Cyberataki typu DDoS z perspektywy teorii władztwa nad czynem zabronionym w międzynarodowym prawie karnym: nowe wyzwanie, utrwalone rozwiązania?

Przedmiotem niniejszych badań są **zachowania polegające na kierowaniu lub przeprowadzaniu cyberataków typu distributed denial-of-service (dalej: „DDoS”).** Cyberataki typu DDoS należą do najbardziej rozpowszechnionych form złośliwych operacji w sieci; zasadniczo można je zdefiniować jako kolektywną i zarazem skoordynowaną serię działań, mającą na celu przesyłanie wielu żądań komunikacyjnych do docelowego systemu bądź systemów komputerowych. Co istotne z perspektywy rozważań materialnoprawnych przewidywanych w drugiej i trzeciej części projektu badawczego, cyberataki typu DDoS wyróżniają się tym, że są realizowane w układzie wieloosobowym. Sprawowanie kontroli (władztwa) nad tzw. **botnetem** – zorganizowaną siecią, zrzeszającą wielu nieświadomych użytkowników – stanowi kluczowy element omawianych zachowań, który umożliwia skuteczną realizację cyberataku.

Zawężenie obszaru badawczego do cyberataków typu DDoS można uznać za uzasadnione zarówno ze względu na podejmowane działania prawodawcze, jak i dostępne dane statystyczne. W 2011 roku Europejski Komitet Ekonomiczno-Społeczny w opinii w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady dotyczącej ataków na systemy informatyczne zwrócił szczególną uwagę na cyberataki popełniane z użyciem tzw. botnetu. Jak z kolei wskazano w pkt 5 motywów przyjętej dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne, istnieją dowody wskazujące na tendencję do coraz bardziej niebezpiecznych ataków na wielką skalę, a tendencja ta występuje wraz z opracowywaniem coraz bardziej wyrafinowanych metod, takich jak tworzenie i wykorzystywanie tzw. botnetów.

Zauważenia wymaga, że tego typu stanowisko ujęto w motywach dyrektywy przyjętej ponad dekadę temu, przy czym od tego okresu obserwuje się wyraźną, nieprzerwaną rosnącą tendencję w występowaniu cyberataków typu DDoS. Z ostatnich danych statystycznych wynika bowiem, że **w pierwszym kwartale 2025 roku odnotowano 20,5 miliona cyberataków typu DDoS, co stanowi wzrost o 358% w porównaniu z analogicznym okresem roku poprzedniego** (Cloudflare, 2025).

Wydaje się również oczywiste, że wzrost cyberprzestępczości i rozpowszechnienie cyberataków typu DDoS ma wpływ na sposób prowadzenia działań wojennych w XXI wieku. W tym przedmiocie warto przytoczyć stanowisko ujęte w raporcie Organizacji Narodów Zjednoczonych z 2021 roku, w którym stwierdzono, że **zachowania polegające na kierowaniu lub przeprowadzaniu cyberataków, przy których możliwe jest wykazanie relewantnego związku (*nexusu*) z konkretnym konfliktem zbrojnym, mogą wypełniać znamiona czynów zabronionych stypizowanych w art. 8 ust. 2 Rzymskiego Statutu Międzynarodowego Trybunału Karnego** sporządzonego w Rzymie dnia 17 lipca 1998 r. (dalej: „Statut Rzymski”, „Statut”) (The Council of Advisers’ Report Prepared by the Permanent Mission of Liechtenstein to the United Nations, 2021; podobnie Ambos, 2021; Freeman, 2023; Khan, 2023). Zbliżoną interpretację w tym zakresie przedstawiono w najnowszym dokumencie Biura Prokuratora Międzynarodowego Trybunału Karnego z 6 marca 2025 roku (Draft Policy on Cyber-Enabled Crimes Under the Rome Statute of 6 March 2025).

Doprecyzowując zatem niniejszy obszar badawczy, należy podkreślić, że głównym przedmiotem badań nie są wszystkie cyberataki DDoS, lecz **takie, które są popełniane w układzie wieloosobowym, potencjalnie skutkujące obrażeniami lub śmiercią osób, uszkodzeniem bądź zniszczeniem obiektów, lub też powodujące poważne zakłócenia w funkcjonowaniu infrastruktury krytycznej, stosowane w ramach międzynarodowych i wewnętrznych konfliktów zbrojnych.**

Znaczenia projektu należy poszukiwać przede wszystkim w tym, że realizacja przewidywanych zadań badawczych zmierza do spełnienia dwóch tradycyjnych funkcji prawa karnego: **funkcji prewencyjnej oraz funkcji retrybutywnej.** Pierwsza z nich zwraca się ku przyszłości, uzasadniając podjęte badania tym, że doprecyzowanie podstaw odpowiedzialności karnej za współuczestnictwo w kierowaniu lub przeprowadzaniu cyberataków typu DDoS ma oddziaływać prewencyjnie zarówno na potencjalnych sprawców cyberataków, jak i na społeczność międzynarodową w ogóle. Druga zaś, równie istotna, wskazuje na konieczność położenia kresu bezkarności przy uwzględnieniu, uzasadnionych zresztą, oczekiwań ofiar zbrodni. Założenia leżące u podstaw obu tych funkcji wzmacniają zatem tezę o pilnej potrzebie **opracowania precyzyjnych podstaw odpowiedzialności karnej za współuczestnictwo w kierowaniu lub przeprowadzaniu cyberataków typu DDoS w ramach międzynarodowych i wewnętrznych konfliktów zbrojnych (cel badawczy projektu).**