Polsko-Ukraińskie Studia Interdyscyplinarne
2025, nr 2 (15), s. 33–38

https://czasopisma.marszalek.com.pl/en/10-15804/pom
DOI: 10.15804/PPUSI.2025.2.03

Zuzanna Bakun
Uniwersytet Szczeciński
Wydział Nauk Społecznych
Instytut Nauk o Polityce i Bezpieczeństwie
243403@stud.usz.edu.pl

CYBERATAKI JAKO NARZĘDZIE NOWOCZESNYCH KONFLIKTÓW ZBROJNYCH

Streszczenie: Artykuł dotyczy cyberataków w kontekście wojny na Ukrainie, ze szczególnym uwzględnieniem ataków hakerskich na instytucje państwowe, banki, infrastrukturę krytyczną oraz obywateli. Przedstawia, jaką rolę odgrywają cyberataki w nowoczesnych konfliktach zbrojnych, zwłaszcza w kontekście toczącej się wojny na Ukrainie. Omówione zostanie, jak cyberataki zostały użyte przez Federację Rosyjską jako narzędzie destabilizacji państwowej, zakłócania funkcjonowania kluczowych sektorów oraz destabilizacji życia obywateli. Szczególna uwaga zostanie zwrócona na ataki, które dotyczyły administracji publicznej, w tym urzędów rządowych i infrastruktury krytycznej, a także ataki na sektor finansowy, który miał na celu zarówno destabilizację gospodarki, jak i kradzież danych osobowych obywateli. Poruszone zostaną również zagadnienie ataków hakerskich skierowanych na sojuszników Ukrainy, w tym inne państwa NATO, oraz metody obrony przed tego typu zagrożeniami, w tym działania podejmowane przez Ukrainę oraz współpracę międzynarodową w celu ochrony przed cyberatakami. Celem jest ukazanie, jak cyberataki stały się integralnym elementem współczesnych konfliktów zbrojnych i w jaki sposób państwa oraz społeczeństwa muszą wzmacniać swoje zdolności w zakresie obrony cyfrowej, by skutecznie przeciwdziałać tym zagrożeniom.

Słowa kluczowe: Ukraina, wojna hybrydowa, cyberataki

CYBERATTACKS AS A TOOL IN MODERN ARMED CONFLICTS

Abstract: The article concerns cyberattacks in the context of the war in Ukraine, with particular emphasis on hacker attacks on state institutions, banks, critical infrastructure, and citizens. It will present the role that cyberattacks play in modern armed conflicts, especially in the context of the ongoing war in Ukraine. It will discuss how cyberattacks have been used by the Russian Federation as a tool to destabilize the state, disrupt key sectors, and destabilize the lives of citizens. Particular attention will be paid to attacks that targeted public administration, including government offices and critical infrastructure, as well as attacks on the financial sector, which aimed to both destabilize the economy and steal citizens' personal data. The issue of hacker attacks on Ukraine's allies, including other NATO countries, and methods of defending against such threats, including actions taken by Ukraine and international cooperation to protect against cyberattacks, will also be discussed. The aim is to show how cyberattacks have become an integral part of contemporary armed conflicts and how states and societies need to strengthen their cyber defence capabilities to effectively counter these threats.

Keywords: Ukraine, hybrid war, cyberattacks

Wstęp

Cyberprzestrzeń od ponad dekady stanowi pole walki w konfliktach międzynarodowych, jednak dopiero konflikt rosyjsko-ukraiński ukazał jego pełne spektrum. Ukraina od 2014 roku doświadczała wzmożonych cyberataków na infrastrukturę krytyczną, instytucje rządowe czy obywateli, jednakże owe ataki przybrały na wyrafinowaniu i poszerzyły swoją skalę wraz z inwazją Rosji w lutym 2022 r. Cyberataki stały się wtedy integralną częścią działań wojskowych, a nie tylko działaniami wspomagającymi. Konflikty w cyberprzestrzeni charakteryzują się trudnościami w przypisaniu winnych, wielowarstwowością działań oraz połączeniem aspektów militarnych, politycznych i psychologicznych. Ukraina stała się nie tylko polem walki w tradycyjnym rozumieniu, lecz także poligonem cyfrowym, gdzie testowane są nowe techniki, narzędzia i strategie cyberprzestępcze.

Ewolucja cyberataków 2014–2022

Pierwsze związki cyberprzestępczości z prowadzonymi działaniami militarnymi były widoczne już w 2014 r., zaraz po aneksji Krymu. Ukraina stała się celem operacji związanych z rosyjskimi grupami hakerskimi, takimi jak Sandworm, APT28, APT29 oraz Gamaredon. Celem tych działań była przede wszystkim dezintegracja instytucji rządowych, sianie paniki i dezinformacji wśród obywateli ukraińskich oraz pozyskiwanie ważnych informacji z zainfekowanych systemów państwowych (EPRS, 2022).

Momentem przełomowym był przeprowadzony w grudniu 2015 r. atak na infrastrukturę energetyczną, kiedy doszło do przejęcia kontroli nad systemem SCADA (Supervisory Control And Data Acquisition), co doprowadziło do wyłączenia prądu w zachodniej części kraju. Dotknięty atakiem Prykarpattya Oblenergo dostarcza energię elektryczną tylko w obwodzie iwano-frankiwskim. Ów obwód zamieszkiwało wtedy około 1,4 miliona mieszkańców, z czego ponad połowa została dotknięta skutkami cyberataku (Fundacja im. Kazimierza Pułaskiego, 2016).

W 2016 r. podobny incydent nastąpił w Kijowie, z użyciem narzędzia Industroyer, a w 2017 r. pojawił się NotPetya – destrukcyjny malware, który wywołał globalne szkody gospodarcze. Zainfekowano systemy aktualizacji programu MeDoc, co umożliwiło penetrację setek firm i instytucji. Ucierpiały również podmioty poza Ukrainą, w tym w USA i krajach UE. Wydarzenia te dowiodły, że cyberatak może mieć wymiar międzynarodowy i wpływ na globalne bezpieczeństwo (Sekurak, 2021).

Ataki „przedinwazyjne" styczeń–luty 2022

Kilka tygodni przed zbrojną inwazją na Ukrainę Federacja Rosyjska zaczęła prowadzić intensywną kampanię cybernetyczną, która miała na celu osłabić zdolności reagowania ukraińskich instytucji, szerzenie strachu i chaosu wśród społeczeństwa oraz osłabienie morali wśród ludności.

14 stycznia 2022 r. ponad 70 witryn rządowych, jak i publicznych (państwowych i międzynarodowych) padło ofiarą ataku typu defacement. W wyniku ataku doszło do podmiany zawartości strony. Opublikowany został plik graficzny zawierający treść napisaną w języku ukraińskim, rosyjskim i polskim. Treść głosiła: „Ukrainiec! Wszystkie Twoje dane osobowe zostały przesłane do wspólnej sieci. Wszystkie dane na komputerze są niszczone, nie można ich odzyskać. Wszystkie informacje o Tobie stały się publiczne, bój się i czekaj na najgorsze. To dla Ciebie za twoją przeszłość, teraźniejszość i przyszłość. Za Wołyń, za OUN UPA, Galicję, Polesie i za tereny historyczne" (CSIRT MON, 2022). Ów komunikat miał na celu wprowadzić niepewność, strach i zawirowania w stosunkach między Polską a Ukrainą. Nie ułatwiał tego fakt, że dane geograficzne pliku graficznego wskazywały Parking Głównej Szkoły Handlowej w Warszawie. Jednak nie zachwiało to stosunkami między sąsiadami, ale z pewnością miało negatywny wpływ na odczucie bezpieczeństwa wśród ukraińskich obywateli.

15 lutego 2022 r. doszło do skoordynowanych ataków typu DDoS na największe banki – PrywatBank i Oschadbank – oraz instytucje rządowe, jak Ministerstwo Obrony Ukrainy (Business Insider Polska, 2022). Ataki były krótkotrwałe, ale bardzo intensywne – w szczycie osiągano nawet 200 Gbps ruchu. Atak polegał na przeciążeniu serwerów, co spowodowało niedostępność stron rządowych, bankowości internetowej i aplikacji mobilnych banków (PISM, 2022). Oprócz niedostępności usług klienci banków otrzymywali fałszywe wiadomości SMS z polskich numerów kierunkowych, które informowały o problemach technicznych. Miało to wskazywać

na Polskę jako kraj odpowiedzialny za przeprowadzenie ataku. Podobnie jak we wcześniejszym ataku, celem było szerzenie strachu i dezinformacji wśród ludności cywilnej, ale również był to sprawdzian zdolności obronnych ukraińskich instytucji.

W przeddzień kinetycznej inwazji doszło do kolejnego cyberataku na infrastrukturę krytyczną, w instytucjach rządowych, sektorze obronnym, lotniczym, finansowym oraz branży IT. Złośliwe oprogramowanie znajdowało się na urządzeniach już w listopadzie–grudniu 2021 r., co jednoznacznie wskazuje na długotrwałe przygotowanie do owego ataku. HermeticWiper, bo to o nim tutaj mowa, wykorzystywał legalnie wyglądający certyfikat EV z firmy Hermetica Digital Ltd z Cypru, co skutecznie ułatwiło ominięcie ukraińskich systemów bezpieczeństwa. Celem było szybkie oraz masowe wyłączenie infrastruktury strategicznej w sytuacji konfliktu zbrojnego (ESET, 2022). Takowe działania wpisują się w strategię cyberwojny Rosji, która zakłada destabilizację przeciwnika przed atakiem lądowym.

Skala ataków podczas wojny (2022–2024)

Od rozpoczęcia inwazji wojskowej w lutym 2022 r. Ukraina stała się celem bezprecedensowej liczby cyberataków. Z danych podanych przez Ministerstwo Transformacji Cyfrowej oraz CERT-UA publikowanych w ukraińskich mediach wynika, że:

- w 2022 r. odnotowano 1 785 incydentów,
- w 2023 – 2 541 incydentów,
- w 2024 – 4 315 incydentów.

To ponad 8 tysięcy ataków w ciagu trzech lat (Ukrainska Pravda, 2025). Tylko w pierwszym kwartale 2024 r. zanotowano więcej incydentów niż w całym 2021 r. Dominującymi typami ataków były: zaawansowane kampanie DDoS, ransomware, phishing spear-targeted, exploitowanie systemów legacy, a także wykorzystanie socjotechniki (INFO ITTA, 2023).

Warto dodać, że celem nie były wyłącznie instytucje państwowe. Wzrastała liczba ataków na:

- systemy transportowe (kolej, lotnictwo, metro),
- firmy IT oraz dostawców usług w chmurze – ok. 4000 ataków hakerskich,
- organizacje pozarządowe i media niezależne,
- placówki opieki zdrowotnej, w tym mobilne szpitale wojskowe – WHO odnotowała 2 254 ataki,
- infrastrukturę krytyczną.

Przypadki strategicznej destrukcji infrastruktury

Atak 12 grudnia 2023 r. na ukraińskiego operatora komórkowego – Kyivstar, wywołał największy jak do tej pory chaos komunikacyjny w kraju (PAP, 2024). Zakłócenie usług dotknęło ponad 24 miliony obywateli, komunikację wojskową, ale co ważniejsze z punktu widzenia bezpieczeństwa cywili, systemy ewakuacyjne oraz system ostrzegania przed nalotami (syreny, powiadomienia mobilne) przestały działać w wielu regionach. Ukraińskie służby szybko wprowadziły alternatywne metody ostrzegania, jednak wywołało to ogromny chaos i niepokój wśród społeczeństwa (AP News, 2023).

Ataki na infrastrukturę energetyczną są jednymi z najczęstszych cyberataków od czasu pełnoskalowej inwazji na Ukrainę. Między październikiem 2022 a wrześniem 2024 przeprowadzono ponad 1 024 ataki na obiekty energetyczne – podaje minister energii Herman Gałuszczenko (UNN, 2024). To doskonale obrazuje skalę owych ataków. Takowe ataki wpływają negatywnie oczywiście na podmioty militarne, ale przede wszystkim na ludność cywilną, która w czasie różnych warunków pogodowych i stadium nasilenia konfliktu zostaje bez dostępu do ogrzewania, światła, a także informacji czy komunikatów mających zwiększyć bezpieczeństwo, czy to za pomocą specjalnych aplikacji, czy specjalnych kanałów Telegram. Bardzo często tego typu cyberataki zbiegały się w czasie z rosyjskimi atakami rakietowymi, co pozwalało zmaksymalizować ich skutki.

Statystyki

W 2023 r. liczba cyberataków na Ukrainę znacznie wzrosła, co odzwierciedla rosnące zagrożenia dla różnych sektorów kraju. Według raportu CERT-UA w ciągu roku zarejestrowano 2543 incydenty cybernetyczne, co stanowi wzrost o 15,9% względem roku 2022. Poniżej przedstawiono szczegółowe statystyki dotyczące ataków na poszczególne sektory:

- rządowe organizacje – 347 ataków,
- lokalne władze – 276 ataków,
- sektor bezpieczeństwa i obrony – 175 ataków,
- komercyjne organizacje – 127 ataków,
- sektor energetyczny – 92 ataki,
- telesieci – 81 ataków,

- instytucje edukacyjne – 38 ataków,
- transport – 32 ataki,
- sektor finansowy – 30 ataków,
- IT – 25 ataków,
- media – 15 ataków,
- instytucje medyczne – 12 ataków (Vikna, 2024).

Wsparcie międzynarodowe

Międzynarodowa pomoc obejmowała m.in.:

- transfer infrastruktury chmurowej (USA, Estonia, Polska),
- szkolenia dla ponad 1 000 ukraińskich specjalistów w ramach NATO CCDCOE,
- darmowe licencje Microsoft Defender, Google Shield Project,
- tworzenie bezpiecznych stref danych (Data Safe Havens) na Litwie i w Polsce,
- inicjatywę G7 dotyczącą standardów cyberodporności w państwach objętych wojną,
- pomoc humanitarną dla obywateli Ukrainy,
- pomoc w postaci sprzętu wojskowego.

Ataki na kraje wspomagające

Nie tylko Ukraina mierzy się ze zwiększoną liczbą cyberataków od rozpoczęcia wojny. Ten problem dotyczy również jej sojuszników, jak na przykład Polska, Francja, Niemcy czy USA. Lista państw wpierających jest oczywiście dużo dłuższa.

Niemcy od stycznia do marca 2023 r. mierzyły się z atakami na serwisy Bundestagu, federalnych ministerstw, lotnisk i wybranych banków. Systemy informacyjne lotnisk przestały działać, co było utrudnieniem dla pasażerów (m.in. brak aktualizacji o lotach, problemy z odprawą online). Doszło również do chwilowych zakłóceń w dostępności e-bankowości i płatnościach online. Atak miał typ zakłóceń, a nie kradzieży danych, do jego przeprowadzenia użyto demoty DDoS (BiznesAlert, 2023).

Od września 2022 do grudnia 2023 r. w Stanach Zjednoczonych dochodziło do cyklicznych cyberataków na szpitale i instytucje medyczne wspierające Ukrainę m.in. w Iowa, Illinois, Kalifornii i Nowym Jorku. Skutkowały one czasowym zamknięciem oddziałów ratunkowych, odwołaniem zaplanowanych operacji i zabiegów, opóźnieniem w wydawaniu recept i dostępie do dokumentacji medycznej (Becker's Health It, 2023). Na skutek takich działań jedna osoba zmarła. Ataki zostały przypisane grupie Sandworm i zbiegły się z kolejnymi paktami pomocowymi dla Ukrainy.

Na przełomie stycznia i lutego 2023 r. dochodziło do zmasowanych ataków na infrastrukturę transportową we Francji. Celami były m.in. francuski narodowy operator kolei (SNCF) oraz operator paryskiej komunikacji miejskiej (RATP) (CSIDB, 2023). Ataki zostały wymierzone w aplikacje mobilne, systemy wyświetleń tras i rozkładów jazdy oraz systemy rezerwacji przejazdów. Nie doszło do przejęcia kontroli nad systemami sterowania ruchem, jednak wprowadziło to powszechny chaos wśród obywateli francuskich. Sprawcą ataków była prorosyjska grupa haktywistyczna –Killnet, wspierana przez grupę NoName057(16), która przeprowadziła atak jako odpowiedź Federacji Rosyjskiej na pomoc Francji udzieloną Ukrainie, tj. dostawę haubic CAESAR i wsparcie szkoleniowe.

Cyberataki związane z pomocą udzieloną Ukrainie nie ominęły również Polski, gdzie dnia 31 maja 2024 r. została zaatakowana Państwowa Agencja Prasowa (PAP). O godzinie 14 do opinii publicznej dotarła informacja, że z dniem 1 lipca 2024 r. zacznie się częściowa mobilizacja, która miałaby się wiązać z powołaniem 200 000 Polaków, byłych wojskowych, jak i cywili, którzy mieliby zostać wysłani do Ukrainy. Polskie służby, premier, wicepremier oraz minister cyfryzacji szybko obalili tę fałszywą depeszę (PAP, 2024). Jednak wywołała ona spore zamieszanie wśród Polaków, którzy zaczęli obawiać się wysłania na ukraiński front. Minister cyfryzacji – Krzysztof Gawkowski potwierdził, że było to działanie rosyjskich służb wywiadowczych, mające na celu destabilizację i szerzenie dezinformacji.

Wnioski

Wydarzenia na Ukrainie ukazują, że cyberwojna stanowi realne zagrożenie w XXI wieku i staje się nieodłącznym elementem wojny w tradycyjnym rozumieniu. Ten konflikt pokazał, że obrona cyfrowa musi być częścią strategii narodowego bezpieczeństwa. Kluczowe dla zapewnienia cyberbezpieczeństwa powinno być:

- ustawowe uregulowanie obowiązków bezpieczeństwa dla sektora prywatnego,

- wspólne protokoły reagowania w ramach UE i NATO,
- rozwój centrów kompetencji i lokalnych SOC (Security Operation Center),
- promowanie cyberedukacji od poziomu szkoły podstawowej.

Mimo licznych cyberataków na różne sektory życia, zaczynając od administracji państwowej, a kończąc na sektorze obywatelskim, Ukrainie stale udaje się je odpierać i wzmacniać swoje cyberbezpieczeństwo. Dzięki temu stała się liderem cyfrowej odporności. Jej doświadczenia powinny stanowić fundament europejskiej i globalnej architektury bezpieczeństwa cyfrowego. Należy sobie zatem zadać pytanie, co nowego wymyślą strony konfliktu, żeby zagrozić przeciwnikowi? Jak to wpłynie na postrzeganie bezpieczeństwa nie tylko przez obywateli Ukrainy, ale również obywateli Polski czy całej Unii Europejskiej? Czy wojna w niedalekiej przyszłości będzie opierać się tylko na cyberwojnie?

Bibliografia

1. Przetacznik, J. & Tarpova, S. (2022, czerwiec). *Russia's war on Ukraine: Timeline of cyber-attacks* (EPRS BRI (2022) 733549 EN). European Parliamentary Research Service, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI%282022%29733549_EN.pdf.
2. Gapiński, K. (2016, 5 stycznia). *Blackout w zachodniej Ukrainie – cyber atak o wymiarze międzynarodowym*. Fundacja im. Kazimierza Pułaskiego, https://pulaski.pl/komentarz-blackout-w-zachodniej-ukrainie-cyber-atak-o-wymiarze-miedzynarodowym.
3. Góra, M. (2021, 21 maja). *Rosyjska cyberofensywa na Ukrainie, czyli czego spodziewać się już dziś.* Sekurak, https://sekurak.pl/rosyjska-cyberofensywa-na-ukrainie-czyli-czego-spodziewac-sie-juz-dzis.
4. CSIRT MON (2022, 17 stycznia). *Analiza cyberataku na ukraińskie zasoby rządowe*. Ministerstwo Obrony Narodowej, https://csirt-mon.wp.mil.pl/aktualnosci/analiza-cyberataku-na-ukrainskie-zasoby-rzadowe.
5. Business Insider Polska (2022, 15 lutego). *Ukraińskie władze potwierdzają atak na strony internetowe*, https://businessinsider.com.pl/wiadomosci/ukrainskie-wladze-potwierdzaja-atak-na-strony-internetowe/kckghbl.
6. Polski Instytut Spraw Międzynarodowych (2022, 17 lutego). *Cyberatak na Ukrainę*, https://pism.pl/publikacje/cyberatak-na-ukraine.
7. ESET (2022, 1 marca). *ESET Research: Ukraine hit by destructive attacks before and during the Russian invasion with HermeticWiper and IsaacWiper*. ESET Blog, https://blog.eset.ie/2022/03/01/eset-research-ukraine-hit-by-destructive-attacks-before-and-during-the-russian-invasion-with-hermeticwiper-and-isaacwiper.
8. Artemchuk, O. (2025, 9 stycznia) *Russia carried out 1,400 cyberattacks on Ukraine in 2023 – Intelligence*. Ukrainska Pravda, https://www.pravda.com.ua/eng/news/2025/01/9/7492671.
9. ITTA (2023, 2 stycznia). *CERT-UA responds to over 2,000 cyber attacks on Ukraine in 2022*, https://itta.info/en/cert-ua-responds-to-over-2000-cyber-attacks-on-ukraine-in-2022.
10. Polska Agencja Prasowa (2024, 4 kwietnia). *SBU: Zidentyfikowaliśmy rosyjskich hakerów, którzy zaatakowali Kyivstar*, https://www.pap.pl/aktualnosci/sbu-zidentyfikowalismy-rosyjskich-hakerow-ktorzy-zaatakowali-kyivstar.
11. Novikov, I. (2023, 12 grudnia). *Russian cyberattack on Ukraine's Kyivstar mobile network was one of largest of its kind, officials say*. Associated Press, https://apnews.com/article/russia-ukraine-war-attacks-hackers-ad01b573ecc912c112ece8d63993a4ac.
12. UNN (2024, 11 września). *Halushchenko: Russia attacked Ukrainian energy sector more than 1,000 times in two years*, https://unn.ua/en/news/galushchenko-russia-attacked-ukrainian-energy-sector-more-than-1000-times-in-two-years.
13. Мельник В. (2024, 10 stycznia). *Кількість кібератак в Україні за 2023 рік зросла*. Vikna.tv, https://vikna.tv/dlia-tebe/bezpeka/kilkist-kiberatak-v-ukrayini-za-2023-rik-zrosla.
14. Fedorska, A. (2023, 17 lutego). *Kolejne problemy z cyberbezpieczeństwem lotnisk niemieckich*. BiznesAlert.pl, https://biznesalert.pl/niemcy-lotniska-cyberprzestrzen-transport.
15. Schwartz, N. (2023, 10 listopada). *4 hospitals targeted by cyberattacks*. Becker's Hospital Review https://www.beckershospitalreview.com/healthcare-information-technology/cybersecurity/4-hospitals-targeted-by-cyberattacks.
16. CSIDB (2023, 1 lutego). *Cyberattack targeting Lumila – subcontractor of SNCF*, https://www.csidb.net/csidb/incidents/13372045-a64c-4155-820e-7b69d96f99ba.
17. Polska Agencja Prasowa (2024, 31 maja). *Cyberatak na PAP. W serwisie Polskiej Agencji Prasowej nieprawdziwa depesza o mobilizacji*, https://www.pap.pl/aktualnosci/cyberatak-na-pap-w-serwisie-polskiej-agencji-prasowej-nieprawdziwa-depesza-o.