Ivana Kudláčková, *Kybernetická zbraň: Přístupy k její definici* (Broń cybernetyczna. Próba definicji), „Revue pro právo a technologie" 2020, č. 21, s. 47–71, DOI: 10.5817/RPT2020-1-3

Ivana Kudláčková z Uniwersytetu Masaryka w Brnie zebrała informacje z baz danych: DBLP Computer Science Bibliography, Scopus i Web of Science z lat 2010–2019, sprawdzając, jaką treść nadaje się w nauce pojęciu broni cybernetycznej. Za punkt wyjścia przyjęła rok 2010, gdy wykryty został tzw. robak komputerowy „Stuxnet". Był to pierwszy znany program komputerowy służący szpiegowaniu i sabotowaniu instalacji przemysłowych. Został on zaprojektowany przez wywiady amerykański i izraelski i doprowadził do uszkodzenia wirówek wzbogacających uran w irańskim ośrodku badań nuklearnych w mieście Natanz. Zastosowanie „Stuxnetu" jest uważane za przełomowy moment w dziejach rozwoju technologii informacyjnej. Po raz pierwszy oprogramowaniem zniszczono przedmioty materialne o charakterze militarnym, w tym przypadku – urządzenia służące wytworzeniu broni jądrowej, innymi słowy, wyrządzono szkodę materialną w świecie fizycznym. Przyjęty przez autorkę zakres czasowy jest więc zasadny.

Kudláčková stwierdziła, że wraz ze „Stuxnetem" pojawiła się broń cybernetyczna, która nie miała definicji w prawie. Za cel badań postawiła zatem nie sformułowanie takiego pojęcia, lecz zestawienie definicji występujących w literaturze naukowej. W bazach danych znalazła tylko 124 bezpośrednie odniesienia do broni cybernetycznej, co na liczbę publikacji naukowych na świecie oraz objętość baz wydaje się bardzo niskim wynikiem. Odrzuciła teksty branżowe, monografie i rozdziały, skupiając się na artykułach naukowych oraz materiałach konferencyjnych. Ograniczona była – jak sama przyznała – dostępnością periodyków, ponieważ nie do wszystkich jej macierzysta uczelnia opłaciła licencjonowany dostęp. Szukała jednak takich tekstów, w których głównym tematem była cyberbroń (*cyberweapon*), co pozwoliło jej na zawężenie pola poszukiwań. Finalnie wytypowała 34 publikacje.

We wprowadzeniu omówiła wybrane przykłady ataków cybernetycznych, w tym dokonany na Estonię w roku 2007. Główną część jej rozważań zajęła analiza językowa. Zwróciła uwagę m.in. na, zasygnalizowaną w opracowaniach naukowych, trudność odróżnienia „złośliwego" oprogramowania od cyberbroni. Nie były dla niej zadowalające odwołania do prawa międzynarodowego publicznego, jeśli chodzi o prawo konfliktów zbrojnych. Poszukiwała więc korelacji w prezentowanych definicjach, zestawiając znane i uznane za cyberbroń programy w formie tabeli. Za wspólny mianownik uznała w szczególności: zagrożenie życia lub zdrowia, wyrządzenie szkód, atak na wrogą infrastrukturę krytyczną, instalacje wojskowe i, ogólnie rzecz biorąc, zdolność do wyrządzenia szkód. Interesująca jest analiza desygnatów podawanych przez przedstawicieli różnych dyscyplin: filozofów, matematyków, techników, politologów, prawników, sekuritologów. Wspólnym czynnikiem okazało się definiowanie broni cybernetycznej jako kodu komputerowego.

Artykuł pozostawia niedosyt, ponieważ zamiast wniosków czytelnik otrzymuje powielenie wstępu (omówienie celu badań, streszczenie sekcji itd.), a autorka – co wprawdzie na początku swojej pracy zaznaczyła – zrezygnowała z próby sformułowania własnej definicji cyberbroni. Ze względu jednak na metodyczną poprawność badań nie powinna była tego unikać. Próba przedstawienia takiej definicji, wraz

z propozycją wpisania jej do aktualnego prawodawstwa, spowodowałaby, że jej artykuł miałby szansę stać się istotnym przyczynkiem do dyskusji nad prawną regulacją problematyki bezpieczeństwa; bez tego elementu pozostał wyłącznie tekstem o charakterze przeglądowym.

*Karol Dąbrowski**
DOI: 10.14746/spp.2021.2.34.10

* Karol Dąbrowski, dr, Uniwersytet Marii Curie-Skłodowskiej w Lublinie, e-mail: karol.dabrowski@umcs.pl, https://orcid.org/0000-0002-4513-3873.