



Redakcja: Grzegorz Gil (dyrektor IEŚ), Anton Saifullayev
(zastępca dyrektora IEŚ), Agnieszka Zajdel (sekretarz redakcji),
Spasimir Domaradzki, Aleksandra Kuczyńska-Zonik, Damian
Szacawa, Agata Tatarenko

Nr 1725 (230/2026) | 20.10.2026

ISSN 2657-6996
© IEŚ

Jakub Olchowski

Konsekwencje ukraińskich ataków na centra danych firmy Yandex

Między 7 a 11 października 2026 r. siły ukraińskie przeprowadziły ataki dronowe na centra danych firmy Yandex¹. Zaatakowano trzy z sześciu (wg oficjalnych danych) centrów rosyjskiego giganta technologicznego. W kolejnych dniach pojawiło się wiele doniesień, także w Polsce, że w wyniku ukraińskich ataków zmniejszyła się intensywność rosyjskich działań propagandowych i dezinformacyjnych (m.in. wspierających AfD w Niemczech czy ruch MAGA w USA). Informacje te nie znalazły potwierdzenia – aktywność rosyjskich botów i trolli nie spadła. Ataki przyniosły jednak poważne konsekwencje innego rodzaju.

słowa kluczowe: Rosja, Ukraina, Yandex, dezinformacja, centra danych, odporność społeczna, zaplecze technologiczne

Doniesienia o ograniczeniu rosyjskiej propagandy. Po ukraińskich atakach na centra danych Yandexu pojawiło się wiele opinii internautów, komentatorów, polityków itp., jakoby zmniejszyła się intensywność prorosyjskiej propagandy, zwłaszcza w mediach społecznościowych. W tym kontekście pojawiały się też infografiki i wykresy mające potwierdzać tę tendencję. Jak się później okazało, były one generowane przez sztuczną inteligencję. Według instytucji badających cyberzagrożenia oraz rosyjską dezinformację i propagandę (w tym polskich – Disinfo Digest, Niebezpiecznik, NASK, Demagog) nie doszło do takiego ograniczenia prorosyjskiej aktywności w sieci. Jak wskazywali eksperci, ataki doprowadziły do ograniczenia aktywności *crawlerów*, botów indeksujących strony dla wyszukiwarki, a nie zautomatyzowanych kont siejących dezinformację w mediach społecznościowych. Ponadto wskazywano, że rosyjskie „fabryki trolli” mają inne zaplecze technologiczne, niezwiązane z Yandexem.

Rzeczywiste skutki ataków. Ataki na Yandex w istocie doprowadziły do poważnych konsekwencji dla Rosji. Nastąpiły zakłócenia w działaniu kilkudziesięciu usług Yandexu. Przestały funkcjonować lub działały znacznie wolniej m.in. Yandex Go (odpowiednik Bolta), Yandex Pay (odpowiednik Google Pay), Yandex Music, asystent SI Alisa, usługa wideokonferencji Telemost, poczta elektroniczna, usługi w chmurze Yandex Cloud (np. serwis randkowy Twinby), liczne sklepy i usługi dowozu żywności – łącznie dotyczyło to ponad 80 usług. Problemy te dotknęły nie tylko Rosję, ale także państwa, w których popularne są usługi oparte na rozwiązaniach i infrastrukturze sieciowej Yandexu, np. Mołdawię, Uzbekistan, Kazachstan, Armenię czy Białoruś. Silne uzależnienie innych rosyjskich podmiotów technologicznych od usług Yandexu spowodowało efekt domina i załamanie się wielu innych serwisów chmurowych, sieci i usług. Dodatkowo atak na centra danych wpłynął na możliwości rozwoju rosyjskiej sztucznej inteligencji.

Wnioski. Ukraińskie ataki na rosyjskie centra danych były odpowiedzią na analogiczne działania Rosji wymierzone w ukraińską infrastrukturę cyfrową. Ich znaczenie wykracza jednak poza wzajemne uderzenia w zaplecze

¹ Największe rosyjskie przedsiębiorstwo technologiczne, od 2024 r., po wymuszonych przez zachodnie sankcje przekształceniach własnościowych, *de facto* kontrolowane przez państwo. Podobnie jak np. Google oferuje szeroki zestaw usług: wyszukiwarkę, pocztę elektroniczną, mapy, nawigację, system płatności, asystenta SI, serwisy chmurowe itp.



technologiczne przeciwnika. Pokazują one, że jednym z nowych frontów współczesnej wojny staje się infrastruktura warunkująca funkcjonowanie społeczeństwa i gospodarki, w coraz większym stopniu uzależnionych od usług cyfrowych. Ukraina, dzięki decentralizacji infrastruktury i przeniesieniu jej części poza granice kraju, okazała się mniej podatna na tego rodzaju ataki. W Rosji natomiast blisko 80% centrów danych znajduje się w Moskwie i jej okolicach, co zwiększa ich podatność na uderzenia ukraińskich dronów. Należy przy tym podkreślić, że w październiku zaatakowana została nie tylko infrastruktura Yandexu, ale również centra danych koncernu VK (operatora m.in. sieci społecznościowej VKontakte i komunikatora Max) oraz największej rosyjskiej instytucji finansowej – Sberbanku.

Ataki ujawniły słabości rosyjskiego modelu rozwoju infrastruktury cyfrowej. Prowadzony od dekady proces budowy „suwerennego internetu” (Runetu), zakładający utrzymywanie infrastruktury i danych na terytorium Rosji oraz podporządkowanie ich państwowej kontroli, miał zwiększyć niezależność od zagranicznych rozwiązań. W praktyce doprowadził jednak do koncentracji zasobów i powstania wzajemnych zależności między usługami i podmiotami technologicznymi. Zakłócenia w funkcjonowaniu Yandexu wywołały efekt domina, który objął również liczne serwisy innych dostawców. W ten sposób próba zwiększenia cyfrowej suwerenności ujawniła zarazem podatność rosyjskiego systemu na uderzenia w jego kluczowe elementy. Konsolidacja wielu usług w ramach jednego podmiotu-dostawcy naraziła funkcjonowanie całego ekosystemu rosyjskiej gospodarki.

Konsekwencje ataków mogą być odczuwalne w Rosji przez dłuższy czas. Przywrócenie pełnej funkcjonalności usług będzie wymagało czasu i znacznych nakładów finansowych. Dodatkowym utrudnieniem są sankcje oraz wynikająca z nich ograniczona dostępność zachodnich komponentów i technologii wykorzystywanych przy budowie i wyposażaniu centrów danych. Zakłócenia uderzają nie tylko w użytkowników indywidualnych, lecz także w przedsiębiorstwa, szczególnie w dużych miastach, i mogą przekładać się na wzrost kosztów usług. W dłuższej perspektywie problemy techniczne mogą również osłabić pozycję rynkową Yandexu w państwach, w których jego rozwiązania są popularne.

Nie ma natomiast potwierdzenia, że ataki doprowadziły do ograniczenia rosyjskiej propagandy i dezinformacji w mediach społecznościowych. Ewentualny spadek aktywności niektórych kont mógł mieć charakter przejściowy i wynikać z zakłóceń technicznych, ale nie oznaczał wyłączenia zaplecza rosyjskich operacji informacyjnych. Co istotne, same doniesienia o rzekomym osłabieniu propagandy okazały się przykładem dezinformacji. Warto też podkreślić, że SI będzie coraz ważniejszym narzędziem tworzenia i uwiarygodniania fałszywych treści.

Ukraina zapowiada kontynuację działań, a ich dotychczasowe rezultaty można uznać za istotny sukces operacyjny. Nie należy jednak utożsamiać go z osłabieniem rosyjskich operacji informacyjnych. Znaczenie ataków polega przede wszystkim na ujawnieniu podatności rosyjskiej infrastruktury cyfrowej, wywołaniu realnych kosztów gospodarczych i technologicznych oraz pokazaniu, że w warunkach współczesnego konfliktu infrastruktura cyfrowa staje się równie istotnym celem jak inne elementy zaplecza państwa.

Problem ten ma szersze znaczenie dla bezpieczeństwa państw zachodnich, które również muszą uwzględniać ryzyko ataków na infrastrukturę cyfrową. Wzajemne uderzenia rosyjskie i ukraińskie nie są jedynym przykładem tego rodzaju działań wojennych. W marcu i kwietniu 2026 r. Iran zaatakował dronami centra danych Amazon Web Services (AWS) w Bahrajnie i Zjednoczonych Emiratach Arabskich. Spowodowało to zawieszenie działalności Amazonu w regionie i zakłócenia w funkcjonowaniu bankowości oraz infrastruktury cyfrowej opartej na chmurze AWS. Pół roku później koncern przyznał, że doszło do nieodwracalnej utraty wielu zasobów i danych.



Infrastruktura cyfrowa, coraz istotniejsza z punktu widzenia funkcjonowania państw, ich gospodarek, społeczeństw i potencjałów militarnych, będzie celem ataków, ponieważ uderzenia w nią mogą przynosić zarówno korzyści *stricte* wojskowe, jak i osłabiać odporność społeczną poprzez zakłócanie usług cywilnych. Przykład Rosji pokazuje, że błędem jest próba budowania suwerenności cyfrowej poprzez izolację i centralizację infrastruktury.