ARTYKUŁY

„Polityka i Społeczeństwo" 1(24) / 2026
ISSN 1732-9639; eISSN 3072-5917
DOI: 10.15584/polispol.2026.1.2

Robert Białoskórski*

CYBERKULTURA JAKO ŚRODOWISKO OPERACYJNE INTERFEJSU STRUKTURALNO-TECHNOLOGICZNEGO POTĘGI INFORMACYJNEJ PAŃSTWA

Streszczenie

Artykuł analizuje rolę cyberkultury w strukturze potęgi informacyjnej państwa w ramach systemowego modelu potęgi informacyjnej (SMPI). Punktem wyjścia jest pytanie, w jaki sposób cyberkultura, jako środowisko operacyjne interfejsu strukturalno-technologicznego (IST) łączącego moduł strukturalny (SPI) i technologiczny (TPI) modelu SMPI, kształtuje praktyki komunikacyjne, tożsamości oraz sposoby zarządzania bezpieczeństwem informacyjnym. Autor dowodzi, że cyberkultura nie jest wtórnym kontekstem oddziaływania ani autonomiczną domeną potęgi informacyjnej, lecz ustrukturyzowanym środowiskiem operacyjnym, w którym platformy i algorytmy współdziałają z normami oraz instytucjami systemu państwowego. W ujęciu systemowym cyberkultura stanowi przestrzeń przekształcania zasobów technologicznych w trwałe konfiguracje normatywne i interpretacyjne. Mechanizmy selekcji algorytmicznej, hierarchie obecności treści w obiegu informacji oraz praktyki moderacyjne wpływają na relację między potencjałem informacyjnym a zdolnością defensywną państwa. Bezpieczeństwo informacyjne zależy zatem nie tylko od ochrony infrastruktury, lecz także od jakości sprzężenia między SPI i TPI oraz od zdolności systemu do podtrzymywania spójności interpretacyjnej w warunkach zarządzania obiegiem informacji za pośrednictwem platform cyfrowych.

Słowa kluczowe: potęga informacyjna państwa, systemowy model potęgi informacyjnej (SMPI), interfejs strukturalno-technologiczny (IST), cyberkultura, platformizacja, algorytmiczne zarządzanie widzialnością, bezpieczeństwo informacyjne

Wstęp

Cyberkultura stanowi współcześnie coraz ważniejsze środowisko życia społecznego, w którym realizują się uczestnictwo kulturowe, cyrkulacja znaczeń oraz zmagania o legitymizację, wiarygodność i widzial-

* Uniwersytet w Siedlcach, e-mail: robert.bialoskorski@uws.edu.pl, ORCID: 0000-0003-3038-7560.

ność podmiotów infosfery i wytwarzanych przez nie przekazów informacyjnych[1]. Jest zarazem przestrzenią, w której koncentrują się procesy komunikacyjne, kulturowe i symboliczne społeczeństwa informacyjnego. Platformy cyfrowe, infrastruktury algorytmiczne oraz usieciowione formy interakcji kształtują komunikację, a także tożsamości, emocje i orientacje zbiorowe[2]. W proponowanym ujęciu cyberkultura stanowi środowisko operacyjne interfejsu strukturalno-technologicznego (IST) potęgi informacyjnej (PI), w którym kształtują się zdolności państwa do oddziaływania informacyjnego poprzez organizację uwagi, regulację norm oraz zarządzanie uczestnictwem podmiotów w środowiskach platformowych[3].

Dotychczasowe debaty w studiach nad bezpieczeństwem coraz wyraźniej uwzględniają rolę informacji, narracji i procesów poznawczych w kształtowaniu procesów bezpieczeństwa[3]. Podkreślają one, że procesy informacyjne oddziałują na podejmowanie decyzji, zarządzanie percepcją oraz interakcje strategiczne. Jednak sama kultura bywa często traktowana jako warstwa wtórna – wzmacniacz lub kontekst, w którym ujawniają się mechanizmy oddziaływania informacyjnego państwa – a nie jako konstytutywna przestrzeń generowania i stabilizacji potęgi informacyjnej. W rezultacie cyberkultura jest najczęściej postrzegana jako środowisko wspierające operacje wpływu lub komunikację strategiczną, a nie jako ustrukturyzowana przestrzeń, w której kształtowane i utrwalane są mechanizmy oddziaływania informacyjnego, stanowiące element IST w ramach systemowego modelu potęgi informacyjnej (SMPI).

Z perspektywy studiów nad bezpieczeństwem procesy komunikacyjne i kulturowe zachodzące w cyberkulturze nie są wyłącznie zjawiskami społeczno-kulturowymi, lecz coraz wyraźniej współtworzą strukturę współczesnego bezpieczeństwa. Praktyki relewantne dla bezpieczeństwa – takie jak percepcja zagrożeń, mobilizacja zbiorowa, przypisywanie legitymacji oraz formowanie zaufania – są współcześnie głęboko osadzone w platformowo mediowanych środowiskach kulturowych. Cyberkultura strukturyzuje sposób wytwarzania i kontestowania znaczeń politycznych, uznawania lub podważania autorytetu oraz stabilizowania bądź fragmentaryzacji tożsamości zbiorowych. W rezultacie współ-

[1] M. Castells, *Communication Power*, Oxford 2007; J. Van Dijck, *The Culture of Connectivity. A Critical History of Social Media*, Oxford 2013.

[2] D. Boyd, *It's Complicated. The Social Lives of Networked Teens*, New Haven 2014; S. Turkle, *Alone Together. Why We Expect More from Technology and Less from Each Other*, New York 2011.

[3] A.W. Filipek, *Kultura bezpieczeństwa informacyjnego* [w:] *Leksykon bezpieczeństwa informacyjnego*, red. W. Fehler, Siedlce 2023; H. Wyrębek, *Cyberprzestrzeń. Zagrożenia, strategie cyberbezpieczeństwa*, Siedlce 2021.

kształtuje warunki artykulacji, negocjowania i zarządzania bezpieczeństwem, wykraczając poza klasyczne, państwocentryczne lub militarne ramy badawcze.

Założenia badawcze i koncepcyjne

W niniejszym artykule przez cyberkulturę rozumie się zespół praktyk komunikacyjnych, norm oraz form uczestnictwa podmiotów infosfery w środowiskach platformowych kształtowanych przez platformy i algorytmy. Celem artykułu jest odpowiedź na pytanie, w jaki sposób cyberkultura – traktowana jako środowisko operacyjne IST w SMPI państwa – kształtuje praktyki, tożsamości oraz tryby zarządzania bezpieczeństwem informacyjnym. W artykule przyjęto tezę, że cyberkultura stanowi ustrukturyzowane środowisko operacyjne IST, w którym platformy (PL) oraz algorytmy – jako elementy modułu technologicznego (TPI) – współkształtują praktyki, tożsamości i normy w interakcji z komponentami modułu strukturalnego (SPI). Podejście to odróżnia sposób ujmowania cyberkultury w SMPI od innych koncepcji potęgi obecnych w literaturze, takich jak *cyber power* w sensie techniczno-operacyjnym[4] czy *soft power* opartej na atrakcyjności normatywnej[5].

Cyberkultura jest środowiskiem, w którym realizuje się uczestnictwo kulturowe, cyrkulacja znaczeń oraz rywalizacja o legitymizację i widzialność w przestrzeni komunikacyjnej[6]. Platformy cyfrowe, infrastruktury algorytmiczne oraz usieciowione formy interakcji kształtują nie tylko komunikację, lecz także orientacje zbiorowe, emocje i tożsamości[7].

Z perspektywy studiów nad bezpieczeństwem procesy te wpływają na sposób postrzegania zagrożeń informacyjnych, mobilizację zbiorową, uznawanie określonych aktorów za wiarygodne źródła interpretacji wydarzeń oraz na poziom zaufania użytkowników w środowisku komunikacji cyfrowej. W konsekwencji cyberkultura współkształtuje warunki, w których bezpieczeństwo informacyjne jest postrzegane, interpretowane i zarządzane[8].

---

[4] J.S. Nye, *Cyber Power*, Cambridge (MA) 2010; T. Rid, *Cyber War Will Not Take Place*, Oxford 2013.

[5] J.S. Nye, *Soft Power: The Means to Success in World Politics*, New York 2004; *idem*, *The Future of Power*, New York 2011.

[6] M. Castells, *Communication Power…*, s. 245; J. Van Dijck, *op.cit.*, s. 37.

[7] D. Boyd, *op.cit.*; S. Turkle, *Alone Together...*

[8] N. Couldry, U.A. Mejias, *The Costs of Connection. How Data Is Colonizing Human Life and Appropriating It for Capitalism*, Stanford 2019.

W niniejszym artykule cyberkultura jest ujmowana jako element IST w SMPI państwa. W tym środowisku mechanizmy oddziaływania informacyjnego kształtują się poprzez organizację uwagi, selekcję widzialności oraz regulację uczestnictwa podmiotów w infosferze.

Przegląd literatury i luka badawcza

Cyberkultura od ponad trzech dekad stanowi przedmiot badań w obrębie studiów nad mediami, socjologii kultury, antropologii oraz krytycznej teorii informacji. W literaturze podkreśla się, że pojęcie cyberkultury ma charakter wieloznaczny i bywa używane w odniesieniu do różnych zjawisk związanych z rozwojem technologii informacyjno-komunikacyjnych oraz ich kulturowymi konsekwencjami. Termin ten może odnosić się do subkultur technologicznych, środowisk hakerskich, ruchu cyberpunkowego i do praktyk komunikacyjnych użytkowników sieci, nowych form wspólnotowości oraz badań nad mediami cyfrowymi. W rezultacie cyberkultura funkcjonuje w literaturze jako pojęcie obejmujące szeroki zakres zjawisk kulturowych związanych z rozwojem technologii cyfrowych[9].

Wczesne ujęcia cyberkultury przedstawiały ją jako nową formę kulturową powstającą w wyniku komunikacji sieciowej, inteligencji zbiorowej oraz interakcji społecznych w środowisku cyfrowym. Prace fundamentalne akcentowały transformacyjny potencjał technologii sieciowych wobec tożsamości, wspólnoty oraz praktyk komunikacyjnych, podkreślając decentralizację, uczestnictwo i nowe formy produkcji symbolicznej[10]. W tej perspektywie cyberkultura była rozumiana jako nowy horyzont kulturowy kształtowany przez komunikację, eksperymentowanie, a także zacieranie granic między producentami a odbiorcami.

Kolejne badania odeszły od początkowych interpretacji cyberkultury i zaczęły koncentrować się na codziennych praktykach oraz sposobach kształtowania tożsamości w środowiskach cyfrowych. Badania nad komunikacją w sieci pokazują, że interakcje na platformach cyfrowych zmieniają sposób funkcjonowania intymności, wspólnot i norm społecznych[11]. Jak wynika z badań nad komunikacją w sieci, interakcje na platformach cyfrowych sprzyjają powstawaniu nowych nawyków i form

---

[9] J. Macek, *Defining Cyberculture* [w:] *Média a realita*, red. P. Binková, J. Volek, Brno 2004, s. 35–65.

[10] P. Lévy, *Cyberculture*, Minneapolis 2001.

[11] S. Turkle, *Life on the Screen. Identity in the Age of the Internet*, New York 1995; D. Boyd, *op.cit*.

wspólnotowości[12]. Ten nurt badań ugruntował cyberkulturę jako trwałe środowisko funkcjonowania ludzi i instytucji, a nie krótkotrwałe zjawisko technologiczne.

Równolegle rozwinął się nurt krytyczny, który koncentruje się na aspektach władzy, nierówności i ideologii w kulturze cyfrowej. Krytyczna teoria informacji oraz studia kulturowe pokazały, że kultura cyfrowa nie jest wyłącznie neutralna i nie jest również źródłem pozytywnych zmian społecznych. Badacze wskazują, że cyberkultura jest ściśle związana z polityką, gospodarką cyfrową oraz sposobami kontroli informacji i komunikacji w środowiskach platformowych. W tej perspektywie cyberkultura nie jest jedynie przestrzenią kreatywności i partycypacji, lecz także obszarem wykluczenia, nadzoru, ekonomizacji aktywności oraz kształtowania zasad uczestnictwa w środowiskach platformowych. Praktyki kulturowe online są kształtowane przez ograniczenia infrastrukturalne, struktury własności oraz systemy wartości wpisane w działanie platform, które sprzyjają określonym podmiotom i ich formom ekspresji, a inne czynią mniej widocznymi w komunikacji cyfrowej[13].

Ważnym nurtem badań były studia nad genealogią cyberkultury oraz wskazanie jej związków z wcześniejszymi narracjami kontrkulturowymi. Analizy historyczne wykazały, że ideały otwartości, decentralizacji i wspólnotowości zostały włączone w instytucje i infrastrukturę sieci cyfrowych[14]. Narracje te stały się później ważnym źródłem kulturowej legitymizacji korporacyjnych modeli platformowych, które odwoływały się do retoryki partycypacji, a jednocześnie opierały się na gromadzeniu danych użytkowników i wykorzystywaniu ich aktywności jako źródła wartości ekonomicznej. Pomaga to zrozumieć, dlaczego dominująca pozycja platform cyfrowych bywa postrzegana jako naturalna lub nawet wyzwalająca, mimo że w praktyce wiąże się z koncentracją kontroli i ograniczoną odpowiedzialnością tych podmiotów. Badania te wskazują, że wykorzystanie potęgi informacyjnej nie zależy jedynie od zasobów materialnych, lecz również od zdolności kształtowania sposobów postrzegania zagrożeń, interpretowania wydarzeń i nadawania im znaczeń oraz wykorzystywania ich w praktyce[15].

Jednak w znacznej części studiów nad bezpieczeństwem kultura bywa traktowana jedynie jako narzędzie oddziaływania informacyjnego

[12] C. Marcinkowski, *Cyberculture of Everyday Life in the Second Decade of the 21st Century*, „Journal of Modern Science" 2020, vol. 43, nr 4.

[13] R.E. Day, *The Modern Invention of Information. Discourse, History, and Power,* Carbondale 2001.

[14] F. Turner, *From Counterculture to Cyberculture. Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism,* Chicago 2006.

[15] A.W. Filipek, *op.cit.*; H. Wyrębek, *op.cit*.

– jako medium, wzmacniacz lub cel takich działań, a nie jako przestrzeń, w której kształtują się warunki oddziaływania informacyjnego państwa. Procesy kulturowe analizowane są jako kanały dystrybucji narracji strategicznych, perswazji odbiorców lub mobilizacji grup społecznych. Rzadziej traktuje się je jako zorganizowane środowiska, które wpływają na to, jak informacje są postrzegane, interpretowane i weryfikowane. W efekcie cyberkultura funkcjonuje w analizach jako kontekst, a nie główny przedmiot badań.

Nowsze badania nad zarządzaniem platformami oraz rolą algorytmów w komunikacji cyfrowej zaczęły częściowo wypełniać tę lukę badawczą. Studia nad platformami oraz krytyczne analizy mediów pokazują, że platformy cyfrowe strukturyzują widzialność treści, uczestnictwo użytkowników oraz obowiązujące normy komunikacji poprzez sposób projektowania interfejsów, praktyki moderacyjne oraz systemy rekomendacyjne[16]. Platformy funkcjonują jako podmioty pełniące funkcje zbliżone do instytucji, które zarządzają komunikacją za pomocą prywatnych, transnarodowych i często nieprzejrzystych mechanizmów. Systemy algorytmiczne nie tylko dystrybuują informacje, lecz także aktywnie kształtują emocje użytkowników, oczekiwania kulturowe oraz wzorce uznania.

Jednak nawet w tym nurcie badań implikacje dla bezpieczeństwa są często analizowane pośrednio. Zarządzanie platformowe rozpatrywane jest głównie w kontekście demokracji, etyki medialnej lub potęgi ekonomicznej, natomiast jego znaczenie dla bezpieczeństwa pozostaje niedostatecznie ugruntowane teoretycznie. Fragmentacja publiczności, wzmacnianie emocji w komunikacji online oraz coraz większe różnice w sposobach interpretowania informacji i wydarzeń ujmowane są jako problemy społeczne lub polityczne.

W rezultacie utrzymuje się luka badawcza na pograniczu badań nad cyberkulturą i studiów nad bezpieczeństwem. Cyberkultura rzadko jest traktowana jako przestrzeń mająca istotne znaczenie dla bezpieczeństwa państwa. Z kolei analizy bezpieczeństwa, skoncentrowane na informacji i oddziaływaniu na odbiorców komunikacji, często pomijają środowiska kulturowe, w których praktyki informacyjne stają się stałym elementem komunikacji oraz są przyswajane i utrwalane przez podmioty infosfery.

Artykuł odnosi się do tej luki badawczej i umieszcza cyberkulturę w strukturze SMPI jako składową IST. Zamiast traktować ją jako sektor, medium lub studium przypadku, ujmuje ją jako relacyjne środowisko, w którym realizuje się oddziaływanie potęgi informacyjnej poprzez zarzą-

[16] J. Van Dijck, *op.cit.*; J. Van Dijck, T. Poell, M. de Waal, *The Platform Society. Public Values in a Connective World,* Oxford 2018.

dzanie platformami (PL w obrębie TPI), działanie algorytmów rekomendacyjnych i moderacyjnych (komponenty TPI) oraz praktyki uczestnictwa kulturowego (komponenty SPI).

Prezentowane w artykule podejście opiera się na wynikach badań nad cyberkulturą, studiach nad platformami oraz relacyjnymi ujęciami bezpieczeństwa informacyjnego – w tym SMPI – i ujmuje cyberkulturę jako środowisko, w którym potęga informacyjna państwa oraz jego zdolności w zakresie bezpieczeństwa informacyjnego pozostają w dynamicznej relacji w strukturze IST. W ten sposób artykuł wnosi wkład do studiów nad bezpieczeństwem, rozszerzając analizę potęgi informacyjnej państwa poza infrastrukturę, dane i komunikację strategiczną. Analiza obejmuje także kulturowe warunki kształtujące percepcję zagrożeń, legitymizację działań oraz odporność informacyjną.

Potęga informacyjna jako zjawisko relacyjne i systemowe

Zidentyfikowana luka badawcza wskazuje na potrzebę ujęcia cyberkultury nie tylko jako kontekstu komunikacji cyfrowej, lecz jako elementu struktury potęgi informacyjnej państwa. W tym celu konieczne jest przyjęcie relacyjnego i systemowego rozumienia potęgi informacyjnej. Potęga informacyjna nie ogranicza się do kontroli nad danymi, sieciami ani zdolnościami technicznymi. Obejmuje również zdolność kształtowania znaczeń, normalizowania praktyk oraz strukturyzowania warunków, w których aktorzy postrzegają, interpretują i wykorzystują informacje[17]. W tym ujęciu przejawia się jako potęga produktywna (wytwarzanie norm i tożsamości), potęga strukturalna (organizacja widzialności i interakcji) oraz potęga dyskursywna (cyrkulacja i sankcjonowanie narracji). Procesy te obejmują zarówno wymiar normatywno-narracyjny, jak i infrastrukturalne warunki ich realizacji.

Cyberkultura nie jest w tym ujęciu synonimem komunikacji online ani mediów cyfrowych. Odnosi się do historycznie ukształtowanych formacji kulturowych powstających w związku z rozwojem sieciowego przetwarzania informacji. Obejmują one wizje technologii, normy uczestnictwa oraz wzorce tożsamości i wspólnoty wbudowane w infrastruktury społeczno-techniczne. Wczesne konceptualizacje cyberkultury ujmowały ją jako hybrydową konfigurację, w której technologia i kultura wzajemnie się przekształcają, a nie funkcjonują jako odrębne domeny. Dlatego cyberkultura nie może być redukowana do wtórnej „warstwy" nakładanej

[17] M. Castells, *The Rise of the Network Society…*; P. Lévy, *Collective Intelligence. Mankind's Emerging World in Cyberspace*, Cambridge (MA) 1999.

na systemy informacyjne. Stanowi raczej środowisko, poprzez które znaczenia są wytwarzane, dystrybuowane i sankcjonowane.

Istotne znaczenie ma także genealogia cyberkultury, która pokazuje, w jaki sposób ideały otwartości, wspólnotowości i decentralizacji zostały przekształcone w konkretne mechanizmy zarządzania i kontroli kształtujące architekturę uczestnictwa cyfrowego[18]. Proces ten wpływa na konfigurację SPI, a pośrednio również na sposób wykorzystania zasobów technologicznych w obrębie TPI. Jednocześnie pojęcie „cyberkultura" pozostaje przedmiotem sporów. Krytyczna teoria informacji wskazuje, że może ono maskować materialne relacje władzy oraz uwarunkowania gospodarki politycznej[19]. Uwzględnienie tej krytyki wzmacnia przyjętą ramę teoretyczną. Cyberkultura nie jest tu afirmatywnym opisem kreatywności cyfrowej, lecz konfiguracją norm, infrastruktur oraz form uczestnictwa, w ramach których organizowana jest potęga informacyjna.

Cyberkultura strukturyzuje normy uczestnictwa, reżimy widzialności oraz repertuary tożsamości, poprzez które znaczenia są wytwarzane i rozpoznawane. W ten sposób tworzy zestaw warunków brzegowych bezpieczeństwa informacyjnego państwa. Określa, co może zostać uznane za zagrożenie, co zostaje znormalizowane jako akceptowalne ryzyko, kto może być uznany za aktora legitymowanego oraz które formy działania stają się zrozumiałe, dopuszczalne lub odrzucane. W tym sensie współkształtuje systemowe warunki funkcjonowania potęgi informacyjnej państwa.

W konsekwencji cyberkultura może być analizowana jako środowisko operacyjne IST, w którym elementy modułów SPI i TPI splatają się w procesach kształtowania i wykorzystywania potęgi informacyjnej państwa.

Cyberkultura jako środowisko operacyjne systemowego modelu potęgi informacyjnej

Artykuł odwołuje się do SMPI, państwocentrycznego modelu porządkującego potęgę informacyjną jako wielowymiarową i emergentną właściwość systemu państwowego[20]. Właściwość ta wyraża się w zdolności do pozyskiwania, przetwarzania, ochrony oraz wykorzystywania informacji w celu realizacji interesów strategicznych.

---

[18] F. Turner, *op.cit*.

[19] R.E. Day, *op.cit*.

[20] Szerokie ujęcie metodologiczne wcześniejszej wersji modelu, określanego jako syntetyczny model potęgi informacyjnej (SMPI), przedstawiono w: R. Białoskórski, *Bezpieczeństwo informacyjne. Dyskurs naukowy i normatywny*, Wydawnictwo Uniwersytetu w Siedlcach, Siedlce 2026.

Model ten opiera się na założeniu, że potęga informacyjna państwa ma strukturę dwumodułową. Obejmuje ona moduł strukturalny (SPI) oraz moduł technologiczny (TPI), które pozostają względem siebie komplementarne, lecz analitycznie rozdzielne, ponieważ obejmują odmienne kategorie zasobów, instytucji oraz technologii kształtujących funkcjonowanie infosfery. Dwumodułowość pozwala uniknąć zarówno redukcjonizmu technologicznego, który sprowadza potęgę informacyjną do infrastruktury i innowacji technologicznych, jak i redukcjonizmu instytucjonalnego, który wyjaśnia ją wyłącznie poprzez instytucje, normy i organizację systemu informacyjnego państwa. Moduł SPI odnosi się do organizacji krajowej infosfery jako układu instytucji, norm, zasobów i praktyk regulujących przepływy informacyjne. Moduł TPI obejmuje natomiast zdolności państwa do wytwarzania, skalowania i wykorzystywania technologii cyfrowych umożliwiających przetwarzanie oraz rozpowszechnianie informacji w skali systemowej i międzynarodowej. Rozróżnienie to ma charakter analityczny, ponieważ w praktyce oba moduły pozostają w relacji stałego sprzężenia zwrotnego.

Relacja ta ujawnia się w IST, rozumianym jako mechanizm powiązania zasobów technologicznych z architekturą instytucjonalną i kulturową infosfery. Technologie cyfrowe ulegają instytucjonalizacji i stają się elementem praktyk społecznych, natomiast struktura infosfery uzyskuje nowe właściwości dzięki integracji zasobów technologicznych. Potęga informacyjna państwa ma zatem charakter właściwości systemowej, a jej poziom zależy od jakości sprzężenia między modułami SPI i TPI.

W tym ujęciu cyberkultura nie stanowi dodatkowego modułu modelu, lecz jest środowiskiem operacyjnym IST, czyli przestrzenią, w której zasoby technologiczne (np. platformy cyfrowe i systemy algorytmiczne) oraz struktury normatywne i kulturowe wchodzą w relację sprzężenia i wzajemnie się przekształcają.

Platformy cyfrowe stanowią szczególny przykład działania tego interfejsu. W module TPI funkcjonują jako narzędzia skalowania i globalnego rozpowszechniania informacji (PL), natomiast w module SPI organizują krajowe przepływy informacyjne oraz podlegają ramom regulacyjnym (PRI). Ich podwójne osadzenie sprawia, że stają się mechanizmem integrującym strukturę i technologię w jedną dynamiczną konfigurację.

Cyberkultura jako środowisko operacyjne IST wpływa zatem na jakość sprzężenia między modułami SPI i TPI. W sprzyjających konfiguracjach może wzmacniać spójność narracyjną, kompetencje informacyjne oraz zdolności analityczne państwa. W konfiguracjach niespójnych może natomiast prowadzić do fragmentacji przestrzeni informacyjnej, polaryzacji debat publicznych oraz erozji zaufania podmiotów infosfery do instytucji państwa.

Platformowo-algorytmiczny mechanizm operacyjny interfejsu strukturalno-technologicznego

Platformizacja stanowi główny mechanizm, poprzez który IST działa w środowisku cyberkulturowym. Platformy cyfrowe nie pełnią jedynie funkcji infrastrukturalnych, lecz kształtują sposób komunikacji i interakcji między użytkownikami, oddziałując na sposób prezentowania treści, systemy rekomendacyjne, moderację treści, metryki zaangażowania oraz mechanizmy mierzenia aktywności[21]. W ten sposób platformy tworzą pomiędzy modułami SPI i TPI architekturę sprzężenia zwrotnego, w której zasoby technologiczne ulegają instytucjonalizacji i stają się elementem praktyk kulturowych, natomiast struktury normatywne i instytucjonalne kształtują sposób projektowania i wykorzystania technologii.

W module TPI platformy funkcjonują jako komponent zdolności oddziaływania (PL), umożliwiający skalowanie widzialności, koncentrację danych oraz transnarodowe rozpowszechnianie informacji. W module SPI organizują krajowe przepływy informacyjne (IK), wpływają na kulturę informacyjną użytkowników (ICU) oraz podlegają – w różnym stopniu – regulacji instytucjonalnej (PRI). Ich podwójne osadzenie sprawia, że platformy stają się szczególnie istotnym miejscem działania IST, w którym technologia i struktura wzajemnie się przekształcają.

Jeżeli platformy stanowią architekturę sprzężenia między modułami SPI i TPI, algorytmy pełnią funkcję jego operacyjnego mechanizmu. Systemy selekcji, rankingowania i rekomendacji przekształcają aktywność kulturową użytkowników w hierarchie widzialności, istotności oraz legitymizacji treści[22]. W praktyce to one realizują bieżące działanie modułu TPI: wybierają, wzmacniają, przyspieszają lub marginalizują treści na masową skalę.

Algorytmiczna mediacja nie jest neutralnym filtrowaniem przepływu informacji[23]. Poprzez hierarchizowanie i wzmacnianie widzialności treści wywołujących intensywne reakcje emocjonalne – strach, oburzenie lub moralną mobilizację – systemy rekomendacyjne kształtują wzorce percepcji i uwagi użytkowników. Widzialność staje się w ten sposób zasobem dystrybuowanym zgodnie z logiką zaangażowania, a nie wyłącznie według kryteriów instytucjonalnej wiarygodności czy jakości debaty publicznej.

---

[21] J. Van Dijck, *op.cit.*

[22] T. Striphas, *Algorithmic Culture*, „European Journal of Cultural Studies", 2015, vol. 18, nr 4–5, s. 395–412.

[23] Oznacza to, że algorytmy platform cyfrowych nie działają jak bierny filtr, który jedynie porządkuje ogromną liczbę informacji. W rzeczywistości aktywnie kształtują to, co użytkownicy widzą, jak często to widzą i w jakiej kolejności.

Z perspektywy IST oznacza to, że sprzężenie między modułami TPI i SPI podlega ciągłym zmianom. Algorytmy przekształcają potencjał technologiczny w efekty widoczne w kulturze komunikacji: stabilizują określone ramy interpretacyjne, wzmacniają wybrane style komunikacyjne oraz zmieniają relacje między narracją, kompetencjami informacyjnymi i regulacją. Algorytmiczne mechanizmy selekcji informacji opierają się na rutynowej akceptacji technicznych zasad wyboru i porządkowania treści[24].

Rozwój generatywnej sztucznej inteligencji (GAI) wprowadza jakościową zmianę w funkcjonowaniu IST. Systemy generujące tekst, obraz i dźwięk zwiększają tempo oraz skalę wytwarzania treści, przyspieszając obieg symboli i narracji w środowisku cyfrowym. Produkcja kulturowa staje się w coraz większym stopniu zautomatyzowana i skalowalna, a granice między twórczością a reprodukcją ulegają zatarciu[25].

W ujęciu modelowym oznacza to przyspieszenie rozwoju TPI, które może wyprzedzać zdolność do adaptacji SPI. Instytucje regulacyjne, praktyki weryfikacji informacji oraz kompetencje kulturowe nie zawsze rozwijają się w tym samym tempie co narzędzia generatywne. Interfejs strukturalno-technologiczny ulega przyspieszeniu: relacja między technologią a strukturą staje się bardziej intensywna, mniej stabilna i bardziej podatna na gwałtowne zmiany dynamiki obiegu informacji.

Nie chodzi o eliminację prawdy, lecz o destabilizację społecznych mechanizmów jej weryfikacji oraz uzgadniania wspólnych interpretacji rzeczywistości. Zdolność wytwarzania bardzo dużej liczby przekonujących treści zwiększa znaczenie kontroli tempa oraz intensywności obiegu informacji. W takich warunkach potęga informacyjna przejawia się poprzez skalę, powtarzalność oraz zdolność szybkiego dostosowywania przekazów informacyjnych do reakcji odbiorców.

Platformowo-algorytmiczna konfiguracja IST sprzyja segmentacji środowisk informacyjnych. Personalizacja i filtrowanie treści prowadzą do powstawania częściowo odrębnych wspólnot interpretacyjnych w infosferze[26]. Wspólne ramy odniesienia mogą w takich warunkach ulegać osłabieniu, podczas gdy mobilizacja emocjonalna użytkowników staje się łatwiejsza do wywołania, lecz trudniejsza do długotrwałego utrzymania[27]. W ujęciu systemowym nie jest to wyłącznie rezultat operacji wpływu, lecz także strukturalny efekt sprzężenia między logiką zaangażowania,

[24] R.E. Day, *op.cit.*

[25] L. Manovich, *AI Aesthetics*, Moscow 2019.

[26] E. Pariser, *The Filter Bubble. What the Internet Is Hiding from You*, New York 2011.

[27] B.-C. Han, *The Transparency Society*, Stanford 2015.

architekturą platform a adaptacyjnymi praktykami użytkowników. Technologiczna zdolność wzmacniania i rozpowszechniania informacji może rosnąć szybciej niż zdolność instytucji i społeczeństwa do ich interpretowania oraz kontrolowania ich obiegu, co prowadzi do powstawania asymetrii w obrębie IST.

Fragmentacja infosfery nie oznacza jednak anarchii informacyjnej, a raczej zmianę mechanizmów jej oddziaływania: większą rolę zaczynają odgrywać mechanizmy selekcji informacji, dynamika obiegu przekazów oraz emocjonalny charakter komunikacji. W takim środowisku mechanizmy potęgi informacyjnej państwa działają w warunkach platformowo-algorytmicznego kształtowania obiegu informacji. Nie zmieniają one struktury modelu SMPI, lecz wpływają na sposób relacji jego modułów.

Mikroregulacja cyberkulturowa jako poziom strukturalny interfejsu strukturalno-technologicznego

Jeżeli platformowo-algorytmiczna architektura stanowi główny mechanizm działania IST, to praktyki cyberkulturowe odpowiadają za jego funkcjonowanie w codziennej komunikacji społecznej. Cyberkultura nie jest środowiskiem neutralnym pod względem norm i wartości ani przestrzenią nieuporządkowanej komunikacji, lecz środowiskiem kształtowanym przez reguły platform, mechanizmy algorytmiczne i praktyki użytkowników. Cyberkultura obejmuje rozproszone mechanizmy regulacyjne, które stabilizują oczekiwania, sankcjonują zachowania użytkowników oraz wpływają na obieg treści w infosferze[28].

Mechanizmy te nie mają charakteru formalno-prawnego, lecz opierają się na reputacji, rozpoznawalności, samoregulacji użytkowników oraz algorytmicznie wzmacnianych sygnałach oceny w środowisku platformowym. Polubienia, udostępnienia, liczba obserwujących, reakcje społeczności i decyzje moderacyjne tworzą system ocen, w którym określone zachowania są nagradzane większym zasięgiem, a inne stopniowo tracą znaczenie w obiegu komunikacji. W ten sposób komponenty strukturalne SPI – kultura informacyjna (ICU), potencjał narracyjny (NP) oraz wymiar regulacyjny (PRI) – funkcjonują także na poziomie mikrospołecznym.

W prezentowanym ujęciu widzialność jest efektem sprzężenia między technologiczną selekcją (TPI) a kulturową legitymizacją (SPI), określającym, które treści i podmioty uzyskują trwałą ekspozycję w środowisku

[28] L. Shifman, *Memes in Digital Culture*, Cambridge (MA) 2014.

platformowym[29]. Jako zasób cyberkultury widzialność podlega nierównomiernej dystrybucji i ciągłym zmianom w hierarchiach ekspozycji kształtowanych przez mechanizmy algorytmiczne. Praktyki uczestników dostosowują się do dominujących norm komunikacyjnych, stylów ekspresji oraz form wyrażania emocji, które sprzyjają utrzymaniu lub zwiększeniu obecności w obiegu komunikacji. Odchylenie od tych wzorców może prowadzić do symbolicznej marginalizacji, ograniczenia zasięgu treści lub negatywnych reakcji społeczności. Reakcje te pełnią funkcję sankcji społecznych. Mają one najczęściej charakter nieformalny i przyjmują formę zawstydzania, wykluczenia z dyskusji, masowego raportowania treści, osłabienia pozycji w hierarchii uznania czy algorytmicznego obniżenia zasięgu wywołanego zbiorowym zachowaniem użytkowników. Ich skuteczność wynika nie tyle z formalnej mocy egzekucyjnej, ile z ich przewidywalności. Oczekiwanie sankcji wpływa na zachowanie uczestników komunikacji, jeszcze zanim zostaną zastosowane. Władza działa poprzez antycypację, a nie wyłącznie poprzez bezpośrednią interwencję.

W kategoriach SMPI oznacza to, że mechanizmy reputacyjne, czyli społeczna ocena pozycji podmiotów w platformowym obiegu informacji, wpływają na jakość sprzężenia między SPI i TPI. Platformowa infrastruktura (TPI) dostarcza metryk aktywności i zasięgu, takich jak liczba polubień, udostępnień, komentarzy, obserwujących czy wyświetleń treści, które wpływają na zakres ich rozpowszechniania w środowisku platformowym. Reputacja podmiotów infosfery staje się ważnym zasobem potęgi informacyjnej poprzez wpływanie na sposób interpretowania informacji i wydarzeń oraz na uzyskiwanie społecznej legitymizacji.

Tożsamość w cyberkulturze kształtuje się w warunkach sprzężenia między technologiczną selekcją widzialności a kulturowymi mechanizmami uznania w infosferze[30]. Jednostki uczą się, które style wypowiedzi,

[29] W artykule pojęcie widzialności odnosi się do stopnia obecności i ekspozycji treści w środowisku komunikacji cyfrowej. Obejmuje ono zarówno techniczne mechanizmy selekcji i rankingowania informacji (np. algorytmy rekomendacyjne, kolejność wyświetlania treści, systemy trendów), jak i społeczne mechanizmy legitymizacji, takie jak reakcje użytkowników, reputacja nadawców czy uznanie określonych narracji za wiarygodne. Widzialność nie oznacza zatem jedynie fizycznej dostępności informacji w sieci, lecz ich realną obecność w obiegu komunikacji oraz zdolność przyciągania uwagi odbiorców.

[30] W artykule pojęcie tożsamości cyberkulturowej odnosi się do sposobów, w jakie jednostki i zbiorowości przedstawiają oraz definiują siebie w środowisku komunikacji cyfrowej. Obejmuje ono zarówno formy autoprezentacji w mediach społecznościowych (np. profile, narracje o sobie, styl komunikacji), jak i społeczne procesy uznania, w których inni uczestnicy komunikacji potwierdzają lub kwestionują określone role, poglądy i przynależności. Tożsamość cyberkulturowa ma charakter dynamiczny i relacyjny: kształtuje się w interakcji między praktykami użytkowników, normami cyberkultury oraz mechanizmami platform i algorytmów, które wpływają na zasięg i interpretację przekazów.

orientacje normatywne i sposoby prezentacji sprzyjają większej obecności ich przekazów w obiegu komunikacji oraz uzyskiwaniu społecznej legitymizacji, a które prowadzą do ich marginalizacji[31]. Tożsamość w cyberkulturze nie jest wyłącznie indywidualną formą wyrażania siebie, lecz kształtuje się w dostosowaniu do sposobu funkcjonowania platform oraz do norm i oczekiwań społeczności użytkowników. Dynamika ta ma charakter ambiwalentny, gdyż z jednej strony środowiska cyfrowe umożliwiają tworzenie nowych wspólnot i eksperymentowanie z różnymi formami identyfikacji, z drugiej zaś wzmacniają presję normatywną i zwiększają ryzyko negatywnych konsekwencji dla tych, którzy odchodzą od dominujących wzorców komunikacyjnych. Autorytet i wiarygodność podmiotów w infosferze coraz częściej zależą od zgodności z normami komunikacji platformowej oraz od uznania społeczności użytkowników.

W ujęciu systemowym oznacza to, że mikrospołeczne mechanizmy cyberkultury wpływają na sposób powiązania komponentów SPI – szczególnie kultury informacyjnej (ICU) i potencjału narracyjnego (NP) – z technologiczną architekturą TPI. Zdolność do oddziaływania informacyjnego zależy więc nie tylko od zasobów infrastrukturalnych, lecz także od dostosowania do norm i oczekiwań obowiązujących w środowisku komunikacji cyfrowej.

Platformowe mikrospołeczności – kanały tematyczne, serwery czy społeczności skupione wokół twórców – stanowią przestrzenie, w których modelowe konfiguracje IST przyjmują konkretną formę w praktyce komunikacyjnej. W tych środowiskach stabilizują się rytmy uczestnictwa, hierarchie obecności treści oraz wzorce sankcjonowania zachowań. Twórcy treści pełnią rolę węzłowych aktorów, łączących mechanizmy platform z normami wspólnotowymi poprzez moderację dyskusji, selekcję tematów i sposób prowadzenia narracji.

Ekonomizacja uczestnictwa, przejawiająca się w systemach subskrypcji, darowizn i nagród dla twórców, dodatkowo wzmacnia sprzężenie między kulturą a technologią. Uwaga i zaangażowanie użytkowników zyskują w ten sposób wymiar ekonomiczny, co stabilizuje określone style komunikacji oraz sposoby prowadzenia narracji. Mikrospołeczne mechanizmy regulacyjne funkcjonujące na platformach nie stanowią autonomicznej sfery wobec SMPI, lecz przestrzeń operacyjną, w której sprzężenie między SPI i TPI jest realizowane w rutynowych praktykach uczestnictwa, uznania i normowania komunikacji w infosferze.

Na tym poziomie potęga informacyjna nie działa poprzez formalne decyzje instytucjonalne, lecz poprzez kumulatywne efekty powtarzalnej obecności treści w obiegu komunikacji, stabilizowanych norm oraz

[31] S. Turkle, *Alone Together*...

przewidywalnych sankcji społecznych. Cyberkultura ujawnia się w ten sposób jako rozproszony, lecz uporządkowany mechanizm sprzężenia zwrotnego między SPI i TPI.

Konsekwencje dla studiów nad bezpieczeństwem

Ujęcie cyberkultury jako środowiska operacyjnego IST przesuwa analizę bezpieczeństwa informacyjnego z poziomu pojedynczych incydentów i narzędzi na poziom systemowych relacji między strukturą a technologią. Zagrożenia informacyjne nie wynikają wyłącznie z działań wrogich aktorów, lecz także z jakości sprzężenia między strukturą normatywną a infrastrukturą i mechanizmami technologicznymi, które wspólnie kształtują sposób rozpowszechniania informacji, ich interpretowania oraz uzyskiwania społecznego uznania przez określone przekazy i źródła.

W takim ujęciu bezpieczeństwo informacyjne nie sprowadza się jedynie do ochrony infrastruktury informacyjnej czy zwalczania dezinformacji, lecz obejmuje również kształtowanie środowiska komunikacyjnego, w którym formują się percepcje zagrożeń, uznawane są autorytety interpretujące wydarzenia oraz utrwalają się sposoby nadawania znaczeń, które pozwalają społeczeństwu wspólnie interpretować wydarzenia i reagować na nie w sposób skoordynowany.

Z perspektywy SMPI oznacza to, że zdolność państwa w zakresie bezpieczeństwa informacyjnego zależy nie tylko od poziomu regulacji czy potencjału technologicznego, lecz także od spójności relacji między modułami SPI i TPI oraz od sposobu ich funkcjonowania w cyfrowym środowisku społeczno-kulturowym. Cyberkultura nie jest zatem dodatkiem do potęgi informacyjnej państwa, lecz środowiskiem, w którym weryfikowana jest jej efektywność, trwałość i stabilność.

W tym sensie bezpieczeństwo informacyjne oznacza zdolność systemu do podtrzymywania pluralizmu oraz spójności interpretacji informacji i wydarzeń w warunkach algorytmicznie kształtowanego obiegu informacji oraz rozproszonego kształtowania norm komunikacyjnych. Analiza zjawiska cyberkultury pozwala zauważyć, że współczesne środowisko bezpieczeństwa informacyjnego jest w mniejszym stopniu kształtowane przez spektakularne decyzje polityczne, a w większym przez codzienne, rutynowe mechanizmy selekcji informacji, ich interpretowania oraz uzyskiwania społecznego uznania przez podmioty infosfery.

Zakończenie

Celem artykułu było udzielenie odpowiedzi na pytanie, w jaki sposób cyberkultura – traktowana jako środowisko IST w SMPI państwa – kształtuje praktyki, tożsamości oraz tryby zarządzania bezpieczeństwem informacyjnym.

Przeprowadzone badania prowadzą do wniosku, że cyberkultura nie jest wtórnym kontekstem oddziaływania informacyjnego podmiotów ani neutralnym środowiskiem transmisji treści, lecz ustrukturyzowaną przestrzenią operacyjną, w której dochodzi do trwałego sprzężenia zwrotnego między modułami SPI i TPI w architekturze SMPI.

Po pierwsze, wykazano, że praktyki komunikacyjne w środowisku platformowym podlegają jednoczesnej regulacji technologicznej i kulturowej. Algorytmiczna selekcja, hierarchie widzialności oraz mechanizmy moderacyjne (TPI) współdziałają z normami uznania, legitymizacji i sankcjonowania (SPI), tworząc warunki, w których określone style komunikacji, ramy interpretacyjne i wzorce uczestnictwa zyskują trwałość. W rezultacie praktyki bezpieczeństwa informacyjnego nie są wyłącznie efektem decyzji instytucjonalnych, lecz wyłaniają się w codziennych mechanizmach widzialności i uznania społecznego.

Po drugie, cyberkultura kształtuje tożsamości w sposób relacyjny i regulowany. Jednostki oraz podmioty zbiorowe funkcjonują w warunkach sprzężenia między technologicznymi mechanizmami rozpowszechniania treści a kulturową oceną przekazów, ucząc się, które formy ekspresji zwiększają zasięg i społeczną legitymizację, a które prowadzą do ich marginalizacji. Tożsamość w cyberkulturze nie ma charakteru wyłącznie ekspresyjnego, lecz stanowi efekt dostosowania do sposobu funkcjonowania platform oraz do norm i oczekiwań wspólnoty użytkowników. Mechanizm ten ma bezpośrednie znaczenie dla bezpieczeństwa informacyjnego, ponieważ wpływa na wiarygodność podmiotów w debacie publicznej oraz na pozycję interpretacyjną tworzonych przez nie narracji.

Po trzecie, cyberkultura modyfikuje sposoby zarządzania bezpieczeństwem informacyjnym poprzez rozproszenie funkcji regulacyjnych. Platformy (PL) oraz systemy algorytmiczne jako elementy TPI nie tylko pośredniczą w komunikacji, lecz współuczestniczą w określaniu warunków uczestnictwa, rozpowszechniania treści oraz sankcjonowania zachowań. Jednocześnie komponenty SPI – takie jak potencjał regulacyjno-instytucjonalny (PRI) czy kultura i kompetencje informacyjne – wpływają na sposób, w jaki te zasoby technologiczne są włączane w praktyki społeczne i ramy instytucjonalne. Zarządzanie bezpieczeństwem informacyjnym

staje się zatem procesem hybrydowym, rozproszonym między państwem, podmiotami prywatnymi oraz wspólnotami użytkowników infosfery.

Zgodnie z przyjętą tezą cyberkultura stanowi środowisko operacyjne IST, w którym potęga informacyjna państwa nie jest jedynie wykorzystywana, lecz podlega nieustannej rekonfiguracji. Odróżnia to proponowaną konceptualizację zarówno od ujęć *cyber power* skoncentrowanych na zdolnościach techniczno-operacyjnych, jak i od koncepcji *soft power* opartych na atrakcyjności normatywnej. W przeciwieństwie do tych podejść cyberkultura nie jest traktowana jako instrument projekcji wpływu, lecz jako przestrzeń systemowego przekształcania zasobów technologicznych w trwałe konfiguracje normatywne i praktyki interpretacyjne.

Z perspektywy studiów nad bezpieczeństwem informacyjnym wyniki badań wskazują, iż nie zależy ono wyłącznie od ochrony infrastruktury ani od neutralizacji wrogich narracji, lecz także od jakości sprzężenia między SPI i TPI oraz od zdolności systemu do podtrzymywania pluralizmu, spójności interpretacji i autonomii decyzyjnej w warunkach algorytmicznie kształtowanego obiegu informacji.

Konkludując, cyberkultura jako przestrzeń operacyjna IST w SMPI kształtuje bezpieczeństwo informacyjne państwa poprzez bieżące mechanizmy selekcji informacji, uznania społecznego oraz utrwalania sposobów interpretacji wydarzeń. To właśnie na tym poziomie kształtuje się realna efektywność potęgi informacyjnej państwa w złożonym i rozproszonym środowisku informacyjnym.

Bibliografia

Batorski D., *Internet a kultura. Rola nowych mediów w kształtowaniu relacji społecznych*, Warszawa 2007.

Boyd D., *It's Complicated. The Social Lives of Networked Teens*, New Haven 2014.

Castells M., *Communication Power*, Oxford 2007.

Castells M., *The Rise of the Network Society*, Oxford 2000.

Couldry N., Mejias U.A., *The Costs of Connection. How Data Is Colonizing Human Life and Appropriating It for Capitalism*, Stanford 2019.

Day R.E., *The Modern Invention of Information. Discourse, History, and Power*, Carbondale 2001.

Filipek A.W., *Kultura bezpieczeństwa informacyjnego* [w:] *Leksykon bezpieczeństwa informacyjnego*, red. W. Fehler, Siedlce 2023, s. 211–212.

Han B.-C., *The Transparency Society*, Stanford 2015.

Jemielniak D., Socjologia internetu, Warszawa 2019.

Lévy P., *Collective Intelligence. Mankind's Emerging World in Cyberspace*, Cambridge (MA) 1999.

Lévy P., *Cyberculture*, Minneapolis 2001.

Manovich L., *AI Aesthetics*, Moscow 2019.

Marcinkowski C., *Cyberculture of Everyday Life in the Second Decade of the 21st Century*, „Journal of Modern Science" 2020, vol. 43, nr 4, s. 167–180.
Nye J.S., *Soft Power. The Means to Success in World Politics*, New York 2004.
Nye J.S., *Cyber Power*, Cambridge (MA) 2010.
Nye J.S., *The Future of Power*, New York 2011.
Pariser E., *The Filter Bubble. What the Internet Is Hiding from You*, New York 2011.
Rettberg J.W., *Machine Vision. How Algorithms Are Changing the Way We See the World*, Cambridge 2023.
Rid T., *Cyber War Will Not Take Place*, Oxford 2013.
Shifman L., *Memes in Digital Culture*, Cambridge (MA) 2014.
Striphas T., *Algorithmic Culture*, „European Journal of Cultural Studies" 2015, vol. 18, nr 4–5.
Turner F., *From Counterculture to Cyberculture. Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*, Chicago 2006.
Turkle S., *Life on the Screen. Identity in the Age of the Internet*, New York 1995.
Turkle S., *Alone Together. Why We Expect More from Technology and Less from Each Other*, New York 2011.
Van Dijck J., *The Culture of Connectivity. A Critical History of Social Media*, Oxford 2013.
Van Dijck J., Poell T., de Waal M., *The Platform Society. Public Values in a Connective World*, Oxford 2018.
Wyrębek H., *Cyberprzestrzeń. Zagrożenia, strategie cyberbezpieczeństwa*, Siedlce 2021.

Cyberculture as the Operational Environment of the Structural–Technological Interface of State Informational Power

Abstract

The article analyses the role of cyberculture in the structure of the state's informational power within the Systemic Model of Informational Power (SMIP). The study addresses the question of how cyberculture, understood as the operational environment of the structural-technological interface (IST) linking the structural module (SIP) and the technological module (TIP) of the SMIP, shapes communication practices, identities, and modes of managing informational security. The author argues that cyberculture should not be understood as a secondary context of informational influence or as an autonomous domain of informational power, but rather as a structured operational environment in which platforms and algorithms interact with the norms and institutions of the state system. From a systemic perspective, cyberculture constitutes a space in which technological resources are transformed into durable normative and interpretative configurations. Mechanisms of algorithmic selection, hierarchies of content visibility, and moderation practices influence the relationship between the informational potential of the state and its defensive capacity. Consequently, informational security depends not only on the protection of infrastructure but also on the quality of the coupling between SIP and TIP and on the system's capacity to maintain interpretative coherence under conditions of platform-mediated governance of the information environment.

Keywords: state informational power; Systemic Model of Informational Power (SMIP); Structural-Technological Interface (STI); cyberculture; platformisation; algorithmic governance of visibility; informational security