Andrzej Skwarski*
Przemysław Szkudlarek
*ORCID: 0000-0001-8961-7098
Akademia im. Jakuba z Paradyża
w Gorzowie Wielkopolskim

Rola informacji i zagrożenia dezinformacją w systemie bezpieczeństwa państwa

Streszczenie

Problem natłoku informacyjnego ma w dzisiejszym świecie ogromne znaczenie. Informacja jest przedmiotem handlu, a w wielu przypadkach staje się walutą. Poważnym wyzwaniem jest ochrona informacji istotnych z punktu widzenia jednostki, przedsiębiorstwa czy też całego państwa. Wraz ze wzrostem znaczenia informacji pojawiło się zjawisko dezinformacji stanowiące zagrożenie dla wymienionych powyżej podmiotów.

Celem artykułu jest próba zdefiniowania informacji oraz dezinformacji, oraz przedstawienie ich roli w systemie bezpieczeństwa państwa. Ponadto wskazano nowe formy zagrożeń dezinformacyjnych. W celu precyzyjnego omówienia podjętego problemu zwrócono się o pomoc do ekspertów z dziedziny ochrony informacji oraz przeciwdziałania dezinformacji z pytaniami zawartymi w wywiadzie eksperckim.

Słowa kluczowe: informacja, dezinformacja, system bezpieczeństwa państwa

1. Definicje i funkcje informacji

Informacja jest pojęciem interdyscyplinarnym oraz złożonym. Od wieków badacze różnych dziedzin naukowych definiują informację w przeróżny sposób. Termin ten niesie ze sobą ogrom koncepcji oraz teorii, łącząc i przeplatając ze sobą wszystkie znane nam dyscypliny naukowe. Mechanika kwantowa, filozofia, historia, psychologia, teoria komunikacji, biologia molekularna, teoria systemów, informatyka, cybernetyka – to tylko niektóre z nich. Do dziś nie udało się nikomu zdefiniować informacji w taki sposób, by ująć wszystkie obszary, w których informacja występuje[1]. Jest to

[1] https://encyklopedia.pwn.pl/haslo/informacja;3914686.html [dostęp: 10.05.2020].

całkiem logiczne, gdyż informacja jest nierozerwalnym i nieodłącznym elementem naszego życia. Z tego powodu bardzo trudno jest odszukać wspólną wykładnię co do interpretacji informacji. Dzięki niej podejmujemy próbę poznania i zrozumienia otaczającego nas świata. Bogdan Stefanowicz twierdzi, że informacja funkcjonuje, jako dokładne odbicie rzeczywistości, dokonując podziału na wszystkie zjawiska i procesy, jakie w niej zachodzą, obiekty, jakie w niej funkcjonują oraz zdarzenia, które w tej rzeczywistości zachodzą[2]. W ujęciu filozoficznym informacja to odwzorowanie zróżnicowania rzeczywistości. Juliusz Kulikowski twierdzi, że wszystkie obiekty istniejące w rzeczywistości, funkcjonują na zasadzie wzajemności, zawierają informację oraz są różnorodne. Informacja jest właśnie tą wspomnianą przez niego różnorodnością[3]. Natomiast w chemii i fizyce informacją jest struktura materii lub niemożność jej określenia. W biologii będzie to zbiór sygnałów werbalnych i niewerbalnych wysyłanych i odbieranych przez obiekty. W psychologii bodźce, jakie człowiek odbiera z otaczającej go rzeczywistości. Informacja występuje wszędzie tam, gdzie pojawia się odrębność czy zróżnicowanie, przy czym warunkiem jest pojawienie się obserwatora oraz obserwowanego. Poniżej kilka opinii wyrażonych przez specjalistów przeróżnych dziedzin.

- Według Norberta Wienera (matematyka i pioniera cybernetyki) informacją jest nazewnictwo treści, które pojawiają się podczas naszej interakcji z rzeczywistością. Warto tu nadmienić, że interakcja ta zachodzi nieustannie w trakcie trwania naszego życia, a jej celem jest adaptacja nas samych oraz naszych zmysłów poznawczych do rzeczywistości[4].
- Glynn Harman w swojej publikacji opisuje informację jako wiązkę energii, funkcjonującą we wszystkich systemach naturalnych lub sztucznych, która organizuje całość tej energii bądź większe jej ilości[5].
- Elżbieta Niedzielska polska specjalistka w dziedzinie informatyki określa informację jako szczególny rodzaj dobra niematerialnego, które stale zwiększa swoją istotność oraz modeluje gospodarki w wyniku rozwoju form i środków komunikacji[6].

Powyższy przegląd opinii bardzo dobrze obrazuje bogactwo wypowiedzi na temat informacji wynikającej ze złożoności tego terminu. Wspólnym akcentem

---

[2] B. Stefanowicz, *Informacja. Wiedza. Mądrość*, Główny Urząd Statystyczny, Warszawa 2013, s. 8.
[3] J. L. Kulikowski, *Informacja i świat, w którym żyjemy*, Warszawa 1978, s. 44.
[4] N. Wiener, *The Human Use of Human Beings*, Nowy Jork 1954, s. 17.
[5] G. Harmon, *Computer Development and Information Management, in The Next 200 Years. Programs 48-84 and 49-84*, Teksas 1984, s. 193.
[6] E. Niedzielska, *Komunikacja gospodarcza w złożonych systemach informacyjnych*, Wrocław 1988, s. 20.

przytoczonych definicji jest obserwator, który odbiera i przetwarza płynące z otoczenia informacje, zachodzące zjawiska oraz ich cechy. Obserwatorem może być zarówno człowiek, jak i różnego rodzaju systemy, w tym systemy informacyjne, w których wykorzystuje się środki informatyczne dla usprawniania przepływu informacji oraz wszystkich procesów z nią związanych. Należy tu nadmienić, że niezbywalną właściwością informacji jest fakt, że jest ona zależna od obserwatora, zarówno od jego opinii, poglądów, jak i jego woli czy celów. Tak jak efekt obserwatora i klasyczny już paradoks kota Schrödingera[7].

Demokracja to ustrój, który konstytucyjnie gwarantuje prawa i swobody obywatelskie wszystkim obywatelom danego państwa w ramach wspólnego kształtowania organizacji politycznych, społecznych czy zasad regulujących jego funkcjonowanie. Wymienić tu należy oddziaływanie i kontrolowanie organów władzy, czynny udział w życiu gospodarczym państwa czy nieograniczony dostęp do kultury, nauki i oświaty. Swobodny przepływ i dostęp do informacji warunkuje wzrost rozwoju danego państwa. Pozwala to obywatelom oceniać każdy jego aspekt i śledzić na bieżąco wydarzenia w życiu danego państwa. Do rzetelnej opinii potrzeba wiarygodnej wiedzy o działaniach władz i ich skutkach. Teoretyzując, demokratyczny ustrój liczy się ze zdaniem wszystkich obywateli. Poprzez nieskrępowany dostęp i na podstawie informacji społeczeństwo podejmuje świadomą decyzję podczas wyborów, oddziaływując na układ sił parlamentu. Stefan Garczyński słusznie zauważył, że informacja jest czynnikiem decydującym w aspekcie rzetelności demokracji[8]. Bez podstawowej wiedzy na temat podejmowanych decyzji, współudział jednostki w tworzeniu systemu (w tym przypadku państwa) jest pozorny. Współdecydowanie obywateli czy *de facto* współrządzenie państwem bez powszechnego dostępu do informacji nie ma prawa zaistnieć, nie wspominając już o umiejętnościach interpretacji, analizy, czerpania z informacji przy jednoczesnej aktywnej, niezależnej i obiektywnej ocenie władz. Bardzo intrygującą oraz logicznie spójną tezą jest twierdzenie, że ustrój demokratyczny krajów europejskich zrodził się właśnie poprzez informację. Wszakże informacja o dążeniach niepodległościowych Ameryki Północnej czy ruchy rewolucyjne francuskiego społeczeństwa poprzez niezwykle silny symbol zburzenia bastylii jako ten czynnik sprawczy pchnęła ludy Europy do rozważań oraz przewartościowania światopoglądu w obszarach takich jak życie społeczne i jego zasady, wolność obywatelska, sprawiedliwość.

[7] Eksperyment myślowy przeprowadzony przez austriackiego fizyka Erwina Schrodingera.
[8] S. Garczyński, *Z informacją na bakier*, Warszawa 1981, s. 12.

Spośród ogromnego zbioru, autorzy przytoczyli tylko kilka funkcji, jakie spełnia informacja. Wymienione przez autorów funkcje skłaniają do refleksji na temat ogromnej odpowiedzialności uczestników obiegu informacji w każdym systemie informacyjnym. Wszakże każdy funkcjonujący system informacyjny jest niezwykle newralgiczny w swojej istocie oraz funkcjonalności zarówno w wymiarze czysto technicznym, jak i ludzkim. Odpowiedzialność ta bez względu na świadomość bądź jej brak uczestników wymiany informacji o wieloaspektowości każdej wysyłanej i przyjmowanej wiadomości prowadzi do wniosków, że wszyscy uczestnicy muszą chronić informację i zapewniać jej jakość. Ma to szczególne znaczenie, gdy uczestnicy obiegu korzystają ze zdobyczy oraz osiągnięć nowoczesnych technologii, które usprawniają przekazywanie informacji.

2. Informacja i dezinformacja w systemie bezpieczeństwa państwa

Współcześnie informacja pełni nadzwyczaj istotną rolę. Rozwój technologiczny oraz cywilizacyjny podnosi jej znaczenie. Rewolucja technologiczna całkowicie odmieniła sposoby komunikacji społeczeństw, a rozwój technologii daje nam dostęp do coraz efektywniejszych narzędzi komunikacji. Wraz z rozwojem pojawiają się nowe formy zagrożeń oraz nowe sposoby przechwytywania informacji istotnych i newralgicznych, z punktu widzenia funkcjonowania państwa oraz obywatela. To niejako wymusza na organach i instytucjach publicznych kreowanie nowych rozwiązań w obszarze ochrony informacji oraz sposobów reagowania na zagrożenia, w celu zapewnienia wysokiego poziomu bezpieczeństwa oraz ciągłości funkcjonowania państwa.

Wszelkie instytucje oraz organy zajmujące się na co dzień bezpieczeństwem gromadzą i przetwarzają informację. Na wstępie warto zaznaczyć, że to właśnie od jej jakości i szybkości przepływu zależy funkcjonowanie służb publicznych. To w konsekwencji przekłada się na funkcjonowanie systemu bezpieczeństwa państwa oraz na poziom tego bezpieczeństwa. Szybki przepływ informacji, odpowiednie jej zabezpieczenie poprzez bezpieczne przechowywanie czy przesył, jej trafność w kontekście danej sytuacji oraz wysoki jej poziom w ujęciu jakościowym pozwalają podnosić poziom bezpieczeństwa. Odpowiednie wykorzystanie informacji podczas reagowania na zagrożenia umożliwia skutecznie przeciwdziałać tym zagrożeniom.

Strefa Schengen jest obszarem Unii Europejskiej, w którym kontrola na granicach wewnętrznych została zniesiona. Po wejściu w życie Strefa Schengen stała się jednym z najbardziej widocznych sukcesów postępującej integracji państw

europejskich. Układ został powołany w roku 1995, w obszarze jego obowiązywania zniesiono kontrole paszportowe, a swobodne poruszanie się w obrębie państw sygnatariuszy stało się rzeczywistością. Ma to bezpośrednie przełożenie na rozpoczęcie wielu ciekawych interakcji społeczeństw w obrębie państw członkowskich. Mieszkańcy strefy Schengen mogą żyć, uczyć się, pracować czy pobierać emeryturę w dowolnym miejscu Unii Europejskiej. W strefie Schengen znajduje się obecnie 26 państw, 22 państwa członkowskie Unii oraz cztery państwa spoza niej[9]. System Informacyjny Schengen (SIS)[10] jest najczęściej stosowanym oraz największym systemem wymiany informacji. Został opracowany w celu zapewniania bezpieczeństwa oraz zarządzania granicami Europy. SIS zapewnia właściwym organom państw członkowskich, takim jak policja czy straż graniczna, dostęp do bazy danych oraz jej edycję, poprzez wprowadzanie wpisów odnoszących się do osób lub przedmiotów. Wpis w bazie SIS zawiera nie tylko informacje o konkretnej osobie bądź przedmiocie, ale także szczegółowe wytyczne, jak postępować, gdy dana osoba bądź przedmiot zostaną zidentyfikowane. Specjalnie utworzone na terenie każdego państwa członkowskiego biura SIRENE służą jako punkty kontaktowe do wymiany informacji uzupełniających oraz do koordynacji działań podejmowanych w związku z wpisami w SIS. W końcówce 2017 roku System Informacyjny Schengen zawierał około 77 milionów wpisów. Do wpisów uzyskano dostęp 5,2 miliarda razy, z czego około 244 tysiące wpisów zostało potwierdzonych przez służby ścigania. Głównym celem Systemu Informacyjnego Schengen jest zwiększenie poziomu bezpieczeństwa na terenie Europy. System jest wykorzystywany jako narzędzie pomocnicze przez właściwe organy w celu zachowania bezpieczeństwa wewnętrznego.

Ochrona granic państw członkowskich zarówno zewnętrznych, jak i wewnętrznych jest bardzo istotna w aspekcie zapewniania bezpieczeństwa. Zwiększona migracja, a także wzrost poziomu zagrożenia bezpieczeństwa w związku z terroryzmem czy przestępczością transgraniczną niejako wymuszają na państwach członkowskich reakcję. Stały rozwój technologii, a także organizowanie się grup przestępczych, które prowadzą swoje nielegalne biznesy na terenach przygranicznych Unii zarówno zewnętrznych, jak i wewnętrznych, wymaga od instytucji Unijnych stałej adaptacji do zmieniającej się rzeczywistości. Oprócz adaptacji niezwykle istotnym jest zapewnienie sprawnego i nieprzerwanego funkcjonowania jednolitego systemu organizacyjnego. Ustanowienie przejrzystego systemu kierowania

[9] https://www.europarl.europa.eu/news/pl/headlines/security/20190612STO54307/strefa-schengen-wszystko-co-musisz-wiedziec-o-europejskiej-strefie-bez-granic [dostęp: 24.01.2020].

[10] https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en [dostęp: 24.01.2020].

oraz zaangażowania państw członkowskich w obecne i przyszłe wspólne operacje. Świetnym przykładem takiej reakcji jest obecna sytuacja na granicy grecko-tureckiej, gdzie siły porządkowe Turcji wspierają migrantów chcących nielegalnie przekroczyć granicę zewnętrzną Unii Europejskiej. Błyskawiczna reakcja państw członkowskich, tj. Polski, Austrii, Czech, Węgier oraz Słowacji pozwoliła na czasowe powstrzymanie nielegalnej migracji[11]. Rozwój współpracy oraz rozszerzanie kompetencji w ramach systemu informacyjnego Schengen, prowadzi do szybszej i stanowczej reakcji w obliczu zagrożeń. Prowadzi to do wzrostu bezpieczeństwa, dlatego autorzy w pełni zgadzają się i popierają wszelkie inicjatywy, takie jak nowa, trzecia już generacja SIS-u, która wejdzie w życie w 2021 roku, System informacji wizowej (VIS), System wjazdu i wyjazdu funkcjonujący na granicach Schengen (EES), Europejska Agencja Straży Granicznej i Przybrzeżnej (Frontex). Dodatkowymi inicjatywami, które podejmowane są w celu ochrony granic zewnętrznych Unii Europejskiej oraz zwiększania bezpieczeństwa, są rozszerzanie stanu osobowego korpusu funkcjonariuszy Europejskiej Straży Granicznej do 10 tysięcy, a także ETIAS – europejski system informacji o podróży[12].

Opisane przez autorów systemy to tylko niektóre z całej gamy wykorzystywanych przez ograny państwowe. Wraz ze wzrostem znaczenia informacji pojawiają się nowe formy zagrożeń, takie jak: cyberszpiegostwo czy cyberwywiad. Zagrożenia te mogą bardzo mocno infiltrować administrację publiczną i system bezpieczeństwa państwa. Dlatego instytucje publiczne i te powołane do ochrony bezpieczeństwa powinny rozwijać systemy zabezpieczeń oraz systemy komunikacji, które będą skutecznie chroniły przed zagrożeniami oraz ułatwiały przekazywanie informacji.

3. Współczesne wyzwania i zagrożenia bezpieczeństwa państwa w wymiarze informacji i dezinformacji

Dla osiągnięcia założonego celu badawczego przeprowadzono badania w postaci wywiadu eksperckiego. Przedmiotem badań byli eksperci, którzy posiadają wieloletnie doświadczenie w pracy z informacją i dezinformacją. Doświadczenie to wynika z faktu, iż pracują oni od wielu lat w newralgicznych instytucjach publicznych, które na co dzień pozyskują i analizują informację oraz przeciwdziałają dezinformacji.

[11] https://infosecurity24.pl/frontex-na-poczatku-przyszlego-tygodnia-rozpocznie-operacje-na-greckiej-granicy [dostęp: 29.03.2020].
[12] Ibidem, [dostęp: 24.01.2020].

Cel badania

Głównym celem badań było poszerzenie świadomości czytelników tej pracy w aspekcie dezinformacji i informacji. By tego dokonać, w części teoretycznej dokonano analizy literatury, natomiast w części badawczej przeprowadzono wywiad ekspercki. Uznano, że metoda wywiadu eksperckiego efektywnie i szczegółowo pomoże zrealizować cel badania. Przemawia za tym fakt, iż czytelnicy pracy mogą szerzej zapoznać się z opiniami ekspertów, którzy na co dzień mają styczność z omawianymi terminami na poziomie znacznie wyższym niż obywatel. Autorzy mają tu na myśli, że eksperci pracują w organach państwowych. Co za tym idzie, zarówno informacja, jak i dezinformacja, która pojawia się w ich pracy, mają wpływ na funkcjonowanie państwa.

Hipoteza

Wraz ze wzrostem znaczenia informacji rozwija się zjawisko dezinformacji. Innymi słowy występuje korelacja pomiędzy tymi dwoma terminami. W związku z tym konieczna jest edukacja na szeroką skalę w aspekcie tych terminów. Podniesie ona poziom świadomości społeczeństwa i będzie miała bezpośredni wpływ na poziom bezpieczeństwa państwa.

Pytania badawcze

Aby zrealizować powyższy cel badania oraz udzielić odpowiedzi na powyższą hipotezę postawiono następujące pytania badawcze:

a) odnośnie terminu informacja:
   - Jak Pan/Pani ocenia wagę/znaczenie informacji w aspekcie funkcjonowania instytucji publicznych?,
   - Jak Pan/Pani ocenia zmiany technologiczne odnośnie form przekazywania informacji w aspekcie systemu bezpieczeństwa państwa?,
   - Jaka jest według Pana/Pani najbardziej pozytywna cecha informacji w aspekcie systemu bezpieczeństwa państwa?,
   - Jaka jest według Pana/Pani najbardziej negatywna cecha informacji w aspekcie systemu bezpieczeństwa państwa?;

b) odnośnie terminu dezinformacja:
   - Jak Pan/Pani ocenia poziom oddziaływania dezinformacji na struktury państwowe(czy zjawisko występuje, jeśli tak, to jak intensywnie?)?,
   - Gdzie według Pana/Pani system bezpieczeństwa państwa jest najbardziej narażony na dezinformację [komponent/element systemu lub proces (pozyskiwania, przetwarzania, wymiany lub analizy informacji)]?,

- Które według Pana/Pani podmioty państwowe funkcjonujące na arenie międzynarodowej najbardziej aktywnie wykorzystują dezinformację do realizacji celów oraz zabezpieczenia żywotnych interesów narodowych?,
- Proszę o podanie według Pana/Pani przyszłych szans i zagrożeń w zakresie dezinformacji.

Metoda gromadzenia materiału badawczego.

Do zgromadzenia materiału badawczego wykorzystano wywiad ekspercki.

Materiał badawczy.

Materiałem badawczym są odpowiedzi ekspertów na zadane przez autora pracy pytania.

Ekspert numer 1

Wieloletni pracownik instytucji prowadzących czynności operacyjno-rozpoznawcze oraz zajmujących się pozyskiwaniem i analizą informacji wrażliwych z punktu widzenia interesu państwa. Autor posiada od wielu lat poświadczenie bezpieczeństwa na dostęp do informacji o najwyższych klauzulach zarówno krajowych, jak i UE oraz NATO.

INFORMACJA:

Pyt.: Jak Pan/Pani ocenia wagę/znaczenie informacji w aspekcie funkcjonowania instytucji publicznych?

Odp.: Znaczenie informacji dla funkcjonowania instytucji publicznych jest niezwykle istotne zarówno z punktu widzenia bezpieczeństwa tych podmiotów, jak i skuteczności ich działania. W zależności od charakteru danej instytucji informacja może być jej produktem oraz swoistym „surowcem" poddanym analizie prowadzącej do opracowania informacji według ściśle określonych zasad.

Pyt.: Jak Pan/Pani ocenia zmiany technologiczne odnośnie form przekazywania informacji w aspekcie systemu bezpieczeństwa państwa?

Odp.: Nastąpiły ogromne zmiany technologiczne w zakresie przetwarzania, przesyłania oraz przechowywania i udostępniania informacji. Należy zwrócić uwagę na możliwości bezpiecznego przesyłania informacji po ich zaszyfrowaniu, szczególnie asymetrycznym, co daje duże poczucie bezpieczeństwa odnośnie możliwości ich utracenia. Ponadto postęp nastąpił również w zakresie możliwości przetwarzania oraz przechowywania informacji w dużych ilościach tzw. big data.

Pyt.: Jaka jest według Pana/Pani najbardziej pozytywna cecha informacji w aspekcie systemu bezpieczeństwa państwa?

Odp.: W mojej opinii najbardziej pozytywną cechą informacji jest jej prawdziwość oraz aktualność, ponieważ prowadzi do niezakłóconego jej przetwarzania oraz wykorzystania.

Pyt.: Jaka jest według Pana/Pani najbardziej negatywna cecha informacji w aspekcie systemu bezpieczeństwa państwa?

Odp.: W tym przypadku odwróciłbym odpowiedź na pytanie nr 3. Największym zagrożeniem jest fałszywość informacji oraz brak weryfikacji tego. Również informacja prawdziwa, lecz zdezaktualizowana nie posiada takiej wartości, jak ta posiadająca aktualność.

DEZINFORMACJA:

Pyt.: Jak Pan/Pani ocenia poziom oddziaływania dezinformacji na struktury państwowe (czy zjawisko występuje, jeśli tak, to jak intensywnie?)?

Odp.: W ostatnich latach nastąpił lawinowy wzrost ataków dezinformujących na struktury państwowe. Należy postrzegać je jako niezwykle groźne i niebezpieczne dla struktur państwa, a nawet całych bloków państw zgromadzonych wokół wspólnych idei. Najgłośniejsze z ostatnich lat to dezinformacja społeczeństwa Wielkiej Brytanii podczas działań przedreferendalnych, dotyczących wyjścia tego kraju z Unii Europejskiej czy też mechanizmy wpływające na decyzje wyborców w USA przed wyborami prezydenckimi. Dodatkowym zagrożeniem jest często brak możliwości rozpoznania takiego procederu nawet po upływie odpowiednio długiego czasu.

Pyt.: Gdzie według Pana/Pani system bezpieczeństwa państwa jest najbardziej narażony na dezinformację [komponent/element systemu lub proces (pozyskiwania, przetwarzania, wymiany lub analizy informacji)]?

Odp.: W dobie, gdy informacja stała się najdroższym „produktem" trudno jest wskazać komponent lub element systemu najbardziej narażony na dezinformację, wszystkie są w podobnej sytuacji. Natomiast łatwiej jest dokonać oceny procesu pozyskiwania, przetwarzania, przekazywania oraz przechowywania informacji. Tutaj jako najbardziej podatny na dezinformację, w mojej opinii, jest proces pozyskiwania informacji, szczególnie w sytuacji, gdy proces ten odbywa się z pominięciem procedur bezpieczeństwa w tym zakresie. Chodzi tu o korzystanie z zaufanych źródeł czy wieloźródłowe jej potwierdzenie.

Pyt.: Które według Pana/Pani podmioty państwowe funkcjonujące na arenie międzynarodowej najbardziej aktywnie wykorzystują dezinformację do realizacji celów oraz zabezpieczenia żywotnych interesów narodowych?

Odp.: Sądzę że instytucjami najczęściej prowadzącymi ataki dezinformacyjne są służby wywiadowcze. W niektórych państwach, takich jak Rosja, tworzone są

specjalne podmioty posiadające możliwości techniczne oraz wsparcie państwa w zakresie przepisów prawa, a prościej mówiąc – ich braku, umożliwiające niezakłóconą możliwość takiego działania.

Pyt.: Proszę o podanie według Pana/Pani przyszłych szans i zagrożeń w zakresie dezinformacji.

Odp.: Ze względu na korzyści, jakie przynoszą tego typu ataki ich inspiratorom przy stosunkowo niewielkich nakładach finansowych oraz niewielkiej możliwości ich wykrycia przez stronę atakowaną, w najbliższej przyszłości ilość ich w mojej opinii będzie rosła. Z drugiej strony w ramach mechanizmów obronnych powstają narzędzia i procedury pozwalające coraz skuteczniej przeciwdziałać temu zjawisku. Dopóki nie zmieni się system stawiający informację niezwykle wysoko w hierarchii wartości będziemy mieli do czynienia z atakami dezinformacyjnymi.

Ekspert numer 2

Wieloletni pracownik instytucji prowadzących czynności operacyjno-rozpoznawcze oraz zajmujących się pozyskiwaniem i analizą informacji wrażliwych z punktu widzenia interesu państwa. Autor posiada od wielu lat poświadczenie bezpieczeństwa na dostęp do informacji o najwyższych klauzulach zarówno krajowych, jak i UE oraz NATO.

INFORMACJA:

Pyt.: Jak Pan/Pani ocenia wagę/znaczenie informacji w aspekcie funkcjonowania instytucji publicznych?

Odp.: Informacja w systemie bezpieczeństwa państwa stanowi podstawowy element funkcjonowania instytucji oraz kształtuje zadania, jakie instytucja realizuje.

Pyt.: Jak Pan/Pani ocenia zmiany technologiczne odnośnie form przekazywania informacji w aspekcie systemu bezpieczeństwa państwa?

Odp.: Bardzo dobrze oceniam zmiany technologiczne Pozwoliły one na szybsze przekazywanie informacji do instytucji. Na przykład aplikacja Krajowa Mapa Zagrożeń, pozwala w każdej chwili na przekazanie informacji o zagrożeniach, a instytucja (tut. Policja) reaguje na zdarzenie.

Pyt.: Jaka jest według Pana/Pani najbardziej pozytywna cecha informacji w aspekcie systemu bezpieczeństwa państwa?

Odp.: Prawda.

Pyt.: Jaka jest według Pana/Pani najbardziej negatywna cecha informacji w aspekcie systemu bezpieczeństwa państwa?

Odp.: Fałsz.

DEZINFORMACJA:

Pyt.: Jak Pan/Pani ocenia poziom oddziaływania dezinformacji na struktury państwowe (czy zjawisko występuje, jeśli tak, to jak intensywnie?)?

Odp.: Instytucje bezpieczeństwa korzystają z procedury oceny informacji i informatora (czterostopniowa skala). Najbardziej narażony na dezinformację jest obywatel.

Pyt.: Gdzie według Pana/Pani system bezpieczeństwa państwa jest najbardziej narażony na dezinformację [komponent/element systemu lub proces (pozyskiwania, przetwarzania, wymiany lub analizy informacji)]?

Odp.: W czynniku ludzkim.

Pyt.: Które według Pana/Pani podmioty państwowe funkcjonujące na arenie międzynarodowej najbardziej aktywnie wykorzystują dezinformację do realizacji celów oraz zabezpieczenia żywotnych interesów narodowych?

Odp.: Służba Wywiadu.

Pyt.: Proszę o podanie według Pana/Pani przyszłych szans i zagrożeń w zakresie dezinformacji.

Odp.: Tendencja wzrostowa.

Ekspert numer 3

Osoba z kilkudziesięcioletnim stażem w resorcie obrony narodowej. Autor posiada certyfikaty poświadczenia bezpieczeństwa na dostęp do informacji niejawnych UE i NATO. Posiada przeszkolenie w zakresie ochrony informacji niejawnych i przetwarzania danych osobowych. Studia podyplomowe z zakresu negocjacji, przywództwa i protokołu dyplomatycznego. Szef komórki wewnętrznej w instytucji resortu obrony narodowej.

INFORMACJA:

Pyt.: Jak Pan/Pani ocenia wagę/znaczenie informacji w aspekcie funkcjonowania instytucji publicznych?

Odp.: Informacja w działalności instytucji publicznych ma ogromne znaczenie. To na niej opiera się planowanie, działanie czy sprawozdawczość. Dzięki informacjom szefowie podejmują kluczowe decyzje, które mogą okazać się strategiczne dla przyszłości instytucji czy firmy. Rzetelność pozyskiwanych informacji uzależniona jest od osób, które je przekazują i analizują. Informacja, jak i dezinformacja, to groźna „broń" we współczesnym świecie. Umiejętnie wykorzystana może spowodować określone korzyści i przechylić szalę wygranej. W instytucjach pozyskiwanie i analizowanie informacji, powinno być realizowane przez wyspecjalizowane

komórki i osoby, które są fachowcami w swojej dziedzinie, potrafiącymi oddzielić informacje prawdziwe od *fake newsów*. Informacja w działalności instytucji publicznych ma ogromne znaczenie.

Pyt.: Jak Pan/Pani ocenia zmiany technologiczne odnośnie form przekazywania informacji w aspekcie systemu bezpieczeństwa państwa?

Odp.: Skok technologiczny pomaga w rozwoju ludności (krajów) na świecie. Informacje przekazywane są błyskawicznie do szerokiego grona odbiorców, co może stanowić zarówno korzyść, jak i zagrożenie. Wykorzystywanie nowinek technologicznych ma niebagatelny wpływ na pracę służb zabezpieczających bezpieczeństwo państwa. Umiejętność wykorzystania tego potencjału jest kluczowa dla osiągnięcia celu, jakim jest zagwarantowanie stabilnego i bezpiecznego państwa. Cyfryzacja to dzisiaj 99,9% przekazywania informacji. Zabezpieczenie się przed ingerencją potencjalnego przeciwnika (konkurenta) to zagwarantowanie sukcesu. Sposoby kodowania (szyfrowania) przekazywanych informacji wewnątrz organizacji (państwa) stanowią główne zadanie dla uchronienia się przed pozyskaniem wrażliwych informacji poza adresatami wiadomości. Korzystanie obecnie z nowoczesnych urządzeń bez odpowiednich zabezpieczeń jest łakomym kąskiem dla osób trudniących się pozyskiwaniem informacji. Zdalne skanowanie kart płatniczych, ściąganie obrazów, treści czy pieniędzy nie jest dzisiaj problemem dla wyszkolonych fachowców.

Pyt.: Jaka jest według Pana/Pani najbardziej pozytywna cecha informacji w aspekcie systemu bezpieczeństwa państwa?

Odp.: Najbardziej pozytywną cechą informacji w aspekcie bezpieczeństwa Państwa, według niektórych znawców tematu, jest jej szybkość przekazywania i wymiany, a co za tym idzie również weryfikacji.

Pyt.: Jaka jest według Pana/Pani najbardziej negatywna cecha informacji w aspekcie systemu bezpieczeństwa państwa?

Odp.: Najbardziej negatywną cechą informacji w aspekcie bezpieczeństwa Państwa jest jej podatność na przechwycenie i zniekształcenie, wykorzystując ją docelowo jako dezinformację.

DEZINFORMACJA:

Pyt.: Jak Pan/Pani ocenia poziom oddziaływania dezinformacji na struktury państwowe (czy zjawisko występuje, jeśli tak, to jak intensywnie?)?

Odp.: Dezinformacja w dzisiejszym świecie to największe wyzwanie w dobie cyfryzacji na poziomie krajowym i międzynarodowym. Z uwagi na szeroki horyzont zagrożeń płynących z dezinformacją, narażone mogą być błędnymi (nieprawdziwymi)

informacjami struktury państwa, instytucji i firm. Dezinformacja może wywierać negatywny wpływ na proces decyzyjny, a także prowadzić do niepokoi społecznych, destabilizacji ekonomicznej kraju (regionu) czy kulturowej (etnicznej).

Pyt.: Gdzie według Pana/Pani system bezpieczeństwa państwa jest najbardziej narażony na dezinformację [komponent/element systemu lub proces (pozyskiwania, przetwarzania, wymiany lub analizy informacji)]?

Odp.: Najbardziej zagrożonym komponentem w systemie bezpieczeństwa państwa jest komponent, który pozyskuje, analizuje, wymienia i przetwarza informacje (dezinformacje). Komponentami podatnymi mogą być służby odpowiedzialne za bezpieczeństwo państwa (ich serwery), media czy instytucje rządowe lub biznesowe (posiadające dane wrażliwe) mogące być ważnym elementem składowym w systemie bezpieczeństwa państwa.

Pyt.: Które według Pana/Pani podmioty państwowe, funkcjonujące na arenie międzynarodowej, najbardziej aktywnie wykorzystują dezinformację do realizacji celów oraz zabezpieczenia żywotnych interesów narodowych?

Odp.: Najbardziej aktywnymi podmioty państwowymi wykorzystującymi dezinformację działającymi na arenie międzynarodowej do realizacji celów zabezpieczenia żywotnych interesów państwa są służby wywiadu i kontrwywiadu. Mogą one wykorzystywać do realizacji swoich celów wykwalifikowane grupy ludzi, które w niejawny sposób wykonują zlecenia tych służb (np. opłacane farmy trolli internetowych). Szeroko wykorzystywana jest dezinformacja przez siły zbrojne, które w dzisiejszym świecie traktują dezinformację jako oręż strategiczną o silnej mocy oddziaływania.

Pyt.: Proszę o podanie według Pana/Pani przyszłych szans i zagrożeń w zakresie dezinformacji.

Odp.: Szansą na łagodzenie skutków dezinformacji (eliminacja raczej nie jest możliwa) jest docieranie do jej źródła (co jest raczej mało prawdopodobne) i weryfikowanie danych. Utrudnianie obcym osobom dostępu do naszych urządzeń poprzez instalowanie odpowiednich programów i częste zmienianie haseł (najlepiej niekojarzonych z naszą osobą).

Zagrożeniem natomiast jest niesłabnący popyt na urządzenia elektroniczne, które stanowią niewyczerpane źródło danych o nas. Zagrożeniem jest brak instalowania jakichkolwiek programów zabezpieczających nasze urządzenia przed ingerencją obcych ludzi oraz przede wszystkim podatność i łatwowierność ludzi na otrzymywane informacje, które szerokim strumieniem płyną w mediach społecznościowych.

4. Wyniki badań – Analiza materiału badawczego

INFORMACJA:

W pytaniu pierwszym eksperci zgodnie stwierdzili, iż informacja jest bardzo istotna z punktu widzenia systemu bezpieczeństwa państwa. Ekspert numer 1 zauważył, że informacja decyduje zarówno o bezpieczeństwie, jak i skuteczności instytucji. Ekspert numer 2 podkreślił, iż informacja jest podstawowym elementem instytucji oraz kształtuje jej zadania. Natomiast ekspert numer 3 stwierdził, że na informacji opiera się planowanie, działanie czy sprawozdawczość instytucji. Zwrócił uwagę na fakt, iż jej pozyskiwaniem i analizą powinny zajmować się wyspecjalizowane komórki. Analiza odpowiedzi pozwala na następujące wnioski: Informacja to czynnik, który kształtuje zarówno środowisko funkcjonowania instytucji, jak i ich zadania, w aspekcie celów statutowych (ustawowych). Informacja i jej znaczenie jest doceniana przez ekspertów.

W pytaniu drugim eksperci pozytywnie ocenili zmiany technologiczne. Warto tu nadmienić, iż eksperci po raz kolejny byli zgodni. Ekspert numer 1 zwrócił uwagę na fakt, iż nastąpiły ogromne zmiany technologiczne w zakresie przetwarzania, przesyłania, przechowywania oraz udostępniania informacji. Ekspert numer 2 wskazał na Krajową Mapę Zagrożeń jako przykład zmian technologicznych. Natomiast ekspert numer 3 zaakcentował, że zmiany technologiczne mają ogromny wpływ na funkcjonowanie służb odpowiedzialnych za bezpieczeństwo państwa. Zwrócił on uwagę na fakt, iż rozwój technologiczny niesie zarówno szanse, jak i zagrożenia. Podkreślił w swojej wypowiedzi znaczenie szyfrowania danych w aspekcie bezpieczeństwa, podobnie jak ekspert numer 1. Pozwala to na wyciągnięcie następujących wniosków: zmiany technologiczne, w aspekcie systemu bezpieczeństwa państwa są znaczące; zmiany te powodują skuteczniejsze funkcjonowanie systemu; w konsekwencji informacja staje się coraz ważniejszym elementem tego systemu.

Na pytanie trzecie ekspert numer 2 odpowiedział jednym słowem. Jasno stwierdził, iż prawdziwość informacji jest jej najbardziej pozytywną cechą. Natomiast ekspert numer 1 dodał do tej wypowiedzi słowo „aktualność". Warto nadmienić, iż eksperci jako odpowiedź wskazali tę samą cechę. Wprawdzie ekspert numer 3 określił szybkość przekazywania informacji jako najbardziej pozytywną cechę, jednakże zwrócił uwagę na fakt, iż szybkość wymiany informacji przekłada się na jej weryfikację. Czyli o prawdziwości informacji wypowiedział się w inny sposób. Możemy wyciągnąć następujące wnioski: Z punktu widzenia systemu bezpieczeństwa państwa prawdziwość informacji to jej najbardziej pożądana cecha. Prawdziwość

i aktualność pozyskiwanych oraz przetwarzanych informacji ma realny wpływ na funkcjonowanie systemu bezpieczeństwa państwa.

W pytaniu czwartym, analogicznie jak w pytaniu trzecim, eksperci wskazali na fałszywość informacji jako jej najbardziej negatywną cechę. Ekspert numer 1 ponownie odpowiedział jednym słowem. Z kolei ekspert numer 2 po raz kolejny dodał do tej wypowiedzi słowo „dezaktualizacja". Natomiast ekspert numer 3 wskazał podatność informacji na jej przechwycenie i zniekształcenie. Wnioski odnośnie tego pytania są odbiciem wniosków pytania poprzedniego. Mianowicie: dla funkcjonowania systemu bezpieczeństwa państwa najmniej pożądaną cechą informacji jest jej fałszywość; fałszywa informacja lub niezweryfikowana jej prawdziwość stanowi poważne zagrożenie systemu.

DEZINFORMACJA:

Pytanie pierwsze dotyczące dezinformacji sprawiło, iż po raz pierwszy eksperci nie byli zgodni w swoich odpowiedziach. Ekspert numer 2 wprawdzie nie zaprzeczył, że dezinformacja wobec struktur państwowych ma miejsce, jednak stwierdził, iż system bezpieczeństwa posiada odpowiednie zabezpieczenia w postaci weryfikacji informacji. Jednocześnie stwierdził, że to obywatele są najbardziej podatni na zjawisko dezinformacji. Ekspert numer 3 stwierdził, że dezinformacja jest największym wyzwaniem zarówno na poziomie krajowym, jak i międzynarodowym. Wymienił też kilka konsekwencji dezinformacji w różnych aspektach życia. Natomiast ekspert numer 1, podobnie jak ekspert numer 3, jednoznacznie stwierdził, iż w ostatnich latach dezinformacja na struktury państwowe znacząco wzrosła. Jako potwierdzenie swojej wypowiedzi wskazał przykłady ataków dezinformacyjnych podczas procesów wyborczych USA czy Wielkiej Brytanii. Analizując te wypowiedzi, możemy wyciągnąć następujące wnioski: dezinformacja jest zagrożeniem dla struktur państwowych i międzynarodowych; zjawisko dezinformacji ma tendencję wzrostową, niezależnie, kto jest celem takich działań.

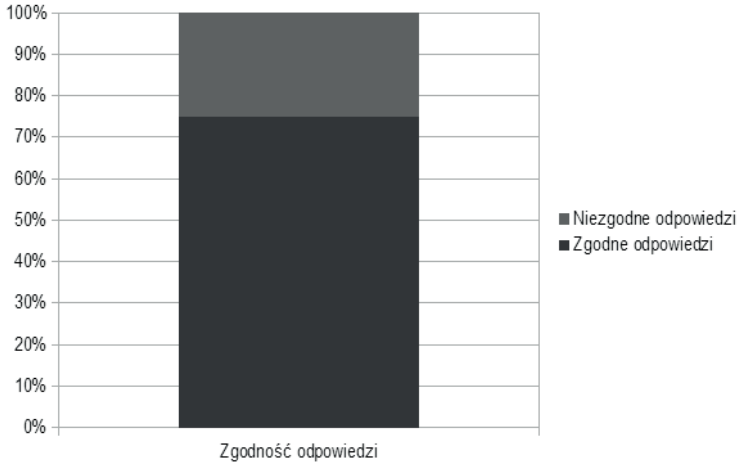
Na pytanie drugie odnośnie dezinformacji dwaj eksperci odpowiedzieli zgodnie. Ekspert numer 2 odpowiedział krótko, że najsłabszym ogniwem systemu bezpieczeństwa państwa w aspekcie dezinformacji jest czynnik ludzki. Natomiast ekspert numer 1 uszczegółowił tę wypowiedź poprzez wskazanie procesu pozyskiwania informacji jako najbardziej narażonego na dezinformację. Warto tu nadmienić, że ekspert numer 1 stwierdził, iż pominięcie procedur bezpieczeństwa w procesie pozyskiwania informacji wzmacnia to zagrożenie. Ekspert numer 3 wskazał jednoznacznie na procesy pozyskiwania, analizy i wymiany informacji. Zwrócił uwagę na fakt, iż komponentami systemu bezpieczeństwa podatnymi na dezinformację

mogą być zarówno ludzie, jak i maszyny. Wnioski: Dezinformacja jest realnym zagrożeniem systemu bezpieczeństwa państwa. Wszędzie tam, gdzie występuje czynnik ludzki, dezinformacja może być stosowana z większym powodzeniem oraz może przynieść większe zagrożenie aniżeli w przypadku komponentów technicznych / maszynowych / automatycznych systemu. Co nie oznacza, iż komponenty techniczne nie są celem ataków dezinformujących.

W pytaniu trzecim eksperci byli zgodni, odpowiadając, iż to służby wywiadowcze są najbardziej aktywnymi podmiotami w zakresie wykorzystywania dezinformacji. Ekspert numer 3 oprócz najbardziej aktywnych podmiotów, czyli służb wywiadu i kontrwywiadu wymienił również siły zbrojne. Zwrócił on uwagę na fakt, iż siły zbrojne traktują dezinformację jako oręż strategiczny. Pozornie krótkie i zwięzłe odpowiedzi dają ciekawe wnioski. Mianowicie: faktem jest, iż każde państwo funkcjonujące na arenie międzynarodowej posiada służby wywiadowcze; każde państwo zatem na arenie międzynarodowej wykorzystuje dezinformację do realizacji celów oraz zabezpieczenia żywotnych interesów.

Pytanie czwarte to po raz kolejny zgodność ankietowanych ekspertów. Ekspert numer 1 odpowiedział zwięźle, że zarówno szanse, jak i zagrożenia w aspekcie dezinformacji mają tendencję wzrostową. Ekspert numer 2 uzupełnił tę wypowiedź, wskazując na fakt, iż stosunkowo niska szansa wykrycia oraz niskie nakłady finansowe skłaniają strony dezinformujące do zwiększania intensywności takich ataków. Jednocześnie nadmienił, iż tworzone są coraz skuteczniejsze narzędzia obrony przed dezinformacją. Podkreślił również, że potrzebne jest przewartościowanie systemu w aspekcie znaczenia informacji. Natomiast ekspert numer 3 również zwrócił uwagę na system zabezpieczeń przed dezinformacją. Jednak jako osoby na pierwszej linii frontu wymienił nas samych. Analiza tych wypowiedzi pozwala na wyciągnięcie następujących wniosków: jeśli chodzi o zagrożenia to ataki dezinformacyjne będą w przyszłości narastać, np. poprzez wzrost skali czy zakresu zjawiska; jeśli chodzi o szanse to rozwój narzędzi obronnych pozwoli na skuteczne przeciwdziałanie temu zjawisku. Świadomość użytkowników jest niezwykle istotna, w aspekcie przeciwdziałania dezinformacji.

Wartym odnotowania jest fakt, iż eksperci byli ze sobą zgodni. Z ośmiu zadanych pytań na 6 odpowiedzieli jednomyślnie. Natomiast na dwa pytania odpowiedzieli rozbieżnie. Poniżej na wykresie przedstawiono procentowy stosunek zgodności odpowiedzi ekspertów.



Rysunek 1. Procentowy wykres zgodności odpowiedzi
Źródło: badania własne.

Zakończenie

Problematyka zagrożeń dezinformacyjnych jest niezwykle istotnym zagrożeniem współczesnego świata. Narzędzie to jest coraz częściej wykorzystywane nie tylko przez służby specjalne, ale również w ramach konkurencji gospodarczej. Informacja i dezinformacja to terminy interdyscyplinarne. Obejmują każdą znaną nam dziedzinę naukową. Dlatego nie wolno rozpatrywać ich w zakresie tylko jednej wybranej przez siebie dziedziny. Funkcjonują w historii ludzkości od zarania dziejów. Gdy tylko spróbujemy przeanalizować dane wydarzenie, zjawisko, wojnę, rewolucję czy wynalazek pod kątem tych terminów, szybko dostrzeżemy wszechobecność i współzależność tych pojęć z analizowanym przypadkiem. Towarzyszą człowiekowi i kształtują historię oraz cywilizację ludzką. Terminy te ewoluowały na przestrzeni lat, przybierając coraz bardziej złożone formy. Dziś słyszymy o nich nad wyraz często. Informacja jest niezwykle istotna w naszym życiu i jest to niepodważalny fakt. Natomiast dezinformacja nasila się, zmieniając skalę, formy czy metody oddziaływania. Mimo to wciąż mało uwagi poświęca się tym terminom w przestrzeni publicznej. Oczywistym jest, iż środowisko akademickie oraz ludzie współtworzący system bezpieczeństwa państwa bardzo szczegółowo omawiają te pojęcia. Zdaniem autorów tylko szeroka edukacja w aspekcie tworzenia, przekazywania oraz przechowywania informacji mogą przynieść pozytywne efekty w tzw. ruchu informacyjnym.

Bibliografia

1. Garczyński S., *Z informacją na bakier*, Warszawa 1981.
2. Harman Glynn, *Computer Development and Information Management*, *in The Next 200 Years*, Teksas 1984.
3. Kulikowski J.L., *Informacja i świat, w którym żyjemy*, Warszawa 1978.
4. Niedzielska E., *Komunikacja gospodarcza w złożonych systemach informacyjnych*, Wrocław 1988.
5. Stefanowicz B., *Informacja*, Warszawa 2010.
6. Wiener N., *The Human Use of Human Beings*, 1950.

Źródła internetowe

1. Frontex na początku przyszłego tygodnia rozpocznie operacje na greckiej granicy, www.infosecurity24.pl/frontex-na-poczatku-przyszlego-tygodnia-rozpocznie-operacje-na-greckiej-granicy.
2. Informacja, https://encyklopedia.pwn.pl/haslo/informacja;3914686.html.
3. Europejska Komisja, www.ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en.
4. Strefa Schengen: wszystko, co musisz wiedzieć o europejskiej strefie bez granic wewnętrznych, www.europarl.europa.eu/news/pl/headlines/security/20190612STO54307/strefa-schengen-wszystko-co-musisz-wiedziec-o-europejskiej-strefie-bez-granic.

The role of information and disinformation threats in the state security system

Abstract

The issue of information barrage has in today's world an enormous significance. Information is a subject of trade and in many cases it becomes a currency. The serious challenge is protection of information crucial from the point of view of individual, enterprises or whole country. Along with the increase of information importance there appeared a new phenomenon of disinformation being a threat to all above mentioned subjects.

The aim of the article is an attempt to define information and disinformation as well as presenting its role in the state security system. Moreover, new forms of disinformation threats have been stated. In order to discuss precisely the issue experts on information protection and disinformation counteracting have been approached with questions included in the expert interview.

Keywords: information, disinformation, state security system