Tutoring Gedanensis

Tutoring Gedanensis 10(1)/2025 (56-64) ISSN 2451-1862

https://doi.org/10.26881/tutg.2025.1.05

Analiza zagadnień związanych z cyberwojną na podstawie cyberataków na Estonię (2007), ukraińską elektrownię (2015) oraz sieć satelitarną KA-SAT (2022)

Mikołaj Nowak
Uniwersytet Gdański, Wydział Filologiczny, Instytut Badań nad Kulturą
E-mail: mikolaj-nowak@outlook.com

tutor: dr Helena Draganik
Uniwersytet Gdański, Wydział Filologiczny, Instytut Badań nad Kulturą

Słowa kluczowe: cyberbezpieczeństwo, cyberprzestępczość, cyberterroryzm, cyberwojna, Ukraina

Wprowadzenie – cyberwojna i jej wizje

Kwestie związane z rozwojem technologii i idące za tym procesem szanse oraz zagrożenia stanowią bogaty rezerwuar idei możliwych do wykorzystania w przestrzeni szeroko rozumianej kultury popularnej. Jedną z koncepcji potencjalnego zagrożenia jest cyberwojna, która w tym obszarze niekiedy występuje jako wizja katastroficznych przemian. Można by w tym momencie odwołać się do skrajnego obrazu przejęcia kontroli nad ludzkością przez zbuntowane maszyny przedstawionego np. w filmie Matrix (1999). Warto byłoby jednak przytoczyć przykład bliższy podejmowanemu zagadnieniu, którym może być gra komputerowa Battlefield 2042 (2021). Rozwój technologiczny, informatyzacja przestrzeni oraz chaos składają się tutaj na przestrzeń funkcjonowania wojny, stanowią jej nieodłączne elementy. Hakowanie, zdalne unieszkodliwianie, namierzanie, manipulowanie otoczeniem za pomocą informatycznych narzędzi, czy zakłócanie są tego wyraźnym przykładem. Jest to natomiast przestrzeń przesadnie zdynamizowana, wynika to jednak z wymagań graczy względem wirtualnego świata oraz ich potrzeb dotyczących natychmiastowych doznań. Odbiorca, bez względu na to, czy jest widzem, czy graczem, nie może się nudzić. Fakt, iż kultura popularna w dużym stopniu operuje przekazami o właściwościach emocjonalnych, a tym samym niekiedy posuwa się do hiperbolizacji przedstawianych aspektów rzeczywistości, zapożyczonych z realnego świata, jest niepodważalny. Pojawiają się więc pytania: czym faktycznie jest cyberwojna i jakie formy może przybrać w rzeczywistości?

Niniejszy artykuł poddaje analizie problematykę związaną z definiowaniem cyber-

wojny i rozróżnieniem jej od innych negatywnych działań w cyberprzestrzeni. Podjęte rozważania mają na celu nakreślić potencjalną charakterystykę realnej wojny cybernetycznej. W oparciu o przegląd literatury, opinie ekspertów i instytucji zajmujących się cyberbezpieczeństwem wykazano, iż cyberwojna jest zjawiskiem wielowymiarowym. W artykule dokonano także analizy przypadków konkretnych incydentów, takich jak zmasowany atak cybernetyczny na Estonię z 2007 roku, atak na ukraińską elektrownię z 2015 roku czy zakłócenie sieci KA-SAT z 2022 roku.

Cyberwojna – problemy z definiowaniem

Cyberwojna to zjawisko, które rozgrywa się w specyficznej przestrzeni zwanej cyberprzestrzenią określanej niekiedy jako świat wirtualny. W polskim prawie cyberprzestrzeń definiowana jest w ramach ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej jako:

> […] przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 2070 oraz z 2022 r. poz. 1087) wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami (Dz. U. z 2002 r. Nr 156, poz. 1301).

W Tallinn Manual 2.0 – zbiorze wniosków z badań rozpoczętych już w 2013 roku (zob. Schmitt, 2013), w którym badacze analizowali możliwości aplikowania prawa międzynarodowego do kwestii związanych z cyberbezpieczeństwem – cyberprzestrzeń definiowana jest jako „środowisko tworzone przez fizyczne i niefizyczne komponenty do przechowywania, modyfikowania oraz wymiany danych za pomocą sieci komputerowych" (Schmitt, 2017: 564). Rozumienie tego zagadnienia jest jednak niejednoznaczne, gdyż jak zauważa Wojciech Cendrowski „większość państw ma swoje własne doktryny i strategie […] co implikuje wiele rozbieżności pod kątem nazewnictwa i kryteriów znamion, które miałyby charakteryzować konkretne zjawiska" (Cendrowski, 2017: 129) – dotyczy to zarówno definiowania cyberprzestrzeni, jak i cyberwojny (zob. Cendrowski, 2020).

Steve Winterfeld i Jason Andress (2013) proponują podejście stricte militarne oraz wskazują, że zarówno cyberprzestrzeń, jak i wojna, pomimo tego, iż zostały wielokrotnie zdefiniowane, nadal nie posiadają definicji używanych powszechnie. Korzystając z różnych źródeł, takich jak publikacje Departamentu Obrony Stanów Zjednoczonych oraz dzieła dotyczące teorii wojennej – O wojnie Carla von Clausewitza (2022) czy Sztuka wojny Sun Tzu (2014), autorzy zauważają fakt, że nie da się jednoznacznie wskazać definicji zarówno cyberprzestrzeni, wojny, jak i cyberwojny, pojęcia te są płynne i zależą w dużym stopniu od perspektywy definiującego (Winterfeld i Andress, 2013: 16–17).

François-Bernard Huyghe stwierdza, że „cyberwojna pozbawiona jest miejsca w przestrzeni i nie jesteśmy w stanie określić jej precyzyjnej lokalizacji" (Huyghe, 2011: 9). Trudności te prowokują pytanie o to, czy akty określane mianem cyberwojny nie mogłyby po prostu być interpretowane jako cyberprzestępstwa. Temat ten podejmuje politolog Thomas Rid (2013), który przytaczając traktat Clausewitza (2022), wskazuje na trzy kluczowe cechy (kryteria) wojny przedstawione przez pruskiego teoretyka – stosowanie przemocy (*violent*), instrumentalność (*instrumental*) oraz polityczność (*political*). Według badacza żadna cyberwojna nie powinna być określana mianem wojny, ponieważ nie spełnia wszystkich trzech kryteriów (Rid, 2013: 1–4).

Wojna cybernetyczna nie musi być jednak postrzegana jako odrębna kategoria, lecz można ująć ją jako na przykład element wojny sensu stricto. Zbliżoną koncepcję przedstawiają Paulo Shakarian, Jana Shakarian oraz Andrew Ruef (2013), którzy wychodząc od Clausewitzowskiej wojny jako „dalszego ciągu stosunków politycznych" (Clausewitz, 2022: 49), definiują cyberwojnę jako:

> [...] rozszerzenie polityki poprzez działania podejmowane w cyberprzestrzeni przez podmioty państwowe lub niepaństwowe, które stanowią poważne zagrożenie dla bezpieczeństwa narodu, lub są prowadzone w odpowiedzi na działania postrzegane jako zagrożenie dla bezpieczeństwa narodu (Shakarian i in., 2013: 2).

Pomimo różnych prób odpowiedzi, pytanie o definiowanie cyberwojny (a także samej wojny) pozostaje otwarte. Choć wydaje się właściwym stwierdzenie, iż w obecnej rzeczywistości cyberwojną można nazwać pojedyncze działania wykorzystujące sferę cyberprzestrzeni do przeprowadzenia ataku, który prowadzi do destabilizacji życia konkretnej społeczności, uszczerbku na zdrowiu, a nawet śmierci. Biorąc pod uwagę ten ostatni aspekt (śmierć) – w praktyce nie istnieje żaden przykład, który odpowiadałby tak zarysowanej definicji wojny cybernetycznej. Istnieje jednak coraz większe ryzyko, że zaawansowane cyberataki na infrastrukturę krytyczną – szpitale, sieci energetyczne czy transport – mogą prowadzić do zagrożeń, w których wystąpią ofiary. Oczywiście taka definicja rodzi kolejne pytania, a mianowicie jak oddzielić cyberwojnę od innych negatywnych działań w cyberprzestrzeni (zob. Cendrowski, 2020).

Cyberprzestępstwo, cyberwojna, cyberterroryzm – rozważania i próba podziału

W kontekście prowadzonych rozważań warto zwrócić uwagę na pojęcia związane z działaniami w cyberprzestrzeni, które zagrażają bezpieczeństwu społecznemu. Jednym z takich terminów jest cyberprzestępstwo stanowiące kolejne, niezwykle szerokie zagadnienie. W polskim prawie definicja tego zjawiska nie została jednoznacznie sformułowana. Można natomiast wysnuć uniwersalne twierdzenie, iż cyberprzestępstwo to wszelkie „czyny zabronione, skierowane przeciwko systemom informatycznym, w których komputer jest celem samym w sobie, oraz czyny dokonane z użyciem komputera, w których stanowi on jedynie narzędzie" (Stefanowicz, 2017: 20). Stąd wynika podział na dwa rodzaje przestępstw: te, w których komputer jest jedynie środkiem lub narzędziem ich popełnienia, choć mogłyby one zaistnieć także bez jego użycia, oraz te, w których komputer stanowi niezbędną podstawę, a ich popełnienie jest możliwe wyłącznie z jego wykorzystaniem (Siwicki, 2012: 243).

Do innych działań – oprócz wyżej przedstawianej cyberwojny i cyberprzestępstwa – które destabilizują społeczeństwo, należy cyberterroryzm, którego definiowanie również sprawia problemy. Amerykańska wykładowczyni Dorothy E. Denning zaproponowała następującą definicję: „bezprawny atak lub groźba ataku na komputery, sieci i przechowywane w nich informacje w celu zastraszenia lub wymuszenia na rządzie, lub obywatelach określonego państwa realizacji celów politycznych, lub społecznych" (Denning, 2000). Jak można zauważyć, cyberterroryzm nieznacznie różni się od cyberwojny. Jego głównym celem, podobnie jak terroryzmu konwencjonalnego, jest wywołanie strachu, a tym samym próba wywarcia presji w celu zainicjowania określonego działania. W tym przypadku określone działanie (reakcja) jest pewnego rodzaju zyskiem dla terroryzmu cybernetycznego, który osiągany jest za pomocą strachu. Strach, natomiast, jest jednym z czynników prowadzących do destabilizacji

(zob. Skubisz, 2017:65) – istotnie widać tutaj znaczące podobieństwo do wojny cybernetycznej.

Każda zaplanowana destabilizacja, która polega na stworzeniu określonej sytuacji i umożliwia dalsze działania lub wywołuje konkretną reakcję, jest dążeniem do osiągnięcia celu. Choć wydaje się, w świetle przedstawionych argumentów i definicji, że rozumienie cyberwojny powinno być ograniczone do narzędzia wykorzystywanego podczas konwencjonalnej wojny, to istnieją również przypadki, które odbiegają od tej reguły. Jeśli cyberwojna jest „rozszerzeniem polityki poprzez działania podejmowane w cyberprzestrzeni" (Shakarian i in., 2013: 2), to można ogólnie stwierdzić, że w obecnej rzeczywistości jej głównym celem jest dążenie do destabilizacji określonej grupy społecznej. Cyberprzestępstwa również mogą zmierzać do takiego celu, jednak różnica tkwi w skali ataku – zakłócenie pracy elektrowni i pozbawienie tysięcy ludzi dostępu do energii elektrycznej powinno być rozpatrywane inaczej niż atak ransomware[1] na określoną spółkę – i fakcie, iż cyberprzestępstwa są najczęściej ukierunkowane na pewien zysk (pozyskanie czegoś np. danych, pieniędzy, dostępu itd.) Nie oznacza to jednak, że oba pojęcia nie są ze sobą związane.

Zmasowany atak cybernetyczny na Estonię (2007)

27 kwietnia 2007 roku rozpoczęła się seria ataków cybernetycznych wymierzonych w estońskie społeczeństwo, których źródło przypisuje się Federacji Rosyjskiej (Warchoł, 2023: 312). Incydent ten był bezpośrednio związany z dążeniami rządu Estonii do usunięcia tzw. posągu Brązowego Żołnierza z centrum Tallina. Pomnik ten był dla Estończyków symbolem radzieckiej okupacji, dla strony rosyjskiej stanowił on jednak wyraz uznania dla poległych żołnierzy radzieckich, a także symbol zwycięstwa nad nazizmem (Lakomy, 2015: 188).

Początkowa fala ataków miała charakter raczej chaotyczny i dotyczyła w większości oficjalnych witryn rządowych, które zakłócano za pomocą prostych ataków DDoS[2]. Jednak już pod koniec kwietnia incydenty stały się bardziej zaawansowane – zaczęto wykorzystywać rozbudowane sieci botnet[3]. 3 i 4 maja oraz w kulminacyjnym okresie w nocy 9 maja (rocznica zwycięstwa Związku Radzieckiego nad nazistami), atakujący skupili się nie tylko na instytucjach państwowych, ale również na sektorze finansowym. Największy estoński bank Hansabank został pozbawiony dostępu do kluczowych usług, co wpłynęło na funkcjonowanie całego systemu płatności i bankowości w kraju. 15 maja do ataku na estońskie instytucje wykorzystano sieć botnet składającą się z około 85 tys. komputerów (Lakomy, 2015: 191–192).

Wydarzenia te określane są w dyskursie jako „pierwsza cyberwojna" (Lakomy, 2015: 184; Landler i Markoff, 2007), jednak jak wskazuje Miron Lakomy, sytuacja ta pozostaje niejednoznaczna, a zdania ekspertów

[1] Ransomware (ang. *ransom* – okup, *software* – oprogramowanie) – „oprogramowanie, które blokuje dostęp do zaatakowanego systemu komputerowego i uniemożliwia odczyt zapisanych w nim danych, często przez ich zaszyfrowanie, a następnie żąda od ofiary okupu za przywrócenie stanu pierwotnego" (Nowakowski, 2021:80).

[2] DDoS (ang. *Distributed Denial of Service*) – atak ukierunkowany na zajęcie wszystkich wolnych zasobów docelowego systemu poprzez skoordynowane i jednoczesne generowanie ruchu z wielu, przejętych przez atakujących, komputerów, czyli tzw. botnetu. (Gu i Liu, 2012).

[3] Botnet (ang. *bot od robot* – automat, *net* – sieć) – „potoczna nazwa sieci komputerów-zombie, czyli komputerów pozostających pod kontrolą hakerów z wykorzystaniem wirusów, koni trojańskich itp." (Pączkowski, 2017).

są podzielone. Incydent ten jest postrzegany między innymi jako hybrydowa forma zagrożenia cybernetycznego, łącząca zarówno elementy spontanicznej mobilizacji, jak i zorganizowanej, państwowej operacji mającej na celu wymuszenie zmian w polityce innego państwa (Lakomy, 2015: 197–200). Pomimo tego, iż uznanie ataków na Estonię za cyberwojnę stanowiłoby pewnego rodzaju „nadużycie" (Lakomy, 2015: 200), sytuacja ta potencjalnie pokazała, że istnieje możliwość prowadzenia autonomicznej cyberwojny.

Cyberatak na ukraińską elektrownię (2015)

23 grudnia 2015 roku doszło do poważnego ataku cybernetycznego na infrastrukturę energetyczną w obwodzie iwano-frankiwskim w zachodniej części Ukrainy. Różne źródła podają odmienne dane, lecz liczba mieszkańców, którzy zostali pozbawieni dostępu do energii elektrycznej, oscyluje wokół 200 tysięcy (Zetter, 2016; Park i Walstrom, 2017), a skutki ataku trwały od czterech do sześciu godzin (Gapiński, 2016).

Ataku dokonano za pomocą złośliwego oprogramowania (malware) – BlackEnergy – które powstało już w 2007 roku i na przestrzeni lat wyewoluowało z narzędzia do przeprowadzania ataków DDoS oraz tworzenia botnetów do skomplikowanego oprogramowania umożliwiającego różnorakie działania, takie jak szpiegostwo, zdalne sterowanie zainfekowaną maszyną, czy pozyskiwanie specyficznych danych (zob. Shrivastava, 2016). Źródła podają, iż wirus BlackEnergy miał dostać się do systemów na kilka miesięcy przed atakiem (Bock i in., 2019; Park i Walstrom, 2017). Dzięki metodzie spear-phising[4] hakerzy skłonili ofiary do pobrania załącznika w postaci pliku Microsoft Office (a konkretniej pliku z rozszerzeniem PPSX odpowiadającego prezentacji multimedialnej w programie PowerPoint (Lipovsky, 2014)) zawierającego trojana[5], który po aktywacji rozpoczynał instalowanie kolejnych niebezpiecznych programów (Gapiński, 2016).

Zgodnie z opisem sytuacji cały atak trwał kilka minut, a pracownik, który stracił kontrolę nad systemem, mógł tylko patrzeć, jak kursor porusza się po interfejsie i wyłącza kolejne komponenty. Podczas próby odzyskania kontroli okazało się, iż operator został wylogowany, a hasło uległo zmianie. Wykorzystano także oprogramowanie KillDisk[6], które posłużyło do wyczyszczenia nośników danych, a tym samym uniemożliwiło ponowne uruchomienie systemu. Dodatkowo poprzez atak TDoS[7] wyłączone zostało biuro obsługi telefonicznej, aby osoby pozbawione elektryczności nie mogły zgłaszać problemów z infrastrukturą energetyczną ani uzyskać bezpośredniej informacji (De Tomas Colatin, 2018; Bock i in., 2019).

Władze Ukrainy stwierdziły, iż źródłem cyberataku jest Federacja Rosyjska (Zetter, 2016; De Tomas Colatin, 2018). Taki scenariusz przyjęły również Stany Zjednoczone,

[4] Spear phishing (ang. *spear* – harpun) – ukierunkowany, przeprowadzany najczęściej za pośrednictwem poczty elektronicznej atak, który ma na celu skłonienie ofiary do wykonania określonej czynności poprzez zawarcie spersonalizowanych i osobisty informacji, które bezpośrednio dotyczą ofiary (Europol EC3, 2019).

[5] Trojan – złośliwe oprogramowanie ukryte w pozornie legalnym programie, które „[…] zawiera ukryty kod umożliwiający hakerowi przejęcie kontroli nad zainfekowanym komputerem […]" (Pączkowski, 2017).

[6] KillDisk – złośliwe oprogramowanie z funkcjami wymazywania dysku, takimi jak uszkadzanie sektorów rozruchowych i nadpisywanie oraz usuwanie plików systemowych, po szkodliwych działaniach na dysku ponownie uruchamia komputer w celu uczynienia go bezużytecznym (MITRE ATT&CK, 2021).

[7] TDoS (ang. Telephony Denial of Service) – atak polegający na zablokowaniu linii telefonicznej przez przeciążenie jej setkami jednoczesnych połączeń, uniemożliwiający odbieranie połączeń przychodzących i/lub wykonywanie połączeń wychodzących (FBI, 2021).

które wszczęły własne śledztwo w tej sprawie (Cybersecurity and Infrastructure Security Agency, 2021; Gapiński, 2016). Atak przypisywany jest grupie Sandworm (G.U. 74455), która podlega Głównemu Zarządowi Wywiadowczemu Federacji Rosyjskiej (GRU). Informacje te nie są jednak w pełni potwierdzone, bowiem podobnie jak w każdym „profesjonalnie" przeprowadzonym (Zetter, 2016) cyberataku, ustalenie konkretnego sprawcy jest bardzo trudne, jeśli nie niemożliwe.

Przyjmując, że za cyberatakiem faktycznie stoi Federacja Rosyjska, biorąc pod uwagę czas ataku, możemy jasno stwierdzić, że miał on na celu destabilizację społeczeństwa. Należy również zauważyć fakt, iż cyberatak ten stwarzał potencjalne zagrożenie dla zdrowia (i życia) mieszkańców dotkniętych przerwą w dostawie prądu – atak został przeprowadzony w grudniu, kiedy temperatury są stosunkowo niskie (Zetter, 2016). Niektórzy „uważają, że atak miał na celu obserwację zachowania ukraińskich władz oraz wypróbowania własnego potencjału" (Kost, 2017). Atak ten można nazwać aktem cyberwojny, który stanowił element prowadzonej na terytorium Ukrainy wojny hybrydowej rozpoczętej wraz z aneksją Krymu w 2014 roku (Ochmann i Wojas, 2015: 87–88).

Cyberatak na sieć satelitarną KA-SAT (2022)

Wraz z otwartym atakiem Rosji na Ukrainę 24 lutego 2022 doszło do zakłócenia sieci Internetu satelitarnego KA-SAT, której operatorem jest amerykańska firma telekomunikacyjna Visat. Atak nie dotyczył bezpośrednio satelity, lecz infrastruktury naziemnej w postaci modemów i routerów (Kerttunen i in., 2023: 6). Hakerzy wykorzystali błędną konfigurację aplikacji VPN[8], zyskując dostęp do zaufanego segmentu zarządzania i korzystając ze złośliwego oprogramowania (malware) AcidRain (zob. Guerrero-Saade, 2022), nadpisali pamięć flash[9] modemów, przez co te nie były w stanie połączyć się z siecią (Visat, 2022; Kerttunen i in., 2023: 6–7; Guerrero-Saade, 2022). Cyberatak początkowo dotyczył jedynie Ukrainy, jednak z czasem obszar zakłóceń zwiększył się i wpłynął także na infrastrukturę innych państw objętych zasięgiem sieci KA-SAT. Poza Ukrainą atak spowodował zakłócenie komunikacji niemieckich turbin wiatrowych z systemami zdalnej konserwacji (Palczewski, 2023; Kerttunen i in., 2023: 2).

Analiza kodu (Guerrero-Saade, 2022) AcidRain wykazała znaczne podobieństwo do oprogramowania VPNFilter[10], które zostało wcześniej powiązane z grupą Fancy Bear (APT28) przez FBI oraz Departament Sprawiedliwości USA. Inna analiza przeprowadzona przez NSA[11] oraz CISA[12] wykazała powiązanie oprogramowania z grupą Sandworm (G.U. 74455). Według analityków obie grupy podlegają Federacji Rosyjskiej (Steinbrecher, 2022; Kerttunen i in., 2023: 5). Odpowiedzialność za ten atak cybernetyczny przypisano więc Rosji – nie tylko na podstawie równoległego rozpoczęcia konwencjonalnej wojny, lecz także w oparciu o analizę struktury oprogramowania wykorzystanego

[8] VPN (ang. *Virtual Private Network*) – "wirtualna sieć oparta na istniejących sieciach fizycznych, która umożliwia bezpieczną transmisję danych i informacji IP pomiędzy różnymi sieciami lub w obrębie tej samej sieci" (Baker i in., 2020: 8).

[9] Pamięć flash – rodzaj pamięci "nieulotnej", która zachowuje dane po odłączeniu zasilania. Powszechnie stosowana w smartfonach, modemach i innych urządzeniach elektronicznych.

[10] VPNFilter – złośliwe oprogramowanie (*malware*), które służy do atakowania urządzeń sieciowych takich, jak routery oraz serwery NAS. Jest w stanie potencjalnie uszkodzić zainfekowane urządzenie (Cybersecurity and Infrastructure Security Agency, 2018).

[11] National Security Agency (Agencja Bezpieczeństwa Narodowego).

[12] Cybersecurity and Infrastructure Security Agency (Agencja Cyberbezpieczeństwa i Infrastruktury).

do jego przeprowadzenia. Incydent był szeroko komentowany oraz potępiany przez wiele państw i organizacji międzynarodowych (Kerttunen i in., 2023: 5, 8–9).

Początkowo postrzegano ten atak cybernetyczny jako strategię w zakłóceniu komunikacji wojskowej. Jednak miał on „ograniczony wpływ na komunikację wojska i policji, ponieważ mogły one polegać na analogowych telefonach stacjonarnych […]" (Kerttunen i in., 2023: 3). Nawet jeśli atak nie wpłynął w znaczącym stopniu na struktury militarne, to i tak część ludności cywilnej pozbawiona została dostępu do sieci, co w szczególnych przypadkach mogło znacząco utrudniać komunikację, która stanowiła istotny element w tak kluczowym czasie, jak rozpoczęcie wojny.

Można w zarysie stwierdzić, iż atak ten – podobnie jak omawiany wyżej atak na elektrownię – stanowił akt cyberwojny, którego ogólnym celem była destabilizacja sytuacji w atakowanym kraju i wprowadzenie chaosu. Tutaj jednak był on elementem konwencjonalnej i otwarcie wypowiedzianej wojny.

Podsumowanie

Cyberwojna jest zjawiskiem wielowymiarowym, którego granice są płynne i niekiedy pokrywają się z charakterystyką innych negatywnych działań w cyberprzestrzeni – takich, jak cyberterroryzm czy cyberprzestępczość. Cyberwojna przede wszystkim stanowi element wojny hybrydowej, która łączy różnego rodzaju strategie, jednak istnieje potencjał dla prowadzenia jej w sposób autonomiczny i niepowiązany z innymi strategiami. Może ona wyznaczać także punkt wyjściowy dla konwencjonalnych i otwartych działań wojennych. Związane z nią zagrożenia obejmują nie tylko destabilizację systemów państwowych, lecz stanowią również realne ryzyko dla zdrowia i życia obywateli poprzez zakłócanie pracy kluczowej infrastruktury.

Wobec ciągłego rozwoju i wzrostu liczby ataków na infrastrukturę krytyczną istotne jest zacieśnienie międzynarodowej współpracy oraz zwiększenie świadomości w zakresie cyberbezpieczeństwa na poziomie społeczeństw i instytucji. W przyszłości cyberwojna może stać się elementem konfliktów zbrojnych o znacznie większej skali niż dotychczas, dlatego konieczne jest, by już teraz przygotować społeczeństwo na potencjalne konsekwencje takich działań.

Literatura:

Baker E., Dang Q., Frankel S., Scarfone K., Wouters P., 2020, *Guide to IPsec VPNs*, Gaithersburg, National Institute of Standards and Technology.

Cendrowski W., 2017, *Cyberwojna i jej znaczenie dla bezpieczeństwa NATO w kontekście przypadków i dokumentów strategicznych*, [w:] H. Batorowska (red.), *Walka informacyjna. Uwarunkowania. Incydenty. Wyzwania*, Kraków, Uniwersytet Pedagogiczny w Krakowie, s. 128–141.

Clausewitz C. von, 2022, *O wojnie*, A. Cichowicz, L.W. Koc (przeł.), Warszawa, Bellona.

Europol EC3, 2019, *Spear Phishing. A Law Enforcement and Cross-Industry Perspective*, Haga, European Union Agency for Law Enforcement Cooperation.

Gu Q., Liu P., 2012, *Denial of Service Attacks*, [w:] H. Bidgoli (red.), *Handbook of computer networks*, t. 3, Hoboken, John Wiley & Sons, s. 454–468.

Huyghe F.-B., 2011, *Cyberwar and its borders*, [w:] D. Ventre (red.), *Cyberwar and information warfare*, Londyn, ISTE, s. 1–30.

Lakomy M., 2015, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice, Wydawnictwo UŚ.

Nowakowski W., 2021, Ransomware, *Człowiek i dokumenty*, 63, s. 80–84.

Ochmann P., Wojas J., 2015, Współczesne znaczenie aktu wypowiedzenia wojny –

uwagi w kontekście konfliktu na wschodzie Ukrainy, *Bezpieczeństwo. Teoria i Praktyka*, 3, s. 81–92.

Pączkowski T., 2017, *Słownik cyberbezpieczeństwa*, Katowice, Szkoła Policji w Katowicach.

Rid T., 2013, *Cyber war will not take place*, Oxford, Oxford University Press.

Schmitt M.N. (red.), 2013, *Tallin manual on the international law applicable to cyber warfare*, Cambridge, Cambridge University Press.

Schmitt M.N. (red.), 2017, *Tallinn manual 2.0 on the international law applicable to cyber operations*, Cambridge, Cambridge University Press.

Shakarian P., Shakarian J., Ruef A., 2013, *Introduction to cyber-warfare. A multidisciplinary approach*, Waltham, Syngress.

Siwicki M., 2012, Podział i definicja cyberprzestępstw, *Prokuratura i Prawo*, 7–8, s. 241–252.

Skubisz J., 2017, Istota bezpieczeństwa, *Zarządzanie Innowacyjne w Gospodarce i Biznesie*, 2, s. 61–77.

Stefanowicz M., 2017, Cyberprzestępczość. Próba diagnozy zjawiska, *Kwartalnik Policyjny*, 4, s. 19–23.

Tzu S., Pin S., 2014, *Sztuka wojny*, wyd. 3, B. Oczko (red.), D. Bakalarz (przeł.), Gliwice, Helion.

Warchoł A., 2023, Od ofiary do światowego lidera. Estonia po cyberatakach z 2007 roku, *Politeja*, 20 (5), s. 307–327.

Winterfeld S., Andress J., 2013, *The Basics of Cyber Warfare. Understanding the Fundamentals of Cyber Warfare in Theory and Practice*, Waltham, Elsevier.

Źródła internetowe:

Bock P., Hauet J.-P., Françoise R., Foley R., 2019, *Lessons learned from a forensic analysis of the Ukrainian power grid cyberattack* [online], https://blog.isa.org/lessons-learned-forensic-analysis-ukrainian-power-grid-cyberattack-malware [dostęp: 03.11.2024 r.].

Cendrowski W., 2020, *Cyberwojna*, [w:] *Vademecum Bezpieczeństwa Informacyjnego* [online], https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/09/cyberwojna/ [dostęp: 27.10.2024].

Cybersecurity and Infrastructure Security Agency, 2018, *VPNFilter destructive malware* [online], https://www.cisa.gov/news-events/alerts/2018/05/23/vpnfilter-destructive-malware [dostęp: 04.11.2024 r.].

Cybersecurity and Infrastructure Security Agency, 2021, *Cyber-attack against Ukrainian critical infrastructure* [online], https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 [dostęp: 03.11.2024 r.].

De Tomas Colatin S., 2018, *Power grid cyberattack in Ukraine (2015)* [online], https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015) [dostęp: 03.11.2024 r.].

Denning D.E., 2000, *Cyberterrorism. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives* [online], https://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm [dostęp: 02.11.2024 r.].

DICE, 2021, *Battlefield 2042*, EA Games.

FBI, 2021, *Telephony Denial of Service Attacks Can Disrupt Emergency Call Center Operations* [online], https://www.ic3.gov/PSA/2021/PSA210217 [dostęp: 29.11.2024].

Gapiński K., 2016, *Blackout w zachodniej Ukrainie. Cyber atak o wymiarze międzynarodowym* [online], https://pulaski.pl/komentarz-blackout-w-zachodniej-ukrainie-cyber-atak-o-wymiarze-miedzynarodowym/ [dostęp: 03.11.2024 r.].

Guerrero-Saade J.A., 2022, *AcidRain. A modem wiper rains down on Europe* [online],

https://www.sentinelone.com/labs/acid-rain-a-modem-wiper-rains-down-on-europe/ [dostęp: 04.11.2024 r.].

Kerttunen M., Schuck K., Hemmelskamp J., 2023, *Major Cyber Incident: KA-SAT 9A* [online], https://eurepoc.eu/wp-content/uploads/2023/12/Viasat-PL-Final.pdf [dostęp: 04.11.2024 r.].

Kost P., 2017, *Nowy etap wojny na Ukrainie. Rosja celuje w infrastrukturę krytyczną* [online], https://energetyka24.com/nowy-etap-wojny-na-ukrainie-rosja-celuje-w-infrastrukture-krytyczna [dostęp: 03.11.2024 r.].

Landler M., Markoff J., 2007, *In Estonia, what may be the first war in cyberspace* [online], https://www.nytimes.com/2007/05/28/business/worldbusiness/28iht-cyberwar.4.5901141.html [dostęp: 17.02.2025].

Lipovsky R., 2014, *CVE-2014-4114. Details on August BlackEnergy PowerPoint campaigns* [online], welivesecurity.com/2014/10/14/cve-2014-4114-details-august-blackenergy-powerpoint-campaigns/ [dostęp: 03.11.2024 r.].

MITRE ATT&CK, 2021, *KillDisk* [online], https://attack.mitre.org/software/S0607/ [dostęp: 29.11.2024].

Palczewski S., 2023, *Rosyjska inwazja na Ukrainę. Jak wygląda walka w sieci?* [online], https://demagog.org.pl/analizy_i_raporty/rosyjska-inwazja-na-ukraine-jak-wyglada-walka-w-sieci/?cn-reloaded=1 [dostęp: 04.11.2024 r.].

Park D., Walstrom M., 2017, *Cyberattack on critical infrastructure. Russia and the Ukrainian power grid attacks* [online], https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/ [dostęp: 03.11.2024 r.].

Shrivastava S., 2016, *Analysis Report. BlackEnergy. Malware for Cyber-Physical Attacks* [online], https://itrust.sutd.edu.sg/research/reports/ [dostęp: 03.11.2024 r.].

Steinbrecher D., 2022, *Viasat KA-SAT attack (2022)* [online], https://cyberlaw.ccdcoe.org/wiki/Viasat_KA-SAT_attack_(2022) [dostęp: 04.11.2024 r.].

Visat, 2022, *KA-SAT Network cyber attack overview* [online], https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview [dostęp: 04.11.2024 r.].

Wachowski L., Wachowski L. (reż.), 1999, *Matrix*, USA.

Zetter K., 2016, *Inside the cunning, unprecedented hack of Ukraine's power grid* [online], https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ [dostęp: 03.11.2024 r.].

Akty prawne

Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz. U. z 2002 r. Nr 156, poz. 1301).

Notka o autorze: Student III roku studiów pierwszego stopnia na kierunku Kulturoznawstwo na Wydziale Filologicznym Uniwersytetu Gdańskiego. Członek studenckiego koła naukowego Mozaika. Interesuje się antropologią przemocy, zjawiskami związanymi z wojną i terroryzmem, komunikacją polityczną, kulturą Bliskiego Wschodu, Skandynawii oraz krajów postjugosłowiańskich, a także literaturą i muzealnictwem.