

**Piotr Bączek**

## **Dezinformacja jako źródło zagrożeń dla współczesnej polityki bezpieczeństwa Polski.**

### **Streszczenie**

**Wstęp:** Gwałtowny skok cywilizacyjny w XX w. sprawił, że nie tylko upowszechniły się znane wcześniej metody przesyłania, przetwarzania, udostępniania informacji, ale równocześnie zaczęły pojawiać się coraz to nowsze technologie do pozyskiwania gromadzenia i wykorzystywania informacji. Rozwój tych technologii doprowadził do wzrostu znaczenia informacji praktycznie w każdej sferze działalności jednostki, społeczeństwa i państwa. Efektem tej trzeciej rewolucji przemysłowej było powstanie społeczeństwa informacyjnego. Cyberprzestrzeń stała się nowym środowiskiem ludzkiej aktywności. Naturalną konsekwencją tego procesu jest większa podatność jednostek, społeczeństw, organizacji na zagrożenia informacyjne. Stosując techniki celowo zniekształcające informacje, modyfikując ich charakter i sens można doprowadzić do ewolucji postawy określonej osoby, grupy, społeczeństwa oraz prominentnych decydentów lub zmiany decyzji instytucji państwa. Jedną z tradycyjnych form walki informacyjnej jest dezinformacja. Metoda ta była stosowana od starożytności, ale termin „dezinformacja” pojawił się dopiero na początku XX w. Za dezinformację uznać należy świadome i intencjonalne działanie struktur państwa, zwłaszcza służb specjalnych, w celu zafałszowania u przeciwnika faktycznego obrazu rzeczywistości. Metoda ta stała się ważnym narzędziem pracy służb specjalnych wielu państw, zwłaszcza z bloku komunistycznego. Również po 1990 r. obserwuje się szereg działań dezinformacyjnych. Na szczególną uwagę zasługuje aktywność w tej sferze Federacji Rosyjskiej (FR).

Działania dezinformacyjne są więc ciągle aktualnym i znaczącym problemem dla współczesnych państw, w tym również Polski. Dlatego uzasadnione jest podejmowanie badań nad zjawiskiem dezinformacji, występowania jej przejawów oraz związanych z tym konsekwencji dla polityki bezpieczeństwa współczesnego państwa polskiego. Kolejnym argumentem uzasadniającym konieczność przeprowadzenia naukowej analizy tego problemu jest fakt, że dotychczas problematyka oddziaływania dezinformacji na politykę Polski była w niewielkim stopniu podejmowana przez polskich badaczy.

**Cel pracy:** Celem głównym rozprawy było poszukiwanie rozwiązania głównego problemu badawczego, czyli udzielenia odpowiedzi na pytanie, w jakim zakresie zagrożenia dezinformacyjne wpływały i wpływają na politykę bezpieczeństwa III RP? Celem poznawczym rozprawy jest identyfikacja, eksplanacja i diagnoza technik dezinformacyjnych

stosowanych wobec państwa polskiego i społeczeństwa. Przedmiotem badań są instytucje współczesnego państwa polskiego. Natomiast celem użytecznym jest wypracowanie założeń przeciwdziałania dezinformacji w procesach kształtowania polityki bezpieczeństwa państwa.

**Materiał i metody:** Ramy czasowe badań obejmują lata 1990 - 2022. Dolna granica jest momentem powstania III RP. Był to okres tzw. transformacji ustrojowej, kiedy kształtowały się demokratyczne instytucje państwa i na nowo definiowana była jego polityka bezpieczeństwa. W latach 1990 – 2022 państwo polskie przeprowadzało systemowe zmiany mające dostosować jego struktury do tzw. rewolucji informacyjnej związanej z rozwojem społeczeństwa informacyjnego. Przyniosła ona niespotykany wzrost znaczenia informacji w życiu państwa i społeczeństw zwiększając tym samym podatność państwa na zagrożenia informacyjne. W tym okresie zauważalna jest aktywność w stosowaniu dezinformacji. Charakter podmiotowy i przedmiotowy rozważań na temat dezinformacyjnych zagrożeń dla współczesnej polityki bezpieczeństwa Polski sprawił, że do rozpatrzenia wskazanego problemu badawczego zastosowano następujące metody: analizy systemów według teorii Davida Eastona, instytucjonalno-prawną, historyczną, komparystyczną, teoretyczne (analizę, syntezę, porównanie, uogólnienie), wnioskowania (dedukcję indukcyjną, analogię) oraz studium przypadku. Analizie poddano jawne dokumenty, w tym m.in. kolejne strategie bezpieczeństwa narodowego, raporty, komunikaty, analizy i opracowania Biura Bezpieczeństwa Narodowego (BBN), Rady Ministrów (RM), Ministerstwa Spraw Wewnętrznych (MSW), Ministerstwa Spraw Wewnętrznych i Administracji (MSWiA), Ministerstwa Obrony Narodowej (MON), Ministerstwa Spraw Zagranicznych (MSZ), Agencji Bezpieczeństwa Wewnętrznego (ABW), Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (NASK-PIB), zespołów Reagowania na Incydenty Komputerowe (CERT) oraz zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSRIT) działających w ABW, MON i NASK-PIB.

**Wyniki:** Na podstawie analizy zgromadzonego materiału badawczego stwierdzono, że od lat 2013-2014 kluczowe instytucje państwa polskiego odpowiedzialne za bezpieczeństwo przedstawiały oceny, że zagrożenia dezinformacyjne w dużym stopniu wpływają na politykę Polski. W 2013 r. eksperci BBN w „Białej Księdze Bezpieczeństwa Narodowego” wymienili dezinformację wśród innych zagrożeń dla bezpieczeństwa Polski. Rok później eksperci ABW ocenili, że sieci społecznościowe w Polsce zostały „zalaną” treściami dezinformacyjnymi promującymi stanowisko Federacji Rosyjskiej. Od 2014 r. instytucje odpowiedzialne za bezpieczeństwo państwa polskiego coraz częściej informowały o tego typu zdarzeniach. W dalszym ciągu brakowało jednak konsekwentnej polityki państwa wobec tego zagrożenia.

Przełom w podejściu do zagrożeń dezinformacyjnych nastąpił na przełomie 2016/2017, chociaż aż do 2018 r. dezinformacja nie była systematycznie ujmowana w państwowych dokumentach określających ochronę cyberprzestrzeni.

Uzyskane wyniki pozwoliły na ustalenie, że najważniejszymi czynnikami warunkującymi politykę bezpieczeństwa Polski są determinanty geopolityczne, które były konsekwencją transformacji ustrojowej z przełomu lat 80. i 90. XX w. Przemiany te doprowadziły do przeorientowania polityki bezpieczeństwa państwa polskiego, przystąpienia do NATO i UE oraz odejścia od systemu gospodarczego „realnego socjalizmu” do systemu wolnorynkowego. Na politykę bezpieczeństwa wpłynęły również zachodzące przemiany cywilizacyjne, rozwój technologiczny, upowszechnienie nowoczesnych technik komunikacyjnych, w tym mediów społecznościowych, które w XXI w. stały się również instrumentem walki informacyjnej..

W toku badań stwierdzono, że dezinformacja może być rozpowszechniana tradycyjnymi oraz nowoczesnymi metodami. W pierwszym przypadku to jednostka lub zespoły ludzkie odgrywają decydującą rolę. Do tego typu kanałów dezinformacji zaliczyć należy m.in. media (w tym prasę oraz radio i telewizję), jednostki wojskowe, dyplomację, służby specjalne i siatki ich tajnych współpracowników, szczególnie agenturę wpływu. W ostatniej dekadzie stulecia nastąpił gwałtowny wzrost wykorzystania do działań dezinformacyjnych nowoczesnych technologii informatycznych. w tym mediów społecznościowych.

W toku analiz ustalono, że dezinformacja jest stosowana do wywierania wpływu na społeczeństwo i struktury państwa. Oddziaływanie to ma charakter negatywny. Konsekwencją dezinformacji jest chaos informacyjny, osłabienie więzi społecznych, obniżenie zaufania do władz, dezintegracja struktur państwa, wprowadzanie do sfery informacyjnej treści sprzecznych z racją stanu, lansowanie poglądów i postaw korzystnych dla podmiotu atakującego. Celem działań dezinformacyjnych jest wprowadzenie w błąd jednostki, wybranych grup ludzkich lub całego społeczeństwa oraz poszczególnych struktur administracji państwowych, łącznie z najwyższymi decydentami. W konsekwencji dezinformacja może prowadzić do formułowania fałszywych ocen oraz podejmowania na tej podstawie błędnych decyzji politycznych, militarnych, dyplomatycznych, gospodarczych. W pierwszych latach transformacji ustrojowej zdarzały się przypadki działań operacyjnych krajowych służb specjalnych, które wykorzystywały dezinformację do zwalczania opozycji politycznej. Była to jedna z nieformalnych i tajnych metod przeprowadzenia zmian politycznych. Celem było wewnętrzne skłócenie, zdestabilizowanie i dezintegracja przeciwników politycznych, ale również wpływanie poprzez media na opinię publiczną. Służby specjalne poprzez swoją agenturę i oficerów pod przykryciem rozpuszczały plotki,

falszowały dokumenty, dokonywały przecieków z wybiórczo dobranych materiałów operacyjnych, inspirowały ich opublikowanie w prasie.

Analiza inicjatyw administracji rządowej potwierdziła, że dezinformacja stanowi istotne zagrożenie dla polityki bezpieczeństwa państwa polskiego. Przez wiele lat znaczenie dezinformacji w operacjach przeciwko państwu polskiemu było niejednokrotnie pomijane lub marginalizowane. Próby aktywnego kształtowania całościowej polityki państwa polskiego w zakresie zwalczania dezinformacji rozpoczęły się dopiero około 2014 r. Pierwszym publicznym przejawem tego było opracowanie projektu „Doktryny bezpieczeństwa informacyjnego RP” z 24 lipca 2015 r. We wcześniejszych latach nie podejmowano takich inicjatyw.

Wykorzystanie metody instytucjonalno-prawnej umożliwiło uzyskanie odpowiedzi na pytanie o działania w ramach polityki bezpieczeństwa skutecznie chroniące struktury państwa przed dezinformacją. Analiza przekształceń w krajowym systemie instytucji realizujących politykę bezpieczeństwa pozwoliła na stwierdzenie, że polityka bezpieczeństwa wymaga zmian, aby skutecznie chronić państwo przed dezinformacją. Potwierdzeniem tej tezy jest proces tworzenia od 2016 r. nowych instytucji państwowych w Polsce. Niektóre z nich mają zajmować się również przeciwdziałaniem dezinformacji, przede wszystkim w cyberprzestrzeni. Takie zadania powierzano również instytucjom już dotychczas istniejącym. Ze względu na brak szczegółowych przepisów prawnych dotyczących zwalczania obcej dezinformacji i organizacji systemu tych instytucji nie jest on formalnie ustrukturyzowany prawnie i ma charakter umowny. Istniejąca obecnie organizacja systemu przeciwdziałania dezinformacji nie posiada jasno określonego hierarchicznego podporządkowania. Taki model może wywołać w sytuacji kryzysowej spory kompetencyjne oraz spowodować niezamierzone utrudnienia w realizacji zadań.

**Wnioski:** Wyniki uzyskane w toku procesu badawczego potwierdzają założenie wstępne, że dezinformacja w znaczącym stopniu wpływa na politykę bezpieczeństwa państwa. W związku z tym za celowe należy uznać prowadzenie dalszych badań dotyczących m. in. ewolucji form i typów dezinformacji; zastosowania nowoczesnych technologii, w tym systemów sztucznej inteligencji, do jej rozpowszechniania. Wypracowanie modelu prowadzenia badań w tych instytucjach umożliwi dokładniejszą eksplorację analizowanego problemu wpływu dezinformacji na politykę III RP.