

# Cyberprzestrzeń między (a)terytorialnością a (bez)granicznością?

**Robert Białoskórski**

Instytut Nauk o Bezpieczeństwie

Uniwersytet w Siedlcach

ORCID: 0000-0003-3038-7560

## **Streszczenie:**

Artykuł podejmuje analizę pojęć aterytorialności i bezgraniczności cyberprzestrzeni poprzez odniesienie ich do kategorii terytorium i granicy. Wskazano, że sposób rozumienia tych pojęć – jako struktur fizycznych bądź нефizycznych – zasadniczo determinuje ocenę własności cyberprzestrzeni. Autor dowodzi, że cyberprzestrzeń posiada strukturę dualistyczną, łączącą komponenty materialne i niematerialne, co podważa uproszczone tezy o jej jednoznacznej aterytorialności i bezgraniczności. W konsekwencji postulowane jest bardziej precyzyjne i kontekstowe stosowanie tych kategorii w analizach naukowych.

**Słowa kluczowe:** cyberprzestrzeń; terytorium; granica; aterytorialność; bezgraniczność

## **1. Wprowadzenie**

W tekstach publicystycznych, a także w literaturze naukowej wśród wymienianych cech cyberprzestrzeni często przytaczane są takie określenia jak: „aterytoriałność” i „bezgraniczność”. O ile w pierwszym przypadku pojęcie to bywa przyjmowane bez głębszej refleksji, o tyle w drugim wymaga badawczej refleksji. Obie te cechy najczęściej odnoszą się do pojęć „terytorium” oraz „granicy”, zatem sposób ich definiowania determinuje rozpatrywane cechy cyberprzestrzeni. Pozwoli to wówczas odpowiedzieć na pytanie, czy cyberprzestrzeń rzeczywiście ma cechy aterytorialności i bezgraniczności? Przyjęta robocza teza zakłada, że odpowiedź może nie być wcale oczywista i jednoznaczna, a problem nie jest tak banalny, jak mogłoby się pozornie wydawać na podstawie lektury literatury przedmiotu.

## **2. Terytorium i granica jako fizyczne (materialne) struktury przestrzenne**

W tradycyjnym ujęciu słownikowym termin *terytorium* oznacza powierzchnię, czyli „obszar o określonych granicach, podległy jakiemuś państwu, władcy, urzędnikowi, jednostce organizacyjnej lub osobie prywatnej”<sup>1</sup>. Natomiast *granica* posiada więcej zakresów znaczeniowych, ale w sensie fizycznym to *granica państwa*, czyli „coś, co oddziela jeden obszar od innego (lub wszystkich pozostałych) i zwykle jest przedstawiane jako wyobrażona linia przebiegająca w terenie i oznaczana na mapach”<sup>2</sup>. W słownikowych i encyklopedycznych ujęciach najczęściej podkreśla się wirtualny, niematerialny i interaktywny charakter

cyberprzestrzeni<sup>3</sup>, a więc pozbawiony fizycznego terytorium i fizycznej granicy. Zatem w tym sensie cyberprzestrzeń posiada obie cechy – aterytorialności i bezgraniczności.

### **3. Terytorium i granica jako niefizyczne (niematerialne) struktury przestrzenne**

Współcześnie pojęcia „terytorium” i „granica” przyjmują także szersze, niefizyczne (niematerialne) znaczenia przestrzenne, wykraczające poza klasyczne odniesienia geograficzne. Termin „granica” może być odnoszony nie tylko do „linii rozdzielającej państwa”, lecz również do innych kontekstów, obejmujących „zjawiska zachodzące w przestrzeni kulturowej lub społecznej”<sup>4</sup>. Oznacza to, że granice funkcjonują także jako konstrukty polityczne, prawne i symboliczne, wyznaczające zakres obowiązywania władzy, jurysdykcji oraz norm. Podobnie pojęcie terytorium traci wyłącznie materialny charakter i nie jest jedynie fragmentem przestrzeni geograficznej, lecz „społecznie i politycznie konstruowanym obszarem”, którego znaczenie wynika z relacji władzy i praktyk społecznych<sup>5</sup>. W takim ujęciu granice nie muszą mieć charakteru fizycznego, lecz mogą być konstruowane normatywnie, symbolicznie lub funkcjonalnie, a ich przebieg pozostaje płynny i zależny od kontekstu społecznego. Terytorium staje się natomiast kategorią analityczną, służącą do opisu zakresu oddziaływania władzy, tożsamości i kontroli w różnych wymiarach rzeczywistości społecznej.

W tym podejściu cyberprzestrzeń wychodzi z ram wyłącznie niematerialnych i posiada również cechy fizyczne (materialne) stanowiąc „wyobrażony świat powstały dzięki połączeniu urządzeń komputerowych w sieci umożliwiającej komunikację”<sup>6</sup>. „Z technicznego punktu widzenia cyberprzestrzeń to przestrzeń pojęciowa, która istnieje w świecie fizycznym i obok niego. Nie jest to fizyczna lokalizacja, ale raczej zbiór danych cyfrowych, kanałów komunikacyjnych i zasobów obliczeniowych, które rozciągają się ponad granicami geograficznymi”<sup>7</sup>. Tym samym granice cyberprzestrzeni wyznaczają jej materialne składniki i możliwe staje się operacyjne wyznaczenie jej granic za pomocą kreującej ją infrastruktury<sup>8</sup>. A zatem cyberprzestrzeń przyjmuje tutaj zarówno cechy terytorialności, jak i graniczności.

### **4. Konkluzje**

Problem (a)terytorialności i (bez)graniczności jako cech cyberprzestrzeni zależy od podejścia do ich struktur bazowych, czyli „terytorium” i „granicy”. Traktowanie ich jako fizycznych struktur przestrzennych ujawnia zarówno ich aterytorialny, jak bezgraniczny charakter. Przyjmując niefizyczny charakter obu tych struktur przestrzennych, cyberprzestrzeń posiada zarówno cechy terytorialne, jak i graniczne. Dla porządku, warto na zakończenie

również odnotować rzadziej spotykaną w literaturze interpretację „aterytorialności” cyberprzestrzeni, jako pewnej ogólnej metafory oznaczającej brak różnorodnych ram (ograniczeń) przestrzennych, tak fizycznych jak i niefizycznych<sup>9</sup>. Konkludując, cyberprzestrzeń ma strukturę dualistyczną, zarówno fizyczną (materialną) jak i niefizyczną (niematerialną) i tak powinna być postrzegana oraz jej własności, a wszelkie uproszczenia w tym zakresie, zwłaszcza w nauce, są błędne i nie powinny mieć miejsca.

## **5. Implikacje dla nauk o bezpieczeństwie**

Rozstrzygnięcia dotyczące (a)terytorialności i (bez)graniczności cyberprzestrzeni mają istotne znaczenie dla badań nad bezpieczeństwem informacyjnym. Traktowanie cyberprzestrzeni jako przestrzeni całkowicie aterytorialnej i pozbawionej granic sprzyja uproszczonemu postrzeganiu zagrożeń informacyjnych jako zjawisk nieosadzonych w konkretnych strukturach. Tymczasem przyjęcie perspektywy uwzględniającej zarówno materialne, jak i niematerialne komponenty cyberprzestrzeni pozwala na realistyczne ujęcie środowiska informacyjnego.

Z punktu widzenia bezpieczeństwa informacyjnego cyberprzestrzeń nie jest przestrzenią pozbawioną granic, lecz obszarem, w którym granice ulegają redefinicji. Są one wyznaczone przede wszystkim przez infrastrukturę informacyjno-komunikacyjną, ramy prawne oraz zdolności instytucjonalne do kontroli i ochrony informacji. Oznacza to, że zagrożenia informacyjne oddziałują poprzez konkretne zasoby, systemy i procesy, a nie w całkowicie „bezgranicznym” środowisku.

Implikacją takiego podejścia staje się konieczność odejścia od abstrakcyjnych ujęć bezpieczeństwa informacyjnego na rzecz analiz koncentrujących się na identyfikacji kluczowych elementów systemu informacyjnego, takich jak węzły infrastrukturalne, przepływy danych czy mechanizmy decyzyjne. Bezpieczeństwo informacyjne należy w tym sensie postrzegać jako proces zarządzania granicami funkcjonalnymi i normatywnymi, a nie jako próbę ochrony przestrzeni całkowicie pozbawionej struktury.

W tym kontekście szczególnego znaczenia nabiera pojęcie „państwowej cyberprzestrzeni”, rozumianej nie jako odrębna, zamknięta przestrzeń techniczna, lecz jako wyodrębniony funkcjonalnie fragment cyberprzestrzeni, nad którym państwo sprawuje określony zakres kontroli, regulacji i odpowiedzialności. Obejmuje ona zarówno materialne komponenty infrastruktury teleinformatycznej zlokalizowanej na terytorium państwa, jak i niefizyczne elementy porządku normatywnego, instytucjonalnego i informacyjnego. Stanowi to przykład praktycznej realizacji tezy o dualistycznej naturze cyberprzestrzeni, łączącej

wymiar terytorialny i graniczny z elementami o charakterze funkcjonalnym i niematerialnym. Jej istnienie podważa skrajne interpretacje cyberprzestrzeni jako przestrzeni całkowicie bezgranicznej i aterytorialnej, wskazując, że także w środowisku cyfrowym możliwe jest wyznaczanie zakresów władzy, odpowiedzialności i ochrony właściwych dla państwa.

W konsekwencji pojęcia aterytorialności i bezgraniczności powinny być w badaniach nad bezpieczeństwem informacyjnym stosowane ostrożnie i precyzyjnie, z wyraźnym wskazaniem, do jakiego wymiaru cyberprzestrzeni się odnoszą. Tylko takie podejście umożliwia formułowanie adekwatnych diagnoz zagrożeń oraz projektowanie skutecznych mechanizmów ochrony informacji.

---

<sup>1</sup> *Wielki Słownik Języka Polskiego*, <https://wsjp.pl/>.

<sup>2</sup> Ibidem.

<sup>3</sup> Agnieszka Warchoń, A, *Pojęcie cyberprzestrzeni w strategiach bezpieczeństwa państw członkowskich Unii Europejskiej*, „*Studia de Securitate*” nr 4/2019, s. 98; Hanna Sommer, Hubert Sommer, Grzegorz Zakrzewski, *Redefinicja oceny kultury cyberbezpieczeństwa przez młodzież Podkarpacia* [w:] Hanna Sommer, Wojciech Sokołowski, Jacek Fabisiak, Grzegorz Zakrzewski (red.), *Czas na bezpieczeństwo: Miscellanea*, część 1. Rzeszów: Oficyna Wydawnicza Politechniki Rzeszowskiej, 2023, s. 25-26; Włodzimierz Fehler (red.), *Leksykon bezpieczeństwa informacyjnego*. Siedlce: Wydawnictwo UPH, 2023, s. 73.

<sup>4</sup> Grażyna Balawajder, *Granica państwa jako kategoria analityczna* [w:] „Pogranicze. Polish Borderland Studies” nr 1/2013, s. 77.

<sup>5</sup> David Delaney, *Territory* [w:] Rob Kitchin, Nigel Thrift (red.), *International Encyclopedia of Human Geography*, Amsterdam: Elsevier, 2009, s. 196.

<sup>6</sup> *Wielki Słownik ...*, op. cit.

<sup>7</sup> Hanna Sommer, Hubert Sommer, Grzegorz Zakrzewski, op.cit.

<sup>8</sup> Andrzej Warchoń, *Pojęcie cyberprzestrzeni w strategiach bezpieczeństwa państw członkowskich Unii Europejskiej* [w:] „*Studia de Securitate*” nr 9/2019, s. 98.

<sup>9</sup> Marek Marczyk, *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru* [w:] „*Przegląd Teleinformatyczny*”, nr 1-2/2018, s. 60; Zbigniew Chmielewski, *Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich* [w:] „*Polityka Publiczna*”, nr 2/2016, s. 105.