*, „Roczniki Kolegium Analiz Ekonomicznych" 2013, nr 29, s. 452.

oznacza „uzasadnione zaufanie podmiotu do jakości i dostępności pozyskiwanej informacji, pojęcie bezpieczeństwo informacyjnego dotyczy zatem podmiotu (człowieka, organizacji), który może być zagrożony utratą zasobów informacyjnych albo otrzymaniem informacji o nieodpowiedniej jakości"[29]. Inni badacze z kolei podkreślają, iż analizowany termin zawiera w sobie dwie kwestie: dostępu do informacji przez podmiot, zdolności do ich ochrony oraz zdobywania przewagi informacyjnej poprzez zdobywanie informacji chronionych przez przeciwnika, a nawet zdolności do prowadzenia wobec niego działań o charakterze dezinformacyjnym[30]. W tym kontekście należy odnotować pogląd, zgodnie z którym bezpieczeństwo informacyjne dotyczy podmiotu, który jest zagrożony przez brak dostępu do informacji, natomiast bezpieczeństwo informacji to ochrona informacji będącej w posiadaniu tego podmiotu[31].

Eugeniusz Nowak i Maciej Nowak proponują bardzo szeroką definicję bezpieczeństwa informacyjnego, zgodnie z którą jest to stan warunków wewnętrznych i zewnętrznych, który pozwala państwu na posiadanie, przetrwanie i swobodę rozwoju społeczeństwa informacyjnego. Zdaniem przywołanych autorów stan ten jest osiągnięty, gdy spełnione są następujące warunki:

- nie są zagrożone strategiczne zasoby państwa;
- organy władzy podejmują decyzje w oparciu o wiarygodne, istotne, dokładne i aktualne informacje;
- przepływ informacji pomiędzy organami państwa jest niezakłócony;
- funkcjonowanie sieci teleinformatycznych tworzących krytyczną infrastrukturę teleinformatyczną państwa jest niezakłócone;
- państwo gwarantuje ochronę informacji niejawnych i danych osobowych obywateli;
- instytucje publiczne nie naruszają prawa obywateli do prywatności;
- obywatele, organizacje pozarządowe i media masowe posiadają dostęp do informacji publicznej[32].

Podobnie definiuje pojęcie bezpieczeństwa informacyjnego Piotr Bączek wskazując, iż jest to taki stan zewnętrzny, w którym:

- nie są zagrożone strategiczne zasoby informacyjne państwa;

---

[29] K. Liderman, *Bezpieczeństwo informacyjne*, s. 22.

[30] Tak np. M. Madej, *Rewolucja informacyjna…*, s. 18, 19. Por. L.F. Korzeniowski, *Podstawy nauk o bezpieczeństwie*, Warszawa 2017, s. 184.

[31] Tak A. Nowak, W. Scheffs, *Zarządzanie bezpieczeństwem informacyjnym*, Warszawa 2010, s. 25.

[32] E. Nowak, M. Nowak, *Zarys teorii bezpieczeństwa narodowego*, Warszawa 2011, s. 103.

- władze podejmują decyzje dotyczące problematyki wewnętrznej i zewnętrznej w oparciu o prawdziwe, sprawdzone, wiarygodne i aktualne informacje, zaś organizacja ich przepływu nie jest zakłócona;
- bezpieczeństwo publicznych sieci informatycznych, prawny system ochrony informacji oraz ochrona danych osobowych obywateli są z mocy prawa gwarantowane przez państwo;
- obywatele mają prawo do prywatności;
- instytucje publiczne i prywatne, zbierając informacje o obywatelach, organizacjach i ich działalności, nie naruszają ustalonych norm prawnych;
- obywatele i ich przedstawiciele (media, organizacje pozarządowe, parlamentarzyści, organy kontrolne) posiadają w swoim zakresie dostęp do informacji o działalności władz[33].

Ze swej strony przywołany autor proponuje warstwowy model bezpieczeństwa informacyjnego. Rdzeniem systemu bezpieczeństwa informacyjnego są techniki i technologie informacyjne, które otoczone są sferami społeczną, etyczną, kulturową, naukową, gospodarczą, polityczną, bezpieczeństwa i obronności. Każda z tych dziedzin życia człowieka generuje innego typu zagrożenia, które posiadają swoją specyfikę i mogą oddzielnie wpływać na stan bezpieczeństwa narodowego. Każda z tych sfer tworzy oddzielny podsystem narodowego bezpieczeństwa informacyjnego, dlatego też musi być zabezpieczona w dwójnasób: poprzez rozwiązania uniwersalne, znajdujące zastosowanie dla wszystkich warstw, oraz poprzez rozwiązania specyficzne dla każdej sfery. Jest to strukturalny model bezpieczeństwa informacyjnego[34]. Zagrożenia dla bezpieczeństwa informacyjnego noszą bowiem charakter transsektorowy, a więc taki, który może dotyczyć wszystkich sektorów bezpieczeństwa (które w modelu Bączka zostały nazwane sferami, zaś w innych opracowaniach – sektorami bezpieczeństwa)[35].

Szerokie rozumienie bezpieczeństwa informacyjnego znalazło swoje odzwierciedlenie w opracowanym w Biurze Bezpieczeństwa Narodowego projekcie Doktryny Bezpieczeństwa Informacyjnego RP z 24 lipca 2015 r. Bezpieczeństwo informacyjne – wraz z jego integralną częścią, jaką jest cyberbezpieczeństwo – traktowane jest jako jeden z najbardziej wrażliwych obszarów bezpieczeństwa narodowego i międzynarodowego, które

[33] P. Bączek, *Zagrożenia informacyjne…*, s. 74.

[34] Tamże, s. 75, 76.

[35] Np. bezpieczeństwo polityczne, społeczne, militarne etc. Zob. T. Aleksandrowicz, *Świat w sieci…*, s. 191–194.

nosi charakter transsektorowy i wpływa na efektywność funkcjonowania całego systemu bezpieczeństwa. W tym ujęciu bezpieczeństwo informacyjne zdefiniowane zostało jako transsektorowy obszar bezpieczeństwa, którego treść odnosi się do środowiska informacyjnego (w tym cyberprzestrzeni) państwa oraz proces, którego celem jest zapewnienie bezpiecznego funkcjonowania państwa w przestrzeni informacyjnej poprzez panowanie we własnej, wewnętrznej infosferze oraz efektywną ochronę interesów narodowych w zewnętrznej (obcej) infosferze. Cele te osiąga się poprzez realizację takich zadań, jak: zapewnienie adekwatnej ochrony posiadanych zasobów informacyjnych oraz ochrony przed wrogimi działaniami dezinformacyjnymi i propagandowymi (w wymiarze defensywnym) przy jednoczesnym zachowaniu zdolności do prowadzenia wobec ewentualnych przeciwników (państw lub innych podmiotów) działań ofensywnych w tym obszarze[36].

Zagrożenia dla bezpieczeństwa informacyjnego

W kontekście powyższych rozważań można zatem stwierdzić, iż zagrożeniem dla bezpieczeństwa informacyjnego podmiotu jest każde naruszenie atrybutów informacji w taki sposób, iż nie może on wypełniać swoich funkcji. Stąd też katalog zagrożeń dla bezpieczeństwa informacyjnego państwa (podmiotu) jest niezwykle obszerny. Co więcej, z uwagi na nieustanny rozwój technologii informacyjnych, próby stworzenia zamkniętego katalogu takich zagrożeń należy z góry uznać za pozbawione szans powodzenia – każda bowiem innowacja technologiczna, szczególnie niosąca ze sobą przełomowe znaczenie dla przekazu i przetwarzania informacji, niesie ze sobą nowe jakościowo zagrożenia. Za tego rodzaju przełomy należy np. uznać powstanie ogólnodostępnych mediów masowych, dzięki którym – poza ewidentnymi pozytywami – możliwa stała się dezinformacja i manipulacja na skalę masową. Podobny charakter nosi powstanie internetu jako powszechnie dostępnej platformy komunikacyjnej, której cechą charakterystyczną jest interaktywność, a więc możliwość nie tylko dostępu do informacji, lecz także jej tworzenia i rozpowszechniania.

Generalnie rzecz biorąc, za podstawowe zagrożenia dla bezpieczeństwa informacyjnego należy uznać:

[36] https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf (dostęp: 3.03.2016).

- brak dostępu do informacji (pustka informacyjna);
- nadmiar informacji (szum informacyjny);
- dostęp do informacji fałszywej i dezinformacji;
- brak ochrony własnych zasobów informacyjnych;
- brak kontroli nad własnymi kanałami informacyjnymi.

Część z tych zagrożeń nosi charakter obiektywny, część zaś jest konsekwencją słabości państwa i jego struktur w infosferze. Trudno bowiem ograniczyć ilość informacji w sposób mechaniczny, redukując szum informacyjny wyłącznie ilościowo; w warunkach społeczeństwa demokratycznego nie sposób także wprowadzić kontroli państwa nad wszystkimi kanałami informacyjnymi, oznaczałoby to *summa summarum* wprowadzenie cenzury prewencyjnej.

Z drugiej strony, brak dostępu do informacji o otoczeniu wynika ze słabości państwa, np. złej pracy służb wywiadowczych i dyplomatycznych. Z kolei brak należytego zabezpieczenia informacji własnych powoduje, że państwo nie jest zdolne do zachowania w tajemnicy tych informacji, które z różnych powodów chce ukryć przed potencjalnym przeciwnikiem. Wreszcie słabością państwa jest niezdolność do przeciwdziałania wrogim akcjom propagandowym czy dezinformacyjnym. W tym kontekście za słabość państwa należy uznać np. brak ośrodków analitycznych, czyli brak zdolności do analizy informacji[37].

Piotr Bączek wśród podstawowych zagrożeń dla bezpieczeństwa informacyjnego państwa wymienia:

- nieuprawnione ujawnienia informacji, które może nosić charakter pomyłkowy, polityczny lub komercyjny (sprzedaż informacji);
- naruszenia przez władze praw obywatelskich (ograniczanie jawności życia publicznego, naruszenia prywatności);
- asymetrię w międzynarodowej wymianie informacji (związaną z nierównoprawną wymianą informacji pomiędzy państwami sojuszniczymi);
- działalność grup świadomie manipulujących przekazem informacji (czego przykładem mogą służyć różnego rodzaju sekty);
- niekontrolowany rozwój technologii bioinformatycznych (np. w postaci uzyskania zdolności manipulacji procesami zachodzącymi w ludzkim mózgu);
- przestępczość komputerową;
- cyberterroryzm;
- samą walkę informacyjną;

[37] Zob. T. Aleksandrowicz, *Podstawy…*, s. 120.

- zagrożenia asymetryczne;
- szpiegostwo[38].

Znacznie szerszy i bardziej szczegółowy katalog zawiera przywołany powyżej projekt Doktryny Bezpieczeństwa Informacyjnego RP, ukazujący je w wymiarze wewnętrznym i zewnętrznym. Przede wszystkim projekt stwierdza, że 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 wyrwanie z kontekstu fragmentów wypowiedzi polityków RP, nadawanie im kontrowersyjnego charakteru).

Typizując zagrożenia w obszarze wewnętrznym, projekt dzieli je na zagrożenia związane z niedoskonałym funkcjonowaniem społeczeństwa obywatelskiego, zagrożenia związane z funkcjonowaniem w cyberprzestrzeni i przestrzeni medialnej oraz – jako wyodrębniony punkt – zagrożenia związane z eksploatowaniem drażliwych kwestii w kontaktach międzynarodowych, w tym bilateralnych, przy wykorzystaniu wsparcia określonych podmiotów i osób.

Projekt w szczególności wskazuje, że występowanie w społeczeństwie deficytów informacyjnych powoduje podatność na dezinformację i ułatwia funkcjonowanie agentury wpływu. Za szczególnie istotne należy uznać zagrożenia w cyberprzestrzeni (także w kontekście mediów społecznościowych), a więc dezinformację, trolling, wrogą propagandę, (zakłócające realizację istotnych zadań administracji publicznej oraz sektora prywatnego); ataki powodujące zakłócenia funkcjonowania sieci teleinformatycznych w sektorach i instytucjach o podwyższonym stopniu wrażliwości, w tym tworzących infrastrukturę krytyczną; istnienie technologicznych luk, które dają szansę, także niezauważonej, ingerencji w treść portali internetowych oraz wpływania na zdolności do działania w cyberprzestrzeni.

Ponadto twórcy projektu zakładają możliwość – w związku z funkcjonowaniem RP w globalnej cyberprzestrzeni – pojawienia się zagrożeń w postaci ataków cybernetycznych na instytucje rządowe, pozarządowe i kulturalne kształtujące świadomość narodową lub blokady rządowego przekazu informacji wskutek ataków cybernetycznych. W projekcie podkreśla się, że poważnym zagrożeniem są niepożądane, zewnętrzne oddziaływania informacyjne, mogące dotyczyć procedur sterowania procesami

[38] P. Bączek, *Zagrożenia informacyjne…*, s. 85 i n.

decyzyjnymi państwa, na które ukierunkowany jest atak informacyjny. 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.

Wnioski

Uzależnienie współczesnego państwa od sprawnie działającego systemu pozyskiwania, przetwarzania i dystrybucji informacji, także w postaci zdigitalizowanej, jest faktem. Pojęcie bezpieczeństwa informacyjnego państw należy zatem rozumieć szeroko; jego zakres przedmiotowy obejmuje zdolność do pozyskiwania informacji, jej analizowania, dystrybucji, ochrony własnych zasobów informacyjnych, a także zdolności do identyfikowania i skutecznego przeciwdziałania skutkom wrogich operacji informacyjnych mających na celu uzyskanie wpływu na politykę państwa, nastroje społeczne etc. W szczególności dotyczy to także informacji funkcjonującej w cyberprzestrzeni.

Pojęcie bezpieczeństwa informacyjnego państwa wiąże się zatem nierozłącznie z walką informacyjną, a więc taką, w której informacja jest zarówno bronią, jak i celem ataku. Wymaga to zatem posiadania przez państwo zdolności defensywnych (ochrona własnych zasobów informacyjnych i systemów informacyjnych), jak też ofensywnych (zdolność do prowadzenia własnych operacji informacyjnych i dezinformacyjnych). Zagrożenia dla bezpieczeństwa informacyjnego państwa wiążą się z atrybutami informacji, bowiem ich naruszenie powoduje, że informacja staje się np. niepełna lub nieprawdziwa, a zatem nie może wypełniać skutecznie swojej roli.

Streszczenie

Artykuł jest poświęcony kwestii bezpieczeństwa informacyjnego państwa. Autor analizuje w tym kontekście atrybuty i funkcje informacji stwierdzając, iż modyfikacje atrybutów informacji powodują, że nie może ona spełniać prawidłowo swoich funkcji. Pojęcie bezpieczeństwa informacyjnego państwa jest nierozłącznie związane z walką informacyjną, Wymaga to zatem posiadania przez państwo zdolności defensywnych (ochrona własnych zasobów informacyjnych i systemów

informacyjnych), jak też ofensywnych (zdolność do prowadzenia własnych operacji informacyjnych i dezinformacyjnych).

Tomasz R. Aleksandrowicz

Information Security of the Republic of Poland

This article deals with issue of information security of the state. The author analyzes in this context the attributes and functions of the information stating that the modification of information's attributes causes that it can not fulfill its functions properly. This requires the state to have defensive capabilities (protecting its own information and information systems) as well as offensive (the ability to carry out its own information and disinformation operations).

Key words: *state security, information, information security*

Bibliografia

Dokumenty

i2010 – Europejskie społeczeństwo informacyjne na rzecz wzrostu i zatrudnienia, Komunikat Komisji Wspólnot Europejskich do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów. Bruksela, dnia 1.6.2005 COM(2005) 229 końcowy, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:PL:PDF (dostęp: 5.04.2012).

Projekt doktryny bezpieczeństwa informacyjnego RP, https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf (dostęp: 3.03.2016).

Publikacje zwarte

Aleksandrowicz T., *Komentarz do ustawy o dostępie do informacji publicznej*, wyd. 4, Warszawa 2008.

Aleksandrowicz T., *Podstawy walki informacyjnej*, Warszawa 2016.

Aleksandrowicz T., *Świat w sieci. Państwa – społeczeństwa – ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*, Warszawa 2014.

Balcerowicz B., *Siły zbrojne w czasie pokoju, kryzysu i wojny*, Warszawa 2010.

Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń 2005.

Fehler W., *Bezpieczeństwo współczesnej Polski. Aspekty teoretyczne i praktyczne*, Warszawa 2012.

Jemioło T., Sienkiewicz P. (red.), *Zagrożenia dla bezpieczeństwa informacyjnego państwa. Identyfikacja, analiza zagrożeń i ryzyka. Tom I – Raport z badań*, Warszawa 2004.

Korzeniowski L.F., *Podstawy nauk o bezpieczeństwie*, Warszawa 2012.

Korzeniowski L.F., *Podstawy nauk o bezpieczeństwie*, wyd. 2, Warszawa 2017.

Levinson P., *Miękkie ostrze, czyli historia i przyszłość rewolucji informacyjnej*, Warszawa 2006.

Liderman K., *Bezpieczeństwo informacyjne*, Warszawa 2012.
Liedel K., *Bezpieczeństwo informacyjne państwa*, [w:] Liedel K. (red.), *Transsektorowe obszary bezpieczeństwa narodowego*, Warszawa 2011.
Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń dla bezpieczeństwa narodowego*, Toruń 2008.
Liedel K., Serafin T., *Otwarte źródła informacji w działalności wywiadowczej*, Warszawa 2011.
Liedel K., *Zarządzanie informacją w walce z terroryzmem*, Warszawa 2010.
Madej M., *Rewolucja informacyjna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, [w:] Madej M., Terlikowski M. (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009.
Nowak A., Scheffs W., *Zarządzanie bezpieczeństwem informacyjnym*, Warszawa 2010.
Nowak E., Nowak M., *Zarys teorii bezpieczeństwa narodowego*, Warszawa 2011.
Potejko P., *Bezpieczeństwo informacyjne* [w:] Wojtaszczyk K.A., Materska-Sosnowska A. (red.), *Bezpieczeństwo państwa*, Warszawa 2009.
Sienkiewicz P., *Wizje i modele wojny informacyjnej*, http://winntbg.bg.agh.edu.pl/skrypty2/0095/373-378.pdf (dostęp: 5.04.2012).
Słownik łacińsko – polski w opracowaniu Kazimierza Kumanieckiego, Warszawa 1975.

Artykuły w czasopismach:

Fehler W., *Informacyjny wymiar zagrożeń dla współczesnej Polski*, „Przegląd Strategiczny" 2015, nr 8.
Więcaszek-Kuczyńska L., *Zagrożenia bezpieczeństwa informacyjnego*, „Obronność. Zeszyty Naukowe" 2014, nr 2(10).
Żebrowski A., *Bezpieczeństwo informacyjne Polski a walka informacyjna*, „Roczniki Kolegium Analiz Ekonomicznych" 2013, nr 29.