



AGNIESZKA WARCHOŁ

Uniwersytet Komisji Edukacji Narodowej w Krakowie

ORCID: 0000-0003-0786-6440

agnieszka.warchol@uken.krakow.pl

Sekurytyzacja wojny informacyjnej w stosunkach międzynarodowych.

Między dyskursem polskich polityków a narracjami
Unii Europejskiej i NATO

The Securitisation of Information Warfare in International Relations:

Between the Discourse of Polish Politicians and the Narratives
of the European Union and NATO

Słowa kluczowe:

sekurytyzacja, wojna
informacyjna, cyberprzestrzeń,
polityka bezpieczeństwa,
bezpieczeństwo
międzynarodowe

Keywords:

securitisation,
information warfare,
cyberspace, security
policy, international
security



Sekurytyzacja wojny informacyjnej w stosunkach międzynarodowych. Między dyskursem polskich polityków a narracjami Unii Europejskiej i NATO

Celem niniejszego artykułu jest omówienie zagadnienia sekurytyzacji wojny informacyjnej w stosunkach międzynarodowych jako procesu, w którym określone działania psychologiczne lub techniczne przedstawiane są przez podmioty bezpieczeństwa jako egzystencjalne zagrożenia dla państwa, porządku demokratycznego oraz stabilności międzynarodowej, co ma na celu legitymizację stosowania nadzwyczajnych środków przeciwdziałania. W pracy wykorzystano wypowiedzi polskich polityków oraz działania Unii Europejskiej i NATO będące poniekąd skutkiem tego procesu na arenie stosunków międzynarodowych.

The Securitisation of Information Warfare in International Relations: Between the Discourse of Polish Politicians and the Narratives of the European Union and NATO

This paper explores the securitisation of information warfare in international relations, understood as a process whereby selected psychological and technical activities are discursively framed by security actors as existential threats to the state, democratic order, and international stability, thus legitimising the deployment of extraordinary countermeasures. The study is based on statements made by Polish politicians and on actions undertaken by the European Union and NATO, which may be interpreted, at least to some extent, as consequences of this process within the sphere of international relations.

Wprowadzenie

W literaturze przedmiotu znajdujemy wiele definicji wojny informacyjnej. Część z nich akcentuje działania podmiotów państwowych, które wpływają na ludność cywilną i wojsko poprzez rozpowszechnianie odpowiednio dobranych informacji¹. Inne ujęcia podkreślają rolę służb specjalnych jako aktywnych uczestników tego rodzaju działań i wskazują, że sama wojna informacyjna wpisuje się w trwające konflikty zbrojne². Kolejne definicje rozszerzają zakres tego pojęcia o działalność podmiotów niepaństwowych³, wskazując dodatkowo, że samo zjawisko jest elementem wojny hybrydowej⁴. Jeszcze inni autorzy, których spojrzenie mieści się w podejściu krytycznym, twierdzą, że większość zjawisk powszechnie nazywanych wojną informacyjną to w rzeczywistości inne rodzaje zagrożeń, np. sabotaż czy szpiegostwo, a nie wojna w ścisłym tego słowa znaczeniu, stąd w niniejszym tekście postulowane jest nienadużywanie tego pojęcia⁵.

Założenia teorii sekurytyzacji mieszczą się właśnie w ramach podejścia krytycznego w studiach nad bezpieczeństwem. Powstała ona w latach dziewięćdziesiątych XX w. w ramach tzw. szkoły kopenhaskiej, której głównymi przedstawicielami byli Barry Buzan, Ole Wæver i Jaap de Wilde. Współcześnie mamy do czynienia z drugą generacją badaczy, którzy – jak pisze Łukasz Fijałkowski – rozwijają teorię sekurytyzacji poza jej pierwotne

- 1 O. Wasiuta, S. Wasiuta, *Wojna informacyjna zagrożeniem dla bezpieczeństwa ludzkości*, [w:] *Walka informacyjna. Uwarunkowania – incydenty – wyzwania*, red. H. Batorowska, Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej, Kraków 2017, s. 71.
- 2 A. Żebrowski, *Obszary zainteresowania służb specjalnych w trzeciej dekadzie XXI wieku. Wybrane aspekty*, „Central European Journal of Security Studies” 2024, vol. 2, issue 1, s. 25.
- 3 J. Kiera, *Wojna informacyjna w polityce zagranicznej Federacji Rosyjskiej wobec Polski w latach 2010–2022*, rozprawa doktorska, Uniwersytet Śląski, Katowice 2025, s. 86: <https://bip.us.edu.pl/sites/default/files/2025-07/Rozprawa_doktorska.pdf> [dostęp: 18 III 2026].
- 4 M. Pietras, *Wojna informacyjna jako współczesne narzędzie działań nieregularnych*, „Cybersecurity and Law” 2021, nr 6 (2), s. 28.
- 5 T. Rid, *Cyber War Will Not Take Place*, „Journal of Strategic Studies” 2012, vol. 35, issue 1: <<https://csl.armywarcollege.edu/SLET/mccd/CyberSpacePubs/Cyber%20War%20Will%20Not%20Take%20Place%20Oby%20Thomas%20Rid.pdf>> [dostęp: 17 III 2026].

założenia, uwzględniając różnorodne problemy, takie jak cyberbezpieczeństwo, migracje czy religia⁶. Teoria sekurytyzacji podważa tradycyjną definicję bezpieczeństwa, która odnosi się wyłącznie do obiektywnych zagrożeń ze strony innych podmiotów i obejmuje użycie lub groźbę użycia siły militarnej⁷.

Fundamenty teorii sekurytyzacji oparte są na założeniu, że bezpieczeństwo rozumiane jest w kategoriach nadzwyczajności i pilności działania, co wynika z jego ścisłego związku z kwestią przetrwania⁸. W ten sposób sekurytyzacja wiąże się z procesem określania danego problemu jako zagrożenia egzystencjalnego⁹, co ma prowadzić do uruchomienia właściwej dla bezpieczeństwa logiki działania¹⁰. W tym ujęciu bezpieczeństwo zachowuje status kategorii egzystencjalnej, osadzonej w realistycznej tradycji myślenia o stosunkach międzynarodowych, podczas gdy sama sekurytyzacja ujmowana jest jako proces o charakterze konstruktywistycznym i dyskursywnym. Ważną rolę odgrywa tu podmiot sekurytyzujący, który za pomocą aktu mowy nadaje problemowi status kwestii bezpieczeństwa, dążąc do uzyskania akceptacji odbiorców dla takiej interpretacji. Buzan, Wæver i de Wilde piszą w swojej książce *Security. A New Framework for Analysis*, że sekurytyzację można postrzegać jako skrajną wersję upolitycznienia¹¹.

Zgodnie z założeniami procesu sekurytyzacji polityka bezpieczeństwa kreowana jest przez polityków i decydentów politycznych¹². Jeżeli w przestrzeni politycznej uznanie zyskują postulaty legitymizujące uprawnienie do zastosowania wszelkich środków uznanych za niezbędne w celu rozwiązania określonego problemu, można mówić o skuteczności tego procesu.

6 Ł. Fijałkowski, *Studia nad sekurytyzacją – między kontynuacją a krytyką*, „Wiedza Obronna” 2025, t. 291, nr 2, s. 12, 14.

7 G. Karyotis, I. Paterson, A. Judge, *Understanding Securitization Success: A New Analytical Framework*, „International Studies Review” 2025, vol. 27, issue 1: <<https://academic.oup.com/isr/article/27/1/viafo06/8100844>> [dostęp: 18 III 2026].

8 Tamże.

9 B. Buzan, O. Wæver, J. de Wilde, *Security. A New Framework for Analysis*, Lynne Rienner Publishers, Boulder-London 2022, s. 24.

10 G. Karyotis, I. Paterson, A. Judge, *Understanding...*

11 Tamże, s. 23.

12 C. Eroukhanoff, *Securitisation Theory: An Introduction*, „E-International Relations” [online], 14 I 2018 [dostęp: 18 I 2026]: <<https://www.e-ir.info/2018/01/14/securitisation-theory-an-introduction/>>.

Wtedy dany problem kwalifikowany jest do kategorii bezpieczeństwa nie tyle ze względu na istnienie obiektywnego i realnego zagrożenia egzystencjalnego, ile przede wszystkim dlatego, że istotni aktorzy (np. polityczni) potrafią przekonująco przedstawić i utrwalić go w debacie publicznej jako zagrożenie o takim właśnie charakterze¹³. Istota sekurytyzacji sprowadza się więc do przekonania odbiorców, że przewidywana skala zagrożenia, niezależnie od jego rzeczywistego obiektywnego znaczenia, uzasadnia uruchomienie nadzwyczajnych środków w celu jego zwalczania¹⁴.

Celem niniejszego artykułu jest omówienie problematyki sekurytyzowania wojny informacyjnej w stosunkach międzynarodowych jako procesu, w którym określone działania psychologiczne lub techniczne¹⁵ przedstawiane są przez podmioty bezpieczeństwa jako egzystencjalne zagrożenia dla państwa, porządku demokratycznego oraz stabilności międzynarodowej, co ma na celu legitymizację użycia nadzwyczajnych środków przeciwdziałania. Dodatkowo sekurytyzacja wojny informacyjnej nierozzerwalnie wiąże się z rolą prawa międzynarodowego w stosunkach międzynarodowych, co również znajdzie odzwierciedlenie w niniejszych rozważaniach.

Konsekwencją określenia celu pracy są następujące pytania badawcze: Jakie podmioty dokonują sekurytyzacji wojny informacyjnej? W jaki sposób zagadnienie takie jak wojna informacyjna rozpatrywane jest w dyskursie międzynarodowym jako zagrożenie dla bezpieczeństwa danego podmiotu? Jakie narracje, argumenty i strategie dyskursywne wykorzystywane są w procesie sekurytyzacji wojny informacyjnej? Jakiego rodzaju konsekwencje niesie za sobą sekurytyzacja wojny informacyjnej?

Przyjęta w artykule hipoteza badawcza brzmi: Sekurytyzacja wojny informacyjnej w stosunkach międzynarodowych prowadzi do przesunięcia oddziaływań informacyjnych z obszaru rywalizacji politycznej do sfery bezpieczeństwa, gdzie są one interpretowane jako zagrożenia egzystencjalne.

13 M. Dunn Cavelty, *Cyber-Security and Threat Politics. US Efforts to Secure the Information Age*, Routledge, London–New York 2008, s. 18: <https://www.researchgate.net/publication/277714726_Cyber-Security_and_Threat_Politics_US_Efforts_to_Secure_the_Information_Age> [dostęp: 19 III 2026].

14 G. Karyotis, I. Paterson, A. Judge, *Understanding...*

15 W zakresie działań psychologicznych mieszczą się oddziaływanie na opinie, emocje, postawy i zachowania odbiorców, a w obrębie technicznych – ingerencja w systemy komputerowe oraz infrastrukturę informacyjną, w tym działania niszczące i zakłócające.

W rezultacie podmioty bezpieczeństwa, takie jak państwa i organizacje międzynarodowe, uzyskują legitymację do wdrażania nadzwyczajnych środków ochrony przestrzeni informacyjnej, co zarazem może nieść ryzyko rozszerzania kontroli nad komunikacją publiczną i ograniczania procedur demokratycznych.

Do realizacji przedstawionego celu wykorzystano następujące metody badawcze: analizę i krytykę źródeł, analizę i krytykę piśmiennictwa, analizę porównawczą oraz studium przypadku¹⁶. Artykuł opiera się na analizie literatury przedmiotu, dokumentów oraz wybranych źródeł prawa międzynarodowego, w tym dotyczących zakazu interwencji, odpowiedzialności państw i ochrony praw człowieka, a także prawa Unii Europejskiej (UE). Przy wyborze materiału do analizy zastosowane zostało kryterium celowości i aktualności wobec problemu sekurytyzacji wojny informacyjnej. Włączono do niej również istotne publikacje z nauk o bezpieczeństwie, politologii i stosunkach międzynarodowych. Uzupełniając wykorzystane zostały także wybrane materiały prasowe oraz treści audiowizualne, ponieważ pozwalają zilustrować praktyczne aspekty sekurytyzacji wojny informacyjnej, sposoby rozpowszechniania konkretnych narracji oraz mechanizmy oddziaływania na odbiorców. Materiały te nie stanowią jednak w analizie podstawy normatywnej, lecz pełnią funkcję pomocniczą.

Polityka lęku

O sekurytyzacji mówimy wówczas, gdy dane zagadnienie zaliczane jest do sfery bezpieczeństwa, co daje określonemu podmiotowi możliwość zastosowania specjalnych środków spoza katalogu standardowych procedur politycznych¹⁷. Elementami procesu sekurytyzacji są: aktorzy sekury-

16 Analiza piśmiennictwa posłużyła do omówienia podstawowych pojęć, analiza źródeł objęła dokumenty strategiczne, akty prawa międzynarodowego i prawa UE oraz raporty organizacji i instytucji, np. EEAS i ONZ. Metoda porównawcza pozwoliła zestawzić podejście prawa międzynarodowego, prawa UE i praktyk instytucjonalnych wobec operacji informacyjnych, a studium przypadku wykorzystane zostało do omówienia wybranych przykładów sekurytyzacji wojny informacyjnej. W artykule przytoczono ponadto wybrane wypowiedzi decydentów politycznych mających wpływ na kształtowanie polityki bezpieczeństwa informacyjnego.

17 J. Czaputowicz, *Teorie stosunków międzynarodowych*, Wydawnictwo Naukowe PWN, Warszawa 2022, s. 186.

tyzujący (nadawcy); obiekty referencyjne, które należy bronić przed zagrożeniem; samo zagrożenie, które ma charakter egzystencjalny; widownia, czyli odbiorcy aktu mowy; a także specjalne środki, czyli działania mające ochronić obiekt referencyjny przed zagrożeniem¹⁸. Co istotne, środki te nie są przewidziane w ramach zwykłego procesu politycznego¹⁹.

W perspektywie sekurytyzacji szczególne znaczenie zyskuje kategoria lęku społecznego, który jednak nie powinien być interpretowany wyłącznie w wymiarze indywidualnym czy psychologicznym. Jak wskazuje Jacek Czaputowicz, lęk ten ma bowiem w dużej mierze charakter strukturalny, ponieważ wyrasta z doświadczenia codziennej niepewności, właściwej społeczeństwu funkcjonującym w warunkach nasilonego ryzyka, niestabilności i podatności na kryzysy²⁰. Mimo że jest to kategoria niezwykle istotna przy analizie społecznych konsekwencji sekurytyzacji, lęk nie jest pojęciem, które często pojawia się w samej teorii tego zjawiska, np. w rozważaniach szkoły kopenhaskiej. Późniejsze próby rozwinięcia tej teorii, np. przez Michaela C. Williamsa, ukazywały, że lęk może też hamować proces sekurytyzacji, co należałoby określić mianem desekurytyzowania sekurytyzacji, gdzie – co ciekawe – to właśnie lęk jest zasobem desekurytyzującym²¹.

Społeczne poczucie zagrożenia nie jest jedynie spontaniczną reakcją na zdarzenia tu i teraz, ale może być ściśle związane z dominującymi dyskursami politycznymi i bezpieczeństwa, które lęk społeczny celowo wzmacniają. W procesie sekurytyzacji lęk nie jest zatem jedynie skutkiem występowania zagrożeń, ale może też stać się narzędziem ich politycznego konstruowania. Za pomocą aktu mowy aktorzy polityczni oraz instytucje odpowiedzialne za bezpieczeństwo przedstawiają określone zjawiska jako zagrożenia o charakterze egzystencjalnym, wymagające natychmiastowej i zdecydowanej reakcji. Warto w tym miejscu zauważyć za Markiem

18 M. Adamczyk, M. Maćkowiak, *„Protecting Americans from Foreign Adversary Controlled Applications Act”, czyli kolejna odsłona amerykańsko-chińskiej wojny o TikTok. Analiza z perspektywy teorii sekurytyzacji szkoły kopenhaskiej*, „Studia Orientalne” 2025, R. 14, nr 1 (33), s. 11: <<https://doi.org/10.15804/so2025101>> [dostęp: 16 II 2026]; R. Siudak, *Cyberbezpieczeństwo w Polsce. Od dyskursów do polityk publicznych*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2022, s. 38.

19 Tamże.

20 J. Czaputowicz, *Teorie...*, s. 186.

21 M. C. Williams, *Securitization on the Liberalism of Fear*, „Security Dialogue” 2011, vol. 42, No. 4–5, s. 453.

Górką, że „obecnie państwo nie ma monopolu na politykę bezpieczeństwa i że oprócz instytucji państwowych istnieją podmioty sektora publicznego, które również mogą zainicjować proces sekurytyzacji”²².

Podsumowując, należy stwierdzić, że aktorami sekurytyzującymi są wszystkie podmioty zdolne do nadawania określonym zjawiskom statusu zagrożenia bezpieczeństwa. Oznacza to, że proces sekurytyzacji może być inicjowany nie tylko przez państwo *sensu stricto*, ale również przez instytucje szeroko pojętego sektora publicznego, organy bezpieczeństwa, organizacje regionalne i międzynarodowe, media oraz środowiska eksperckie, o ile dysponują one wystarczającym autorytetem i siłą oddziaływania, by przekonać odbiorców do uznania danego problemu za zagrożenie egzystencjalne. Jak trafnie podkreśla Górka, podmiot dokonujący sekurytyzacji potrzebuje wystarczającego kapitału społecznego i politycznego, by przekonać odbiorców o istnieniu zagrożenia egzystencjalnego²³. W niniejszych rozważaniach są to m.in. polscy decydenci polityczni, instytucje UE, Europejska Służba Działań Zewnętrznych oraz NATO, opisujący dezinformację czy operacje wpływu jako zagrożenia dla demokracji, odporności społecznej i bezpieczeństwa państw.

W latach dziewięćdziesiątych XX w. Wæver pisał, że poczucie bezpieczeństwa jest konstrukcją społeczną, aktem deklaratywnym i wynikiem dyskursu²⁴. Tego rodzaju dyskurs nie tylko wzmacnia społeczne poczucie niepewności, ale też może podkreślać szczególną rolę podmiotów odpowiedzialnych za ochronę i bezpieczeństwo, takich jak wojsko, policja, służby specjalne czy eksperci w zakresie bezpieczeństwa. Im silniej zagrożenie komunikowane jest jako realne i egzystencjalne, tym łatwiej uzyskać społeczną akceptację dla rozszerzenia kompetencji tych instytucji. Celowo wzmacniany lęk społeczny może więc pełnić funkcję polityczną. Pozwala bowiem przesunąć określony problem z obszaru zwykłej debaty publicznej do sfery bezpieczeństwa, w której dopuszczalne staje się stosowanie

22 M. Górka, *Conceptualising Securitisation in the Field of Cyber Security Policy*, „Journal of Modern Science” 2023, t. 4/53, s. 266.

23 Tamże, s. 278.

24 J. Czaputowicz, *Teorie...*, s. 186; O. Wæver, *Securitization and Desecuritization*, [w:] *On Security*, ed. R. D. Lipschutz, Columbia University Press, New York 1995: <<https://www.libraryofsocialscience.com/assets/pdf/Waever-Securitization.pdf>> [dostęp: 19 III 2026].

środków nadzwyczajnych. W konsekwencji sekurytyzacja opiera się nie tylko na identyfikacji zagrożenia, lecz również na wytwarzaniu takiego klimatu społecznego, w którym określone działania państwa jawią się jako konieczne i racjonalne, a wręcz społecznie pożądane.

Niezwykle istotny jest fakt, że mechanizm ten może prowadzić do rozszerzania kontroli, zwiększania nadzoru oraz ograniczania standardowych procedur demokratycznych, usprawiedliwianych potrzebą ochrony obywateli przed niebezpieczeństwem. Dlatego analiza sekurytyzacji wymaga uwzględnienia nie tylko treści komunikowanych zagrożeń, ale również emocjonalnego i społecznego podłoża ich przyswajania. Lęk staje się tu istotnym elementem procesu politycznego, ponieważ umożliwia skuteczniejsze uzasadnianie działań wykraczających poza ramy zwykłej polityki. W tym sensie sekurytyzacja nie polega wyłącznie na opisie rzeczywistości bezpieczeństwa, lecz również na wytwarzaniu takich warunków społecznych, w których wyjątkowe środki mogą zostać uznane za uzasadnione.

W teorii sekurytyzacji szczególne miejsce zajmuje wobec tego akt mowy, który *de facto* tworzy rzeczywistość²⁵. Przyjmując akt mowy jako podstawowy mechanizm działania, teoria ta odwołuje się do konstytutywnej roli języka w kształtowaniu rzeczywistości społecznej. Jej fundamenty teoretyczne tworzą m.in. teoria aktów mowy Johna Langshawa Austina, zgodnie z którą wypowiedzi nie tylko opisują rzeczywistość, ale same stanowią formę działania społecznego²⁶. Ważna jest tu także refleksja Jacques'a Derridy, który podkreślał, że znaczenie tekstu ujawnia się nie tylko w jego treści, lecz również w skutkach, jakie wywołuje²⁷. Istotne znaczenie ma wreszcie koncepcja stanu wyjątkowego Carla Schmitta, zakładająca możliwość określania przez państwo sytuacji zagrożenia dla wspólnoty politycznej oraz domagania się w takich okolicznościach lojalności obywateli. Uzupełnieniem tego zaplecza jest obecna u Kennetha Waltza

25 P. Polko, A. Urbanek, *Sekurytyzacja*, „Encyklopedia Bezpieczeństwa Narodowego” [online], 10 II 2024 [dostęp: 19 III 2026]: <<https://encyklopedia.revite.pl/articles/view/502>>.

26 J. L. Austin, *How to Do Things with Words*, Oxford at the Clarendon Press, Oxford 1962: <https://pure.mpg.de/rest/items/item_2271128/component/file_2271430/content> [dostęp: 29 V 2026].

27 J. Derrida, *Signature Event Context*, [w:] tegoż, *Limited Inc*, Northwestern University Press, Evanston 1988: <<https://lab404.com/misc/ltidinc.pdf>> [dostęp: 29 V 2026].

realistyczna wizja państwa, ujmująca je jako podmiot zorientowany przede wszystkim na własne przetrwanie²⁸.

Podsumowując, podkreślmy, że to język decyduje o tym, jak rozumiemy i czym wypełniamy naszą świadomość²⁹. Wobec tego wykorzystanie przez elity polityczne odpowiednich, wyselekcjonowanych pojęć jest kluczowe w próbach legitymizowania decyzji związanych z bezpieczeństwem obywateli. Społeczna akceptacja, często osiągnięta poprzez wywołanie u obywateli poczucia lęku, jest istotnym warunkiem optymalizowania decyzji politycznych³⁰.

Wojna informacyjna w języku polskich polityków – wybrane przykłady

Wobec powyższych rozważań należy stwierdzić, że wojna informacyjna nie funkcjonuje wyłącznie jako obiektywne zjawisko, ale także jako kategoria polityczna i strategiczna, której znaczenie współtworzą wypowiedzi decydentów politycznych. Samo pojęcie *wojna informacyjna* rodzi problemy terminologiczne. Nie ma jednej powszechnie akceptowanej definicji, niemniej większość ekspertów zgadza się co do tego, że są to skoordynowane, długotrwałe i wrogie działania prowadzone najczęściej przez państwo lub innego silnego aktora przeciwko innemu państwu lub społeczeństwu z wykorzystaniem manipulacji informacją i dezinformacji w celu osłabienia zdolności politycznych, społecznych lub obronnych³¹. Łukasz Olejnik wskazuje, że o wojnie informacyjnej możemy mówić wówczas, gdy działania mają związek z trwającym już konfliktem zbrojnym³². Zwraca przy tym uwagę, że określe-

28 Ł. Fijałkowski, *Teoria sekurytyzacji i konstruowanie bezpieczeństwa*, „Przegląd Strategiczny” 2012, nr 1, s. 152.

29 B. Krauz-Mozer, *Teorie polityki. Założenia metodologiczne*, Wydawnictwo Naukowe PWN, Warszawa 2007, s. 32.

30 Z. J. Pietraś, *Decydowanie polityczne*, Wydawnictwo Naukowe PWN, Warszawa-Kraków 1998, s. 131.

31 J. Kiera, *Wojna...*, s. 86; *Notions of Disinformation and Related Concepts (ERGA Report)*, European Regulators Group for Audiovisual Media Services, [b.d.m.w.], s. 67: <https://media-board.europa.eu/document/download/00eeb7c2-1abc-443f-9ead-f103b6b577fo_en?filename=ERGA-SG2-Report-2020-Notions-of-disinformation-and-related-concepts-final.pdf&prefLang=sk> [dostęp: 18 III 2026].

32 Ł. Olejnik, *Propaganda. Od dezinformacji i wpływu do operacji i wojny informacyjnej*, Wydawnictwo Naukowe PWN, Warszawa 2024, s. 69.

nie *wojna informacyjna* można usłyszeć także w czasie pokoju, analogicznie do np. *wojny z narkotykami*, co ma wówczas znaczenie publicystyczne, polityczne, a także metaforyczne³³. W polskim dyskursie publicznym pojęcia *wojna informacyjna*, *wojna cyfrowa* czy *cyberwojna* pojawiają się w ostatnim czasie wyjątkowo często, szczególnie w medialnych komentarzach polityków³⁴. Znacznie bardziej zachowawczo wypowiadają się natomiast przedstawiciele wojska, co można interpretować jako przejaw większej ostrożności terminologicznej oraz unikania instrumentalizacji tego pojęcia na potrzeby bieżącej polityki³⁵.

Andrew Heywood pisze, że wojna to „stan otwartego konfliktu zbrojnego między co najmniej dwiema stronami (zwykle państwami)”, ale terminu tego używa się także w przenośni, gdy mowa np. o wojnie handlowej czy zimnej wojnie³⁶. Innymi słowy wojna to przedmiot relacyjny³⁷. Powstaje i rozwija się w wyniku wzajemnych oddziaływań stron konfliktu, a nie jako zjawisko istniejące niezależnie od relacji. W takim rozumieniu wojna informacyjna również ma charakter relacyjny, ponieważ nie polega

33 Tamże, s. 261–262.

34 O tym, że jesteśmy w stanie wojny cyfrowej i informacyjnej, mówi np. minister cyfryzacji: Krzysztof Gawkowski: *cyfrowe czołgi stoją na naszych ulicach* / Gość Poranka, „You Tube. TVP Info” [online], 6 X 2025 [dostęp: 18 III 2026]: <<https://www.youtube.com/watch?v=v83vx6lKTho&t=>>>. W podobnym tonie wypowiedział się ostatnio w mediach doradca ministra obrony narodowej Maciej Samsonowicz: *Incydenty na polskiej granicy. Doradca ministra obrony mówi wprost. „Jesteśmy w stanie wojny informacyjnej”*, „Onet” [online], 3 II 2026 [dostęp: 18 III 2026]: <<https://wiadomosci.onet.pl/kraj/ilu-polakow-jest-gotowych-bronic-kraju-doradca-szefa-mon-mierzymy-regularnie/mpleyqe>>>.

35 Dowódca Komponentu Wojsk Obrony Cyberprzestrzeni gen. dyw. Karol Molenda mówi, że w cyberprzestrzeni mamy do czynienia z konfliktem, budowaniem kompetencji, operacyjnym przygotowaniem środowiska, ale nie z wojną. Wojna to jego zdaniem moment, w którym działania w cyberprzestrzeni lub poprzez cyberprzestrzeń powodują śmierć lub uszkodzenia infrastruktury krytycznej: „Dopóki jednoznacznie nie powiązaliśmy skutków działań w cyberprzestrzeni ze zgonami i zniszczeniem infrastruktury, to jesteśmy na etapie konfliktu, nie wojny”. Zob. *Konferencja SECURE 2024 | Globalne cyberbezpieczeństwo w obliczu nowej zimnej wojny*, „You Tube. NASK PIB” [online], 16 IV 2024 [dostęp: 18 III 2026]: <<https://www.youtube.com/watch?v=wLjScgLhJCQ&t=608s>>>.

36 A. Heywood, *Politologia*, Wydawnictwo Naukowe PWN, Warszawa 2006, s. 467.

37 Własne notatki autorki z wykładów Barbary Krauz-Mozer pn. „Teoria polityki” w Uniwersytecie Jagiellońskim.

wyłącznie na jednostronnym przekazie, lecz rozwija się w przestrzeni wzajemnych oddziaływań między stronami. Jej istota wyraża się w próbach wpływania na percepcję, decyzje i zachowania przeciwnika oraz odbiorców społecznych, dlatego nie może być analizowana w oderwaniu od kontekstu politycznego, komunikacyjnego ani reakcji adresatów przekazu. Jak wskazuje Ignas Kalpokas, jest to celowa i strategiczna manipulacja środowiskiem informacyjnym, wykorzystująca m.in. tendencje postprawdy w celu nakierowania odbiorców na z góry ustalone schematy myślenia³⁸.

Analiza wypowiedzi decydentów politycznych na temat wojny informacyjnej wymaga identyfikacji elementów właściwych aktowi sekurytyzującemu. W tego rodzaju narracjach dostrzegalne jest zazwyczaj wyraźne wskazanie źródła zagrożenia (w wypowiedziach polskich polityków są to np. rosyjskie podmioty³⁹). Dla przykładu podczas jednej z konferencji prasowych minister cyfryzacji Krzysztof Gawkowski powiedział: „W cyberprzestrzeni trwa dzisiaj wojna Rosji z Polską”⁴⁰. Prezydent Andrzej Duda podczas debaty generalnej 78 sesji Zgromadzenia Ogólnego ONZ mówił z kolei:

Trwa wojna informacyjna. Kłamstwo jest wykorzystywane do tuszowania i usprawiedliwienia rosyjskich zbrodni na ludności cywilnej. Rosja nieustannie próbuje oddziaływać na międzynarodową opinię publiczną, budując fałszywy obraz rzeczywistości. W Polsce nie jest to dla nas żadnym zaskoczeniem, ale świat dopiero dziś odkrywa skalę rosyjskiej manipulacji i dezinformacji. Jej ostrze jest często wymierzone także w mój kraj. Próbuje się Polskę oczerniać na rozmaite sposoby. Dzieje się tak dlatego, że konsekwentnie przeciwstawiamy się rosyjskiej imperialnej i neokolonialnej polityce i od samego początku wspieramy broniącą się Ukrainę. Musimy z tego jako społeczność międzynarodowa wyciągnąć wnioski. Musimy walczyć z manipulacją i dezinformacją. Musimy walczyć z za-

38 I. Kalpokas, *Post-Truth and Information Warfare in Their Technological Context*, „ACIG” 2024, vol. 3, No. 2, s. 101.

39 D. Maikowski, „*Jesteśmy w stanie zimnej cyberwojny z Rosją*”. Gawkowski ostrzega, „Gazeta” [online], 16 IV 2024 [dostęp: 15 III 2026]: <<https://next.gazeta.pl/next/7151243,30890519,jestesmy-w-stanie-zimnej-cyberwojny-z-rosja-gawkowski-ostre-ga.html>>.

40 Gawkowski: w cyberprzestrzeni trwa dzisiaj wojna Rosji z Polską, „Polska Agencja Prasowa” [online], 7 I 2025 [dostęp: 17 III 2026]: <<https://www.pap.pl/aktualnosci/gawkowski-w-cyberprzestrzeni-trwa-dzisiaj-wojna-rosji-z-polska>>.

klamywaniem historii. Odwracaniem roli kata i ofiary! Zło trzeba nazywać złem, a zbrodnię zbrodnią!⁴¹

W tego typu wypowiedziach widoczne jest również określenie obiektu referencyjnego, który wymaga ochrony, oraz podkreślenie wyjątkowego i pilnego charakteru sytuacji. Minister spraw zagranicznych Radosław Sikorski, przedstawiając 26 lutego 2026 r. informację o zadaniach polskiej polityki zagranicznej, odniósł się do wrogich operacji informacyjnych i wskazał działania rządu na rzecz ich zwalczania. Najpierw wymieniał, że w przestrzeni informacyjnej widoczne są agresja, kampanie *fake newsów*, manipulacja w internecie, a także niepokojąca skala cyberataków na Polskę, a następnie wskazał kilka działań, które były reakcją polskiego państwa na rosyjską prowokację, np. cofnięcie pozwolenia na funkcjonowanie dwóch ostatnich rosyjskich konsulatów – w Krakowie i Gdańsku. „Cel wroga jest prosty: przestraszyć, podzielić, nastawić różne grupy Polaków przeciwko sobie, osłabić zaufanie do władz politycznych” – mówił minister⁴². Dobrze pokazuje to, że zagrożenie przedstawiane jest jako wymierzone nie tylko w informację, ale też w samą integralność życia politycznego i społecznego. W kontekście sekurytyzacji w wypowiedzi tej można wskazać źródło zagrożenia, obiekt referencyjny oraz legitymizację działań ochronnych. Pierwszym jest wróg utożsamiany z Rosją i jej działaniami informacyjnymi. Obiekt referencyjny, który ma podlegać ochronie, to nie tylko państwo w sensie instytucjonalnym, lecz także społeczna wspólnota Polaków, zaufanie do władz politycznych oraz szerzej rozumiana stabilność wspólnoty. Minister Sikorski nie tylko wskazuje zagrożenie, ale także klasyfikuje je jako istotne dla bezpieczeństwa i wymagające reakcji państwa.

W wypowiedziach polskich polityków wojna informacyjna przedstawiana jest także jako element szerszej konfrontacji na arenie stosunków

41 *Wystąpienie podczas Debaty Generalnej 78. sesji Zgromadzenia Ogólnego ONZ, „Oficjalna Strona Prezydenta Rzeczypospolitej Polskiej”* [online], 19 IX 2023 [dostęp: 18 III 2026]: <<https://www.prezydent.pl/kancelaria/archiwum/andrzej-duda/aktualnosci/wypowiedzi-prezydenta-rp/wystapienia/podczas-debaty-generalnej-78-sesji-zgromadzenia-ogolnego-onz/74976>>.

42 *Informacja Ministra Spraw Zagranicznych o zadaniach polskiej polityki zagranicznej w 2026 r. (tekst wystąpienia)*, „Sejm Rzeczypospolitej Polskiej” [online], 26 II 2026 [dostęp: 18 III 2026]: <<https://www.sejm.gov.pl/Sejm10.nsf/komunikat.xsp?documentId=002995D79C288E3DC1258DAA003F5DE7>>.

międzynarodowych i zarazem zagrożenie dla percepcji społecznej. Przykładem może być wpis Donalda Tuska na platformie „X” z 2020 r., w którym czytamy, że: „Chiny i Rosja rozpoczęły wojnę informacyjną z Zachodem. Główne tezy: »wirus przyszedł z USA« oraz »Unia nic nie robi« rozpowszechniane są przez pożytecznych idiotów, także w Polsce. W czasach prawdziwej zarazy bądźmy odporni na wirus kłamstwa”⁴³.

W procesie sekurytyzacji wojny informacyjnej wykorzystywane są zatem narracje odwołujące się do zagrożenia dla państwa, społeczeństwa i porządku demokratycznego, a także argumenty akcentujące skalę, pilność i szkodliwe konsekwencje tego zjawiska. Można także zauważyć strategie dyskursywne⁴⁴ polegające na wskazywaniu źródła zagrożenia, wykorzystywaniu przekazów emocjonalnych, podkreślaniu wyjątkowości sytuacji i legitymizowaniu potrzeby zastosowania nadzwyczajnych środków ochrony. Wojna informacyjna przedstawiana jest nie jako zwykły element rywalizacji politycznej, ale szczególna forma zagrożenia wymierzona w bezpieczeństwo państwa, stabilność instytucji publicznych, integralność procesu demokratycznego czy bezpośrednio w społeczeństwo.

Sekurytyzacja rosyjskiej wojny informacyjnej w dyskursie Unii Europejskiej i NATO

W dyskursie prowadzonym na forum UE i NATO wojnę informacyjną wyraźnie przesunięto z obszaru zwykłej rywalizacji politycznej do sfery bezpieczeństwa. Dla przykładu zarówno unijne instytucje, jak i Sojusz Północnoatlantycki przedstawiają wrogie działania Rosji w sferze informacyjnej nie jako incydentalne zakłócenia komunikacyjne, lecz jako celowe, skoordynowane i szkodliwe operacje wymierzone w stabilność państw członkowskich, sojuszników, ale także w określone wartości, pro-

43 D. Tusk, *[Chiny i Rosja rozpoczęły wojnę informacyjną z Zachodem]*, „X” [online], 13 III 2020 [dostęp: 18 III 2026]: <<https://x.com/donaldtusk/status/1238435525494747137>>.

44 Strategie dyskursywne rozumiane są w niniejszym artykule za Patrycją Pałką jako „suma decyzji nadawcy co do sposobu przekazu treści w obrębie wybranego gatunku mowy; jest to zaplanowane działanie mowne nastawione na realizację określonego celu komunikacyjnego”. Zob. P. Pałka, *Strategie dyskursywne w rozmowie handlowej*, Wydawnictwo „Śląsk”, Katowice 2009, s. 25.

cesy demokratyczne oraz konkretne społeczności⁴⁵. Mamy zatem do czynienia z klasycznym procesem sekurytyzacji, ponieważ zjawisko nazwane zostało egzystencjalnym zagrożeniem dla bezpieczeństwa, wskazano podmioty zagrożone, a następnie uzasadniano szczególnie środki reakcji⁴⁶.

Środkiem tego rodzaju może być uruchomienie art. 5 *Traktatu północnoatlantyckiego*, który stwierdza:

Strony zgadzają się, że zbrojna napaść na jedną lub więcej z nich w Europie lub Ameryce Północnej będzie uznana za napaść przeciwko nim wszystkim, i dlatego zgadzają się, że jeżeli taka zbrojna napaść nastąpi, to każda z nich, w ramach wykonywania prawa do indywidualnej lub zbiorowej samoobrony, uznanego na mocy artykułu 51 Karty Narodów Zjednoczonych, udzieli pomocy Stronie lub Stronom napadniętym, podejmując niezwłocznie, samodzielnie, jak i w porozumieniu z innymi Stronami działania, jakie uzna za konieczne, łącznie z użyciem siły zbrojnej, w celu przywrócenia i utrzymania bezpieczeństwa obszaru północnoatlantyckiego. O każdej takiej zbrojnej napaści i o wszystkich podjętych w jej wyniku środkach zostanie bezzwłocznie powiadomiona Rada Bezpieczeństwa. Środki takie zostaną zaniechane, gdy tylko Rada Bezpieczeństwa podejmie działania konieczne do przywrócenia i utrzymania międzynarodowego pokoju i bezpieczeństwa⁴⁷.

W komunikacie po szczycie NATO w Brukseli z 2021 r. czytamy natomiast:

W przypadku wojny hybrydowej Rada może podjąć decyzję o powołaniu się na art. 5 traktatu waszyngtońskiego, tak jak w przypadku ataku zbrojnego. [...] Potwierdzając defensywny mandat NATO, Sojusz zdecydowany jest wykorzystywać w każdym czasie pełne spektrum swoich zdolności, aby aktywnie odstraszać, bronić się przed nim i przeciwdziałać całemu

45 *NATO's Approach to Counter Information Threats*, „North Atlantic Treaty Organization” [online], 3 II 2025 [dostęp: 17 III 2026]: <<https://www.nato.int/en/what-we-do/wider-activities/natos-approach-to-counter-information-threats>>.

46 *Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI)*, „European Union External Action” [online], 17 III 2026 [dostęp: 18 III 2026]: <https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en>.

47 Artykuł 5. – *Traktat Północnoatlantycki*. Waszyngton. 1949.04.04, „Wolters Kluwer” [online], 19 X 2000 [dostęp: 17 III 2026]: <<https://sip.lex.pl/akty-prawne/dzu-dzien-nik-ustaw/traktat-polnocnoatlantycki-waszyngton-1949-04-04-16885651/art-5>>.

zakresowi cyberzagrożeń, w tym prowadzonych jako element kampanii hybrydowych, zgodnie z prawem międzynarodowym. Potwierdzamy, że decyzja o tym, kiedy cyberatak prowadziłby do uruchomienia art. 5, będzie podejmowana przez Radę Północnoatlantycką każdorazowo, indywidualnie dla danego przypadku⁴⁸.

Pięć lat wcześniej, podczas szczytu zorganizowanego w Warszawie cyberprzestrzeń została oficjalnie uznana za kolejną sferę działań wojennych. Przyjęto, że cyberataki mogą być równie szkodliwe dla współczesnych społeczeństw co ich konwencjonalne odpowiedniki, dlatego Sojusz musi się bronić w cyberprzestrzeni tak samo skutecznie jak na lądzie, morzu i w powietrzu. Ponadto zadeklarowano współpracę z UE w zakresie cyberbezpieczeństwa⁴⁹. Były to ważne ustalenia, które przyniosły konkretne działania NATO na rzecz rozwoju potencjału w cyberprzestrzeni oraz współpracę między sojusznikami na tym polu.

W zakresie regionalnym UE wprowadza przepisy zwiększające bezpieczeństwo w sieci. Przykładem jest *Akt o usługach cyfrowych*, ale także *Akt o rynkach cyfrowych*, *Akt o sztucznej inteligencji*, *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/900 z dnia 13 marca 2024 r. w sprawie przejrzystości i targetowania reklamy politycznej* czy takie inicjatywy jak włączenie kodeksu postępowania w zakresie zwalczania dezinformacji z 2022 r. do *Aktu o usługach cyfrowych*, Europejska Tarcza Demokracji oraz pakiety sankcji przeciwko rosyjskim podmiotom odpowiedzialnym za kontynuowane przez Rosję operacje informacyjne⁵⁰.

Istotne znaczenie ma w tym zakresie działalność Europejskiej Służby Działań Zewnętrznych (European External Action Service – EEAS)⁵¹,

48 *Brussels Summit Communiqué*, „North Atlantic Treaty Organization” [online], 14 VI 2021 [dostęp: 18 III 2026]: <<https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/06/14/brussels-summit-communication>>.

49 *Warsaw Summit Communiqué*, „North Atlantic Treaty Organization” [online], 9 VII 2016 [dostęp: 18 III 2026]: <<https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/09/warsaw-summit-communication>>.

50 *Timeline – EU Sanctions against Russia*, „European Council. Council of the European Union” [online], 16 III 2026 [dostęp: 19 III 2026]: <<https://www.consilium.europa.eu/en/policies/sanctions-against-russia/timeline-sanctions-against-russia/>>.

51 M. Šenk, N. Hynek, *NATO/EU Synergies against Information Warfare: A „Circulatory Institutional” Model of Expert Voluntarism*, „European Security” 2026, vol. 35,

w centrum zainteresowania której znajdują się obce manipulacje informacyjne i ingerencje (*foreign information manipulation and interference* – FIMI). Skuteczne reagowanie na FIMI jest jednym z priorytetów UE. W marcu 2022 r. przyjęty został Strategiczny Kompas, który zawiera wskazówki i wspólną wizję wzmocnienia unijnej polityki bezpieczeństwa i obrony do 2030 r.⁵² Od tego momentu Unia dąży do standaryzacji sposobów wykrywania i reagowania na FIMI, opierając się na metodzie DISARM, stosowanej m.in. przez Zespół Analizy Danych (Data Analysis Team) w Wydziale Komunikacji Strategicznej, Grup Zadaniowych i Analiz Informacyjnych (SG.STRAT.2) EEAS⁵³. Dzięki niej możliwe jest wprowadzanie do wspólnej bazy danych analizy stosowanych taktyk, technik i procedur, a także informacji na temat infrastruktury wykorzystywanej do przeprowadzenia operacji wpływu⁵⁴. O efektach prac EEAS można przeczytać w opublikowanym w marcu 2026 r. raporcie na temat zagrożeń FIMI, który przedstawia wzmocnioną strategię Unii na rzecz przeciwdziałania podstawowym operacjom FIMI poprzez identyfikację luk w łańcuchu dostaw informacji oraz infrastruktury informacyjnej FIMI⁵⁵. W marcu 2022 r. Rada UE wprowadziła przełomowe sankcje, które ograniczyły nadawanie rosyjskich mediów państwowych Russia Today i Sputnik wobec inwazji na Ukrainę⁵⁶.

No. 2: <<https://www.tandfonline.com/doi/epdf/10.1080/09662839.2025.2566519?nedAccess=true>> [dostęp: 8 V 2026].

- 52 „Strategiczny kompas” na rzecz bezpieczeństwa i obrony, „Rada Europejska. Rada Unii Europejskiej” [online], 28 VIII 2025 [dostęp: 9 V 2026]: <<https://www.consilium.europa.eu/pl/policies/strategic-compass/>>.
- 53 *Foreign Information Manipulation and Interference in Third Countries*, Trade and Technology Council, [b.d.m.w.]: <https://www.eeas.europa.eu/sites/default/files/documents/2023/Annex%203%20-%20FIMI_29%20May.docx.pdf> [dostęp: 9 V 2026].
- 54 F. Bryjka, *Podejście UE do zwalczania obcych manipulacji informacyjnych i ingerencji*, „Polski Instytut Spraw Międzynarodowych” [online], 19 VI 2024 [dostęp: 9 V 2026]: <<https://www.pism.pl/publikacje/podejscie-ue-do-zwalczania-obcych-manipulacji-informacyjnych-i-ingerencji>>.
- 55 *4th EEAS Report on Foreign Information Manipulation and Interference Threats*, European Union External Action, [b.m.w.], 10 III 2026: <https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web%20version_1.pdf> [dostęp: 9 V 2026].
- 56 S. L. Vérieter, *The Collective Securitization of „Disinformation” and the EU’s Ban on Russia Today and Sputnik*, „International Affairs” 2025, vol. 101, issue 5: <<https://doi.org/10.1093/ia/iaf139>> [dostęp: 4 V 2026].

Nie wszystkie z wymienionych inicjatyw można uznać za środki nadzwyczajne, ale w logice sekurytyzacji są to przykłady działań podejmowanych m.in. dlatego, że wojnę informacyjną uznano za zagrożenie dla bezpieczeństwa wspólnoty.

Konsekwencje sekurytyzacji wojny informacyjnej

Sekurytyzacja wojny informacyjnej wywołuje istotne konsekwencje polityczne, prawne i społeczne. W nawiązaniu do powyższych rozważań w kontekście Polski możemy je rozpatrywać zarówno w wymiarze wewnętrznym, jak i szerzej – w międzynarodowym. Dla obszaru państwowego pierwszą konsekwencją jest wzrost znaczenia bezpieczeństwa informacyjnego, w tym cyberbezpieczeństwa, jako osobnego komponentu bezpieczeństwa narodowego. Ponadto sekurytyzacja wojny informacyjnej prowadzi do zmilitaryzowania sposobu myślenia o nim, pomimo że wojna – będąca domeną instytucji wojskowych i charakteryzująca się użyciem siły – jest tutaj wyłącznie metaforą⁵⁷.

Drugim skutkiem sekurytyzacji wojny informacyjnej w Polsce jest rozwój instytucji, procedur i instrumentów przeciwdziałania dezinformacji, cyberzagrożeniom i operacjom wpływu. W ostatnim czasie mamy do czynienia z przebudową architektury systemu cyberbezpieczeństwa w Polsce. Przykładowo w zakresie normatywnym na początku 2026 r. pojawiła się nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa, która wdraża dyrektywę Parlamentu Europejskiego i Rady 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, skrótowo nazywaną NIS 2⁵⁸. Dodatkowo w marcu tego roku Rada Ministrów przyjęła nową strategię cyberbezpieczeństwa Rzeczypospolitej Polskiej, wskazując, że dokument ten wyzna-

57 M. Górka, *Conceptualising...*, s. 279.

58 Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, Dz.U. 2026, poz. 252; Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2), Dz.Urz. UE, L 333, 27 XII 2022: <<https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32022L2555>> [dostęp: 18 III 2026].

cza kierunki rozwoju bezpieczeństwa cyfrowego państwa i ma wzmocnić Krajowy System Cyberbezpieczeństwa, a jego realizacja zwiększy odporność Polski na cyberzagrożenia oraz poprawi bezpieczeństwo obywateli, przedsiębiorstw i instytucji publicznych⁵⁹.

Kolejną konsekwencją sekurytyzacji wojny informacyjnej może być wzrost znaczenia edukacji i odporności społecznej. Uznanie wojny informacyjnej za zagrożenie dla bezpieczeństwa sprzyja podejmowaniu działań ukierunkowanych na rozwijanie wśród obywateli kompetencji cyfrowych. Ich celem jest na przykład wzmacnianie kompetencji w zakresie rozpoznawania dezinformacji, krytycznej oceny przekazów medialnych oraz świadomego uczestnictwa w debacie publicznej, zwłaszcza tej prowadzonej za pośrednictwem mediów społecznościowych.

Jednocześnie zjawisko sekurytyzacji wojny informacyjnej niesie za sobą ryzyko nadużyć politycznych. W sytuacji, gdy pojęcie *wojna informacyjna* zaczyna funkcjonować jako kategoria upolityczniona, może być wykorzystywane nie tylko do opisu rzeczywistych zagrożeń, ale także do delegitymizowania krytyki (np. ze strony opozycji czy organizacji pozarządowych), wzmacniania polaryzacji społecznej, ale także uzasadniania bardziej zaostrzonych form kontroli komunikacji. Szczególnie istotne wydaje się napięcie między potrzebą zapewnienia bezpieczeństwa a ograniczeniami wolności słowa, pluralizmu debaty publicznej i otwartości komunikacyjnej. W szerszej perspektywie sekurytyzacja wojny informacyjnej może wpływać na funkcjonowanie demokracji i praw obywatelskich, ponieważ grozi ograniczeniem standardowych procedur demokratycznych w imię przeciwdziałania zagrożeniom przedstawianym jako egzystencjalne, wyjątkowe i niecierpiące zwłoki.

Ciekawe spostrzeżenia przedstawia w artykule *Digital Im/materiality and the Securitisation of Cyber* Håvard Rustad Markussen, badacz z Nordisk institutt for studier av innovasjon, forskning og utdanning w Oslo. Opisuje mianowicie kontrowersje, jakie wzbudziło w Norwegii masowe przechwytywanie komunikacji elektronicznej stanowiące przykład procesu sekurytyzacji, w którym niejasne i abstrakcyjne pojęcia cyfrowości oraz częste

59 *Nowa strategia cyberbezpieczeństwa. Polska wzmacnia ochronę przed cyberatakami*, „Ministerstwo Cyfryzacji” [online], 10 III 2026 [dostęp: 18 III 2026]: <<https://www.gov.pl/web/cyfryzacja/nowa-strategia-cyberbezpieczenstwa-polska-wzmacnia-ochrone-przed-cyberatakami>>.

odwoływanie się do niematerialnej natury tej cyfrowości odgrywają istotną rolę w legitymizacji wdrożenia nowego, bardziej inwazyjnego systemu nadzoru państwa nad cyberprzestrzenią⁶⁰.

Oprócz przechwytywania komunikacji władze państwowe mogą stosować wiele innych nadzwyczajnych środków w imię zapewnienia obywatelom cyberbezpieczeństwa. W ostatnim czasie obserwujemy próby rozszerzania kompetencji nadzorczych wobec operatorów, platform i użytkowników. W demokracjach liberalnych, w tym w państwach UE i Wielkiej Brytanii, rozszerzanie tych kompetencji wobec operatorów i platform cyfrowych zazwyczaj przybiera formę regulacji mających przeciwdziałać nielegalnym treściom, dezinformacji i zagrożeniom dla użytkowników, choć również tam tego typu działania wywołują spory o proporcjonalność metod czy ograniczenia wolności wypowiedzi. W państwach autorytarnych, jak np. Chiny czy Rosja, polityka cyberbezpieczeństwa przekształca się natomiast w narzędzie kontroli społecznej.

Elementem polityki bezpieczeństwa państwa są regulacje prawne. W zakresie bezpieczeństwa informacyjnego ich wprowadzenie nierzadko wiąże się z szeroką debatą, w której swoje argumenty przedstawiają zarówno zwolennicy, jak i przeciwnicy proponowanych inicjatyw. Regulacje wprowadzające ograniczenia praw i wolności obywateli w imię cyberbezpieczeństwa budzą kontrowersje i niejednokrotnie przyczyniają się do zaostżenia polaryzacji społecznej, która jest charakterystyczna dla polskiego społeczeństwa. Przykładem może być rządowy projekt ustawy o zmianie ustawy o świadczeniu usług drogą elektroniczną oraz niektórych innych ustaw, której przepisy miały wdrażać do polskiego porządku prawnego zapisy unijnego rozporządzenia pn. *Akt o usługach cyfrowych (Digital Services Act – DSA)*. Ustawa została uchwalona w grudniu 2025 r. W uzasadnieniu nowelizacji czytamy, że jest konieczna do zapewnienia stosowania rozporządzenia Parlamentu Europejskiego i Rady UE 2022/2065 z 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (aktu o usługach cyfrowych). Wskazano ponadto, że unijne rozporządzenie ma na celu:

60 H. R. Markussen, *Digital Im/materiality and the Securitisation of Cyber*, „European Journal of International Security” 2025: <<https://doi.org/10.1017/eis.2025.10012>> [dostęp: 20 III 2026].

stworzenie bezpieczniejszego środowiska internetowego dla konsumentów i przedsiębiorstw w Unii Europejskiej (UE), wprowadzając zestaw przepisów, których zadaniem jest:

- skuteczniejsza ochrona odbiorców usługi i ich praw podstawowych;
- określenie jasnych obowiązków dla dostawców usług pośrednich;
- zwalczanie nielegalnych treści, usług lub produktów, m.in. przez obowiązek wdrożenia przez dostawców usługi *hostingu* mechanizmu zgłaszania i działania (ang. *notice and action*);
- osiągnięcie większej przejrzystości przez lepszą sprawozdawczość i nadzór⁶¹.

Rząd podkreślał, że regulacje mają zapewnić skuteczniejszą walkę z hejtem, dezinformacją, treściami pedofilskimi i innymi nielegalnymi materiałami w sieci⁶². W styczniu 2026 r. prezydent Karol Nawrocki odmówił jednak podpisania ustawy, wskazując w uzasadnieniu m.in. na sprzeczność proponowanych przepisów z konstytucyjną zasadą wolności wypowiedzi⁶³. Widać tutaj dwa odmienne sposoby rozumienia bezpieczeństwa i wolności w internecie. Z jednej strony projekt ustawy przedstawiany był jako narzędzie ochrony użytkowników przed nielegalnymi treściami, oszustwami i wykorzystywaniem dzieci w cyberprzestrzeni, a także jako mechanizm wzmacniający pozycję obywatela wobec platform cyfrowych poprzez wprowadzenie ścieżek odwoławczych od decyzji moderatorów. Z drugiej strony jego krytycy wskazywali, że proponowane rozwiązania mogą stworzyć podstawy do nadmiernej ingerencji państwa w sferę komunikacji *online*, a w konsekwencji prowadzić do ograniczania wolności słowa pod pozorem walki z zagrażającymi obywatelom treściami. Odbiór dokumentu wśród

61 *Uzasadnienie*, [Sejm Rzeczypospolitej Polskiej, Warszawa], 29 IX 2025: <<https://orka.sejm.gov.pl/Druki10ka.nsf/o/BBC447BFD5BB3152C1258D1B004435D1/%24F1le/1757-uzasadnienie.docx>> [dostęp: 19 III 2026].

62 *Walka z dezinformacją i ochrona przed nielegalnymi treściami w internecie*, „Kancelaria Prezesa Rady Ministrów” [online], 29 IX 2025 [dostęp: 19 III 2026]: <<https://www.gov.pl/web/premier/walka-z-dezinformacja-i-ochrona-przed-nielegalnymi-treściami-w-internecie>>.

63 *Wniosek Prezydenta RP o ponowne rozpatrzenie ustawy z dnia 18 grudnia 2025 r. o zmianie ustawy o świadczeniu usług drogą elektroniczną oraz niektórych innych ustaw*, „Sejm Rzeczypospolitej Polskiej” [online], 9 I 2026 [dostęp: 19 III 2026]: <<https://www.sejm.gov.pl/Sejm10.nsf/druk.xsp?nr=2171>>.

społeczeństwa i organizacji pozarządowych również nie był jednoznaczny, ale wyraźnie spolaryzowany. Proces sekurytyzacji może więc też sprzyjać polaryzacji społecznej, gdyż poprzez nazywanie określonych zjawisk zagrożeniami egzystencjalnymi przesuwają się debatę z obszaru zwykłej rywalizacji politycznej do sfery bezpieczeństwa, co wzmacnia podziały i wprowadza skrajne emocje związane z proponowanymi przez władze środkami przeciwdziałania zagrożeniom.

Na poziomie międzynarodowym jedną z konsekwencji sekurytyzowania wojny informacyjnej jest instytucjonalizacja zagrożenia. Wojna informacyjna nie jest już traktowana jako temat poboczny, ale obszar wymagający stałego monitoringu, konsultacji politycznych i odpowiedzi zbiorowej. Widoczne są rozwój nowych instrumentów reakcji oraz debata nad możliwymi konsekwencjami wrogich cyberoperacji zarówno w UE, jak i NATO. Problemem może stać się potencjalna pokusa traktowania przestrzeni komunikacyjnej jako obszaru wymagającego większego nadzoru, filtrowania i wyjątkowych interwencji.

Dodajmy tu, że sekurytyzacja wojny informacyjnej nie powinna być analizowana wyłącznie jako zjawisko dyskursywne czy polityczne. Jej konsekwencje mają także wymiar prawny, gdyż uznanie określonych działań o charakterze informacyjnym za egzystencjalne zagrożenie dla państwa, społeczeństwa i porządku konstytucyjnego może skutkować uznaniem dopuszczalności stosowania środków nadzwyczajnych. W tym sensie akt sekurytyzacji jest punktem wyjścia do rozszerzenia dopuszczalnej ingerencji państwa w sfery m.in. komunikacji, mediów, infrastruktury cyfrowej oraz praw i wolności człowieka. Sekurytyzacja wojny informacyjnej może więc uzasadniać stosowanie szczególnych instrumentów prawnych, takich jak choćby wzmożony nadzór nad przestrzenią cyfrową, regulacje dotyczące platform internetowych i mediów czy sankcje wobec podmiotów indywidualnych. Środki te mogą być przedstawiane jako konieczne dla ochrony bezpieczeństwa państwa, integralności procesów demokratycznych czy zachowania odporności informacyjnej państwa. Jednocześnie jednak warto pamiętać, że ich stosowanie wymaga zachowania standardów państwa prawa, np. zasady proporcjonalności, którą można nazwać zakazem nadmiernej ingerencji. Zakłada ona, że „środki zastosowane do osiągnięcia założonego przez prawodawcę celu (w szczególności takie środki, których zastosowanie koliduje z usprawiedliwionymi interesami obywateli

tela) były do tego celu proporcjonalne⁶⁴. Ponadto dopuszczalność stosowania przez państwo środków nadzwyczajnych w odpowiedzi na zagrożenia o charakterze informacyjnym powinna być oceniana w świetle międzynarodowych standardów ochrony praw człowieka, zwłaszcza art. 19 *Międzynarodowego Paktu Praw Obywatelskich i Politycznych*, który dotyczy prawa do swobodnego wyrażania opinii, oraz art. 10 *Europejskiej Konwencji Praw Człowieka* z 1950 r., który stwierdza, że „każdy ma prawo do wolności wyrażania opinii”⁶⁵.

Kolejną istotną kwestią z punktu widzenia prawa jest atrybucja, czyli przypisanie odpowiedzialności za operacje informacyjne⁶⁶. Tego typu działania często prowadzone są przez podmioty trudne do jednoznacznego zidentyfikowania, np. służby specjalne, grupy hakerskie, kolektywy haktivistów, podmioty indywidualne lub inne działające w interesie obcych państw. Wobec tego przypisanie odpowiedzialności konkretnemu państwu lub organizacji napotyka na poważne trudności dowodowe i prawne. Ustalenie odpowiedzialności państwa wymaga wykazania powiązania między tymi podmiotami a organami państwowymi albo udowodnienia, że działały one pod kierownictwem, kontrolą lub na zlecenie danego państwa⁶⁷. Ma to istotne znaczenie zarówno na gruncie prawa międzynarodowego, jak i krajowego, ponieważ od ustalenia sprawcy zależy możliwość zastosowania sankcji, środków odwetowych, odpowiedzialności karnej czy administracyjnej lub reakcji na szczeblu dyplomatycznym.

64 L. Garlicki, *Polskie prawo konstytucyjne*, Wydawnictwo „Liber”, Warszawa 2010, s. 64.

65 *Międzynarodowy Pakt Praw Obywatelskich i Politycznych* otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r., Dz.U. 1977, nr 38, poz. 167: <<https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19770380167>> [dostęp: 9 v 2026]; *Europejska Konwencja Praw Człowieka po nowelizacji przez Protokół nr 11, 14 i 15 z Protokołami nr 1 oraz Protokołami nr 4, 6, 7, 12, 13 i 16*, Europejski Trybunał Praw Człowieka, Council of Europe, Strasbourg [b.r.w.]: <https://www.echr.coe.int/documents/d/echr/convention_POL> [dostęp: 9 v 2026].

66 *Responsibility of States for Internationally Wrongful Acts*, United Nations, [New York] 2005: <https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf> [dostęp: 9 v 2026].

67 M. Milanovic, *Special Rules of Attribution of Conduct in International Law*, Stockton Center for International Law, [Stockton] 2020 (*International Law Studies*, 295, 96): <<https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2926&context=ils>> [dostęp: 8 v 2026].

Normy prawa międzynarodowego – zarówno wynikające z traktatów, jak i innych źródeł prawa, w szczególności międzynarodowego prawa zwyczajowego – znajdują zastosowanie do działań w cyberprzestrzeni. Stanowisko, zgodnie z którym istniejące normy prawa międzynarodowego stosują się do cyberprzestrzeni, wyraziły dotychczas m.in. Unia Europejska, Organizacja Traktatu Północnoatlantyckiego, Grupa Ekspertów Rządowych przy ONZ (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security – UN GGE) oraz szereg państw, w tym Polska. W 2022 r. z inicjatywy Ministerstwa Spraw Zagranicznych rząd przyjął *Stanowisko Rzeczypospolitej Polskiej dotyczące zastosowania prawa międzynarodowego w cyberprzestrzeni*⁶⁸.

W prawie międzynarodowym szczególne znaczenie ma rozróżnienie między działaniami poniżej progu użycia siły a tymi, które mogłyby zostać zakwalifikowane jako naruszenie art. 2 (4) *Karty Narodów Zjednoczonych*, który ustanawia zakaz użycia siły lub groźby jej użycia w stosunkach międzynarodowych⁶⁹. Większość operacji informacyjnych, nawet jeżeli są politycznie szkodliwe i destabilizujące, nie osiąga progu użycia siły w rozumieniu prawa międzynarodowego. Mogą jednak naruszać zakaz interwencji w wewnętrzne sprawy państwa, jeżeli ingerują w kwestie należące do suwerennej kompetencji państwa, takie jak wybory, procesy decyzyjne czy funkcjonowanie instytucji publicznych, oraz mają charakter przymusu, rozumianego jako wywieranie presji zmierzającej do wymuszenia określonego działania, zaniechania lub ograniczenia swobody decyzyjnej państwa⁷⁰.

W zakresie stosowania prawa międzynarodowego w cyberprzestrzeni wpływowym źródłem wiedzy jest opublikowane w 2013 r. eksperckie opracowanie *Tallinn Manual*, dotyczące cyberoperacji naruszających zakaz użycia siły, dających państwom prawo do samoobrony oraz tych, które prowadzone są w czasie konfliktu zbrojnego. W 2017 r. opublikowany został

68 *Stanowisko Rzeczypospolitej Polskiej dotyczące zastosowania prawa międzynarodowego w cyberprzestrzeni*, „Ministerstwo Spraw Zagranicznych” [online], 29 XII 2022 [dostęp: 29 V 2026]: <<https://www.gov.pl/web/dyplomacja/stanowisko-rzeczypospolitej-polskiej-dotyczace-zastosowania-prawa-miedzynarodowego-w-cyberprzestrzeni>>.

69 *Karta Narodów Zjednoczonych*, Dz.U. 1947, nr 23, poz. 90: <<https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19470230090/O/D19470090.pdf>> [dostęp: 9 V 2026].

70 *Use of Force*, „Cyber Law Toolkit” [online, dostęp: 9 V 2026]: <https://cyberlaw.ccd-coe.org/wiki/Use_of_force>.

Tallin Manual 2.0, który uwzględnia zasady prawa międzynarodowego regulujące incydenty cyberbezpieczeństwa, z którymi państwa spotykają się na co dzień, a które nie spełniają kryteriów użycia siły i występują w czasie pokoju. Oba te dokumenty mają istotne znaczenie dla analizy sekurytyzacji wojny informacyjnej, ponieważ pozwalają uchwycić granicę między politycznym dyskursem o zagrożeniu a prawnomiędzynarodową kwalifikacją określonych działań⁷¹.

Podsumowując, należy stwierdzić, że sekurytyzacja może poprawiać zdolności ochronne, ale także zwiększać ryzyko cenzury, poszerzania regulacji i podporządkowania debaty publicznej logice bezpieczeństwa. W kontekście stosunków międzynarodowych i układu sił na międzynarodowej arenie politycznej narracje przypisujące odpowiedzialność za cyberzagrożenia podmiotom pochodzącym z Rosji, Chin, Iranu czy Korei Północnej obecne są w dyskursie politycznym od wielu lat i opierają się na utrwalonych relacjach antagonizmu między tymi państwami a Zachodem⁷². W ramach tych narracji pojawiają się scenariusze potencjalnych cyberoperacji, stanowiących zagrożenia, które mogą powodować skutki porównywalne do ataków konwencjonalnych, czyli utratę zdrowia lub życia ludzi czy też uszkodzenie mienia, np. w rezultacie ataków na infrastrukturę krytyczną.

Podsumowanie

Ingerencja państwa w sferę prywatności obywateli, nadzór cyfrowy na masową skalę, inwigilacja, blokowanie stron internetowych i aplikacji, a także ograniczenia dostępu do sieci lub celowe spowalnianie internetu to tylko część środków, które państwa wdrażają w imię zapewnienia obywatelom bezpieczeństwa w cyberprzestrzeni. Niejednokrotnie to identyfikacja danego problemu jako zagrożenia o charakterze egzystencjalnym w zakresie szeroko pojętego bezpieczeństwa informacyjnego legitymizuje

71 *The Tallinn Manual*, „The NATO Cooperative Cyber Defence Centre of Excellence” [online], 9 V 2026 [dostęp: 9 V 2026]: <<https://ccdcoe.org/research/tallinn-manual/>>; *Rule 66 – Intervention by States*, [w:] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, ed. M. N. Schmitt, United States Naval War College, Newport, 3 II 2017: <<https://doi.org/10.1017/9781316822524>> [dostęp: 9 V 2026].

72 M. Górka, *Conceptualising...*, s. 285.

zastosowanie nadzwyczajnych środków w celu jego zwalczenia⁷³. W procesie sekurytyzacji decydenci polityczni nierzadko wyolbrzymiają pilność i skalę zagrożenia, przedstawiając je jako egzystencjalne, co służy legitymizacji nadzwyczajnych środków przeciwdziałania i przesunięciu problemu poza ramy zwykłej polityki, a niekiedy wręcz ujmowaniu go w kategoriach militarnych.

Uznanie dezinformacji, propagandy czy manipulacji za zagrożenie dla bezpieczeństwa nie może stanowić upoważnienia do cenzury, uznaniowego blokowania treści, ograniczania działalności mediów lub nadmiernego nadzoru nad komunikacją w przestrzeni cyfrowej. Państwo powinno odróżniać skoordynowane operacje wpływu prowadzone przez aktorów zewnętrznych od legalnej debaty publicznej, krytyki politycznej i działalności dziennikarskiej. W przeciwnym razie sekurytyzacja może prowadzić do rozszerzenia kompetencji organów bezpieczeństwa kosztem pluralizmu, wolności słowa i oddolnej demokratycznej kontroli obywateli nad władzą.

Istotną rolę w przedstawionej analizie odgrywa również perspektywa prawa międzynarodowego. Normy prawnomiędzynarodowe wyznaczają granice odpowiedzialności państw oraz dopuszczalności środków reakcji. Punktem odniesienia jest tu zakaz użycia siły wynikający z art. 2 (4) *Karty Narodów Zjednoczonych*, a także zakaz interwencji w wewnętrzne sprawy państw, który może zostać naruszony w przypadku działań ingerujących w wybory, procesy decyzyjne lub funkcjonowanie instytucji publicznych, które mają charakter przymusu. Dodatkowo operacje informacyjne mogą być oceniane przez pryzmat zasady suwerenności, zwłaszcza gdy zakłócają działalność organów państwa⁷⁴. Kwestia odpowiedzialności państwa wymagała natomiast odwołania się do zasad atrybucji określonych w przygotowanym przez ONZ dokumencie *Responsibility of States for Internationally Wrongful Acts*. Ponadto dopuszczalność stosowania przez państwo środków nadzwyczajnych w odpowiedzi na zagrożenia o charakterze informacyjnym powinna być oceniana w świetle międzynarodowych standardów ochrony praw człowieka, zwłaszcza art. 19 *Międzynarodowego*

73 M. Flohr, *Key Concept: Securitization (Copenhagen School)*, „Critical Legal Thinking” [online], 13 III 2025 [dostęp: 19 I 2026]: <<https://criticallegalthinking.com/2025/03/31/key-concept-securitization-copenhagen-school/>>.

74 *Stanowisko Rzeczypospolitej Polskiej...*

Paktu Praw Obywatelskich i Politycznych oraz art. 10 Europejskiej Konwencji Praw Człowieka.

Jak wskazuje Clara Eroukhmanoff,

kwestia staje się sekurytyzowana, gdy społeczność zbiorowo zgadza się co do charakteru zagrożenia i popiera podjęcie nadzwyczajnych środków. Jeśli społeczność odrzuca akt mowy podmiotu sekurytyzującego, stanowi to jedynie ruch sekurytyzujący, a sekurytyzacja kończy się niepowodzeniem⁷⁵.

W sytuacji, gdy podmioty sekurytyzujące mówią, że wojna informacyjna stanowi egzystencjalne zagrożenie dla państwa lub demokracji, nie tylko opisują rzeczywistość, ale też próbują ją współtworzyć. Tego rodzaju wypowiedzi mają skłonić odbiorców do uznania, że zagrożenie ma charakter wyjątkowy i że zwykłe środki polityczne nie wystarczą, by się z nim uporać.

Przeprowadzona analiza pozwala potwierdzić hipotezę, że sekurytyzacja wojny informacyjnej w stosunkach międzynarodowych oznacza przesunięcie oddziaływań informacyjnych z obszaru zwykłej rywalizacji politycznej do sfery bezpieczeństwa, w której dezinformacja, propaganda, operacje wpływu czy FIMI interpretowane są jako zagrożenia dla bezpieczeństwa. Taka interpretacja pozwala zaś państwom i organizacjom międzynarodowym uzasadnić szczególne środki reakcji wobec praktyk w przestrzeni cyfrowej. Granicę dopuszczalnych działań państwa wyznaczają zasady legalności i proporcjonalności, a także ochrona praw człowieka oraz standardy prawa międzynarodowego i regionalnego.

Niniejszy artykuł zwraca uwagę na problem nadużywania terminu *wojna informacyjna* przez decydentów politycznych oraz jego niejednoznaczne definiowanie. Choć praca nie wyczerpuje szerokiej problematyki sekurytyzacji, koncentruje się na analizie sekurytyzowania wojny informacyjnej na przykładzie wybranych wypowiedzi polskich polityków oraz omawia podejmowane przez Unię Europejską i NATO działania, które można uznać za jedne z rezultatów tego procesu w sferze stosunków międzynarodowych.

75 C. Eroukhmanoff, *Securitisation...*

Bibliografia

- Adamczyk M., Maćkowiak M., „*Protecting Americans from Foreign Adversary Controlled Applications Act*”, czyli kolejna odsłona amerykańsko-chińskiej wojny o TikTok. Analiza z perspektywy teorii sekurytyzacji szkoły kopenhaskiej, „*Studia Orientalne*” 2025, R. 14, nr 1 (33): <<https://doi.org/10.15804/so2025101>> [dostęp: 16 II 2026].
- Artykuł 5. – *Traktat Północnoatlantycki*. Waszyngton. 1949.04.04, „Wolters Kluwer” [online], 19 X 2000 [dostęp: 17 III 2026]: <<https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/traktat-polnocnoatlantycki-waszyngton-1949-04-04-16885651/art-5>>.
- Austin J. L., *How to Do Things with Words*, Oxford at the Clarendon Press, Oxford 1962: <https://pure.mpg.de/rest/items/item_2271128/component/file_2271430/content> [dostęp: 29 V 2026].
- Brussels Summit Communiqué, „North Atlantic Treaty Organization” [online], 14 VI 2021 [dostęp: 18 III 2026]: <<https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/06/14/brussels-summit-communique>>.
- Bryjka F., *Podejście UE do zwalczania obcych manipulacji informacyjnych i ingerencji*, „Polski Instytut Spraw Międzynarodowych” [online], 19 VI 2024 [dostęp: 9 V 2026]: <<https://www.pism.pl/publikacje/podejscie-ue-do-zwalczania-obcych-manipulacji-informacyjnych-i-ingerencji>>.
- Buzan B., Wæver O., Wilde J. de, *Security. A New Framework for Analysis*, Lynne Rienner Publishers, Boulder–London 2022.
- Czaputowicz J., *Teorie stosunków międzynarodowych*, Wydawnictwo Naukowe PWN, Warszawa 2022.
- Derrida J., *Signature Event Context*, [w:] J. Derrida, *Limited Inc*, Northwestern University Press, Evanston 1988: <<https://lab404.com/misc/ltdinc.pdf>> [dostęp: 29 V 2026].
- Dunn Cavelty M., *Cyber-Security and Threat Politics. US Efforts to Secure the Information Age*, Routledge, London–New York 2008: <https://www.researchgate.net/publication/277714726_Cyber-Security_and_Threat_Politics_US_Efforts_to_Secure_the_Information_Age> [dostęp: 19 III 2026].
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2), Dz.Urz. UE, L 333, 27 XII 2022: <<https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32022L2555>> [dostęp: 18 III 2026].
- Eroukhmanoff C., *Securitisation Theory: An Introduction*, „E-International Relations” [online], 14 I 2018 [dostęp: 18 I 2026]: <<https://www.e-ir.info/2018/01/14/securitisation-theory-an-introduction/>>.
- Europejska Konwencja Praw Człowieka po nowelizacji przez Protokół nr 11, 14 i 15 z Protokołem nr 1 oraz Protokołami nr 4, 6, 7, 12, 13 i 16, Europejski Trybunał

- Praw Człowieka, Council of Europe, Strasbourg [b.r.w.]: <https://www.echr.coe.int/documents/d/echr/convention_POL> [dostęp: 9 V 2026].
- Fijałkowski Ł., *Studia nad sekurytyzacją – między kontynuacją a krytyką*, „Wiedza Obronna” 2025, t. 291, nr 2.
- Fijałkowski Ł., *Teoria sekurytyzacji i konstruowanie bezpieczeństwa*, „Przegląd Strategiczny” 2012, nr 1.
- Flohr M., *Key Concept: Securitization (Copenhagen School)*, „Critical Legal Thinking” [online], 13 III 2025 [dostęp: 19 I 2026]: <<https://criticallegalthinking.com/2025/03/31/key-concept-securitization-copenhagen-school/>>.
- Foreign Information Manipulation and Interference in Third Countries*, Trade and Technology Council, [b.d.m.w.]: <https://www.eeas.europa.eu/sites/default/files/documents/2023/Annex%203%20-%20FIMI_29%20May.docx.pdf> [dostęp: 9 V 2026].
- [Fourth] 4th EEAS Report on Foreign Information Manipulation and Interference Threats, European Union External Action, [b.m.w.], 10 III 2026: <https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web%20version_1.pdf> [dostęp: 9 V 2026].
- Garlicki L., *Polskie prawo konstytucyjne*, Wydawnictwo „Liber”, Warszawa 2010.
- Gawkowski: w cyberprzestrzeni trwa dzisiaj wojna Rosji z Polską, „Polska Agencja Prasowa” [online], 7 I 2025 [dostęp: 17 III 2026]: <<https://www.pap.pl/aktualnosci/gawkowski-w-cyberprzestrzeni-trwa-dzisiaj-wojna-rosji-z-polska>>.
- Górka M., *Conceptualising Securitisation in the Field of Cyber Security Policy*, „Journal of Modern Science” 2023, t. 4/53.
- Heywood A., *Politologia*, Wydawnictwo Naukowe PWN, Warszawa 2006.
- Incydenty na polskiej granicy. Doradca ministra obrony mówi wprost. „Jesteśmy w stanie wojny informacyjnej”*, „Onet” [online], 3 II 2026 [dostęp: 18 III 2026]: <<https://wiadomosci.onet.pl/kraj/ilu-polakow-jest-gotowych-bronic-kraju-doradca-szefa-mon-mierzymy-regularnie/mpleyqe>>.
- Informacja Ministra Spraw Zagranicznych o zadaniach polskiej polityki zagranicznej w 2026 r. (tekst wystąpienia)*, „Sejm Rzeczypospolitej Polskiej” [online], 26 II 2026 [dostęp: 18 III 2026]: <<https://www.sejm.gov.pl/Sejm10.nsf/komunikat.xsp?documentId=002995D79C288E3DC1258DAA003F5DE7>>.
- Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI)*, „European Union External Action” [online], 17 III 2026 [dostęp: 18 III 2026]: <https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en>.
- Kalpokas I., *Post-Truth and Information Warfare in Their Technological Context*, „ACIG” 2024, vol. 3, No. 2.
- Karta Narodów Zjednoczonych, Dz.U. 1947, nr 23, poz. 90: <<https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19470230090/O/D19470090.pdf>> [dostęp: 9 V 2026].
- Karyotis G., Paterson I., Judge A., *Understanding Securitization Success: A New Analytical Framework*, „International Studies Review” 2025, vol. 27, issue 1: <<https://academic.oup.com/isr/article/27/1/viafo06/8100844>> [dostęp: 18 III 2026].

- Kiera J., *Wojna informacyjna w polityce zagranicznej Federacji Rosyjskiej wobec Polski w latach 2010–2022*, rozprawa doktorska, Uniwersytet Śląski, Katowice 2025: <https://bip.us.edu.pl/sites/default/files/2025-07/Rozprawa_doktorska.pdf> [dostęp: 18 III 2026].
- Konferencja SECURE 2024 | Globalne cyberbezpieczeństwo w obliczu nowej zimnej wojny, „You Tube. NASK PIB” [online], 16 IV 2024 [dostęp: 18 III 2026]: <<https://www.youtube.com/watch?v=wLjScGLhJCQ&t=608s>>.
- Krauz-Mozer B., *Teorie polityki. Założenia metodologiczne*, Wydawnictwo Naukowe PWN, Warszawa 2007.
- Krzysztof Gawkowski: cyfrowe czołgi stoją na naszych ulicach | Gość Poranka, „You Tube. TVP Info” [online], 6 X 2025 [dostęp: 18 III 2026]: <<https://www.youtube.com/watch?v=v83Vx6lKThO&t=>>>.
- Maikowski D., „Jesteśmy w stanie zimnej cyberwojny z Rosją”. Gawkowski ostrzega, „Gazeta” [online], 16 IV 2024 [dostęp: 15 III 2026]: <<https://next.gazeta.pl/next/7,151243,30890519,jestesmy-w-stanie-zimnej-cyberwojny-z-rosja-gawkowski-ostrzega.html>>.
- Markussen H. R., *Digital Im/materiality and the Securitisation of Cyber*, „European Journal of International Security” 2025: <<https://doi.org/10.1017/eis.2025.10012>> [dostęp: 20 III 2026].
- Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r., Dz.U. 1977, nr 38, poz. 167: <<https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdm19770380167>> [dostęp: 9 V 2026].
- Milanovic M., *Special Rules of Attribution of Conduct in International Law*, Stockton Center for International Law, [Stockton] 2020 (International Law Studies, 295, 96): <<https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2926&context=ils>> [dostęp: 8 V 2026].
- NATO's Approach to Counter Information Threats, „North Atlantic Treaty Organization” [online], 3 II 2025 [dostęp: 17 III 2026]: <<https://www.nato.int/en/what-we-do/wider-activities/natos-approach-to-counter-information-threats>>.
- Notions of Disinformation and Related Concepts (ERGA Report), European Regulators Group for Audiovisual Media Services, [b.d.m.w.]: <https://media-board.europa.eu/document/download/00eeb7c2-1abc-443f-9ead-f103b6b577fo_en?filename=ERGA-SG2-Report-2020-Notions-of-disinformation-and-related-concepts-final.pdf&prefLang=sk> [dostęp: 18 III 2026].
- Nowa strategia cyberbezpieczeństwa. Polska wzmacnia ochronę przed cyberatakami, „Ministerstwo Cyfryzacji” [online], 10 III 2026 [dostęp: 18 III 2026]: <<https://www.gov.pl/web/cyfryzacja/nowa-strategia-cyberbezpieczenstwa-polska-wzmacnia-ochrone-przed-cyberatakami>>.
- Olejniak Ł., *Propaganda. Od dezinformacji i wpływu do operacji i wojny informacyjnej*, Wydawnictwo Naukowe PWN, Warszawa 2024.
- On Security, ed. R. D. Lipschutz, Columbia University Press, New York 1995.
- Pałka P., *Strategie dyskursywne w rozmowie handlowej*, Wydawnictwo „Śląsk”, Katowice 2009.

- Pietras M., *Wojna informacyjna jako współczesne narzędzie działań nieregularnych*, „Cybersecurity and Law” 2021, nr 6 (2).
- Pietraś Z. J., *Decydowanie polityczne*, Wydawnictwo Naukowe PWN, Warszawa-Kraków 1998.
- Polko P., Urbanek A., *Sekurytyzacja*, „Encyklopedia Bezpieczeństwa Narodowego” [online], 10 II 2024 [dostęp: 19 III 2026]: <<https://encyklopedia.revite.pl/articles/view/502>>.
- Responsibility of States for Internationally Wrongful Acts*, United Nations, [New York] 2005: <https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf> [dostęp: 9 V 2026].
- Rid T., *Cyber War Will Not Take Place*, „Journal of Strategic Studies” 2012, vol. 35, issue 1: <<https://cs.armywarcollege.edu/SLET/mccd/CyberSpacePubs/Cyber%20War%20Will%20Not%20Take%20Place%20by%20Thomas%20Rid.pdf>> [dostęp: 17 III 2026].
- Siudak R., *Cyberbezpieczeństwo w Polsce. Od dyskursów do polityk publicznych*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2022.
- Stanowisko Rzeczypospolitej Polskiej dotyczące zastosowania prawa międzynarodowego w cyberprzestrzeni*, „Ministerstwo Spraw Zagranicznych” [online], 29 XII 2022 [dostęp: 29 V 2026]: <<https://www.gov.pl/web/dyplomacja/stanowisko-rzeczypospolitej-polskiej-dotyczace-zastosowania-prawa-miedzynarodowego-w-cyberprzestrzeni>>.
- „Strategiczny kompas” na rzecz bezpieczeństwa i obrony, „Rada Europejska. Rada Unii Europejskiej” [online], 28 VIII 2025 [dostęp: 9 V 2026]: <<https://www.consilium.europa.eu/pl/policies/strategic-compass/>>.
- Šenk M., Hynek N., *NATO/EU Synergies against Information Warfare: A „Circulatory Institutional” Model of Expert Voluntarism*, „European Security” 2026, vol. 35, No. 2: <<https://www.tandfonline.com/doi/epdf/10.1080/09662839.2025.2566519?needAccess=true>> [dostęp: 8 V 2026].
- The Tallinn Manual*, „The NATO Cooperative Cyber Defence Centre of Excellence” [online], 9 V 2026 [dostęp: 9 V 2026]: <<https://ccdcoe.org/research/tallinn-manual/>>.
- Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, ed. M. N. Schmitt, United States Naval War College, Newport, 3 II 2017: <<https://doi.org/10.1017/9781316822524>> [dostęp: 9 V 2026].
- Timeline – EU Sanctions against Russia*, „European Council. Council of the European Union” [online], 16 III 2026 [dostęp: 19 III 2026]: <<https://www.consilium.europa.eu/en/policies/sanctions-against-russia/timeline-sanctions-against-russia/>>.
- Tusk D., *[Chiny i Rosja rozpoczęły wojnę informacyjną z Zachodem]*, „X” [online], 13 III 2020 [dostęp: 18 III 2026]: <<https://x.com/donaldtusk/status/1238435525494747137>>.
- Use of Force*, „Cyber Law Toolkit” [online, dostęp: 9 V 2026]: <https://cyberlaw.ccdcoe.org/wiki/Use_of_force>.

- Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw*, Dz.U. 2026, poz. 252.
- Uzasadnienie*, [Sejm Rzeczypospolitej Polskiej, Warszawa], 29 IX 2025: <<https://orka.sejm.gov.pl/Druki10ka.nsf/o/BBC447BFD5BB3152C1258D1B004435D1/%24File/1757-uzasadnienie.docx>> [dostęp: 19 III 2026].
- Vériter S. L., *The Collective Securitization of „Disinformation” and the EU’s Ban on Russia Today and Sputnik*, „International Affairs” 2025, vol. 101, issue 5: <<https://doi.org/10.1093/ia/iaaf139>> [dostęp: 4 V 2026].
- Wæver O., *Securitization and Desecuritization*, [w:] *On Security*, ed. R. D. Lipschutz, Columbia University Press, New York 1995: <<https://www.libraryofsocial-science.com/assets/pdf/Waever-Securitization.pdf>> [dostęp: 19 III 2026].
- Walka informacyjna. Uwarunkowania – incydenty – wyzwania*, red. H. Batorowska, Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej, Kraków 2017.
- Walka z dezinformacją i ochrona przed nielegalnymi treściami w internecie*, „Kancelaria Prezesa Rady Ministrów” [online], 29 IX 2025 [dostęp: 19 III 2026]: <<https://www.gov.pl/web/premier/walka-z-dezinformacja-i-ochrona-przed-nielegalnymi-tresciami-w-internecie>>.
- Warsaw Summit Communiqué*, „North Atlantic Treaty Organization” [online], 9 VII 2016 [dostęp: 18 III 2026]: <<https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/09/warsaw-summit-communique>>.
- Wasiuta O., Wasiuta S., *Wojna informacyjna zagrożeniem dla bezpieczeństwa ludzkości*, [w:] *Walka informacyjna. Uwarunkowania – incydenty – wyzwania*, red. H. Batorowska, Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej, Kraków 2017.
- Williams M. C., *Securitization on the Liberalism of Fear*, „Security Dialogue” 2011, vol. 42, No. 4–5.
- Wniosek Prezydenta RP o ponowne rozpatrzenie ustawy z dnia 18 grudnia 2025 r. o zmianie ustawy o świadczeniu usług drogą elektroniczną oraz niektórych innych ustaw*, „Sejm Rzeczypospolitej Polskiej” [online], 9 I 2026 [dostęp: 19 III 2026]: <<https://www.sejm.gov.pl/Sejm10.nsf/druk.xsp?nr=2171>>.
- Wystąpienie podczas Debaty Generalnej 78. sesji Zgromadzenia Ogólnego ONZ*, „Oficjalna Strona Prezydenta Rzeczypospolitej Polskiej” [online], 19 IX 2023 [dostęp: 18 III 2026]: <<https://www.prezydent.pl/kancelaria/archiwum/andrzej-duda/aktualnosci/wypowiedzi-prezydenta-rp/wystapienia/podczas-debaty-generalnej-78-sesji-zgromadzenia-ogolnego-onz.74976>>.
- Żebrowski A., *Obszary zainteresowania służb specjalnych w trzeciej dekadzie XXI wieku. Wybrane aspekty*, „Central European Journal of Security Studies” 2024, vol. 2, issue 1.