Stanowisko Rzeczypospolitej Polskiej
dotyczące zastosowania prawa międzynarodowego w cyberprzestrzeni

I. Wprowadzenie

Zmiany wynikające z dynamicznego rozwoju technologii cyfrowych, w tym wdrażania i rozwijania cyfrowej administracji publicznej, czy coraz powszechniejszego elektronicznego zarządzania infrastrukturą krytyczną powodują rosnące uzależnienie państw od cyberprzestrzeni[1]. Z jednej strony niesie to za sobą nowe możliwości, z drugiej zaś wiąże się z wyzwaniami dla bezpieczeństwa oraz suwerenności państwa.

Ostatnie lata przyniosły szereg działań w cyberprzestrzeni, realizowanych zarówno przez podmioty państwowe, jak i niepaństwowe, które były wymierzone w stabilność i bezpieczeństwo innych państw, stanowiąc wyzwanie dla oceny ich legalności z perspektywy mających ogólne zastosowanie norm praw międzynarodowego. W tym zakresie wymienić można wykorzystanie działań w cyberprzestrzeni w ramach fenomenu nazywanego popularnie wojną hybrydową, ingerencję w demokratyczne wybory, czy działalność grup terrorystycznych.

Cyberprzestrzeń ze względu na swój, do pewnego stopnia, „aterytorialny" charakter, szybkość z jaką można wykonywać w niej działania oraz relatywną anonimowość jaką cieszą się jej użytkownicy, stanowi wyzwanie dla prawa międzynarodowego. Jej specyfika wymaga bowiem wyjaśnienia, a niekiedy również doprecyzowania w jaki sposób normy prawa międzynarodowego mogą być stosowane w kontekście działań w cyberprzestrzeni.

Poprzez niniejsze stanowisko RP pragnie dołączyć do grupy państw, które sformułowały już swoje poglądy w tym zakresie. W ocenie Polski praktyka publicznego prezentowania stanowisk w kluczowych sprawach z zakresu prawa międzynarodowego zwiększa poziom pewności prawa i transparentności, przyczyniając się zarazem do wzmocnienia poszanowania dla zobowiązań prawnomiędzynarodowych, a także daje możliwość dla rozwoju prawa zwyczajowego.

Polska popiera również dyskusję dotyczącą sposobu zastosowania prawa międzynarodowego do cyberprzestrzeni realizowaną na forum ONZ w obszarze informacji i telekomunikacji w kontekście międzynarodowego bezpieczeństwa od 2013 r. w ramach Grupy Ekspertów Rządowych, a od 2021 r. również w ramach Otwartej Grupy Roboczej. Jak wskazano w stanowisku Polski zaprezentowanym na forum ONZ w 2016 r. „Poszanowanie dla prawa międzynarodowego i norm jest niezbędnym warunkiem dla utrzymania międzynarodowego pokoju i bezpieczeństwa między państwami w cyberprzestrzeni"[2].

[1] Zgodnie z prawem polskim cyberprzestrzeń to 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 2019 r. poz. 700, 730, 848 i 1590) wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami – zgodnie z art. 2 ust. 1b ustawy 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 2017 r. poz. 1932).

[2] Report of the Secretary General: Developments in the field of information and telecommunications in the context of international security, 19 July 2016, A/71/172.

Przestrzeganie fundamentalnych norm prawa międzynarodowego jest z kolei kluczowe dla zapobiegania konfliktom międzynarodowym i ich eskalacji. Powyższe dotyczy również działań w cyberprzestrzeni. Przedstawiane stanowisko jest zatem naturalną kontynuacją dwuletniego niestałego członkostwa RP w Radzie Bezpieczeństwa (2018-2019), gdzie kwestia poszanowania dla prawa międzynarodowego była jednym z polskich priorytetów.

Równocześnie należy odnotować, że 31 października 2019 roku weszła w życie uchwała Rady Ministrów przyjmująca *Strategię Cyberbezpieczeństwa Rzeczypospolitej Polskiej* na lata 2019–2024[3]. Jest to dokument określający strategiczne cele rządu polskiego w zakresie cyberbezpieczeństwa tj. podniesienie poziomu odporności na cyberzagrożenia, a także poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym. Zgodnie ze Strategią: „Rzeczpospolita Polska – we współpracy z partnerami prezentującymi podobny punkt widzenia – będzie promować stanowisko, zgodnie z którym obowiązujące prawo międzynarodowe, przede wszystkim Karta Narodów Zjednoczonych, stosuje się do cyberprzestrzeni." Strategia jako jeden z celów szczegółowych uznaje zbudowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa. Niniejsze stanowisko wpisuje się w realizację tego celu.

Należy również zauważyć, że do problematyki cyberbezpieczeństwa zastosowanie znajdują konkluzje Rady Unii Europejskiej *w sprawie strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę* z 9 marca 2021 r. Wcześniej zagadnienie to było przedmiotem wspólnego komunikatu Komisja oraz Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa do Parlamentu Europejskiego i Rady „*Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę*" z 16 grudnia 2020 r.

II. **Zastosowanie prawa międzynarodowego do działań w cyberprzestrzeni**

1. Istniejące prawo międzynarodowe, w tym Karta Narodów Zjednoczonych, stosuje się do cyberprzestrzeni. Tym samym państwa są zobowiązane do przestrzegania prawa międzynarodowego w cyberprzestrzeni.

Brak uniwersalnych traktatów[4] wprost odnoszących się do działalności państw i innych podmiotów w cyberprzestrzeni nie oznacza, że jest to przestrzeń pozaprawna lub nieuregulowana. Normy prawa międzynarodowego, zarówno te wynikające z traktatów, jak i innych źródeł prawa, w szczególności międzynarodowego prawa zwyczajowego, znajdują w tym zakresie zastosowanie. Stanowisko, zgodnie z którym istniejące normy prawa międzynarodowego stosują się do cyberprzestrzeni, wyraziły dotychczas m.in.: Unia

[3] M.P. 2019 poz. 1037, http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WMP20190001037.

[4] Należy jednak odnotować, że Konwencja Rady Europy o cyberprzestępczości z 23.11.2001 r. stopniowo zyskuje rangę traktatu o globalnym charakterze. Aktualnie jej stronami jest 66 państw, z czego 21 spoza Rady Europy.

Europejska[5], Organizacja Traktatu Północnoatlantyckiego[6], Grupa Ekspertów Rządowych działająca przy ONZ (UN GGE)[7] oraz szereg państw.

2. Do cyberprzestrzeni stosuje się zasada suwerenności

Suwerenność państwa jest podstawową zasadą prawa międzynarodowego[8]. Zgodnie z tą zasadą państwa w stosunkach międzynarodowych są niezależne i równe, a ich integralność terytorialna i niepodległość polityczna są nienaruszalne. W konsekwencji, państwa sprawują najwyższą władzę nad własnym terytorium[9].

Z zasadą suwerenności jest ściśle powiązana zasada dotycząca obowiązku nieinterwencji w sprawy należące do wewnętrznej jurysdykcji jakiegokolwiek państwa. Z zasady suwerenności wywodzą się również normy dotyczące jurysdykcji państwa oraz immunitetów - państwa i jego przedstawicieli.

Państwo sprawuje władztwo nad znajdującymi się na swoim terytorium użytkownikami cyberprzestrzeni, infrastrukturą informatyczną oraz nad danymi. Może – z poszanowaniem wiążących je norm prawnomiędzynarodowych – wykonywać czynności władcze wobec tych podmiotów i obiektów. Ma również prawo do ich ochrony. W rezultacie, RP stoi na stanowisku, że naruszenie suwerenności państwa może nastąpić, zarówno w sytuacji ataku na infrastrukturę państwową, jak i prywatną. Fakt, że infrastruktura informatyczna jest na wiele sposobów połączona z międzynarodową siecią nie sprawia, że państwo traci jakiekolwiek ze swoich uprawnień w stosunku do tej infrastruktury.

Jak wskazano wcześniej suwerenność ma również wymiar zewnętrzny. Suwerenność zewnętrzna oznacza, że państwo jest niezależne w stosunkach zewnętrznych i ma swobodną

---

[5] Wspólny Komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego I Komitetu Regionów Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń , Bruksela, dnia 7.2.2013, JOIN(2013) 1 final; Konkluzje Rady w sprawie szkodliwych działań w cyberprzestrzeni, Bruksela, 16 kwietnia 2018 r., 7925/18, w których wskazano m.in. „UE będzie nadal zdecydowanie stać na straży tego, aby istniejące prawo międzynarodowe miało zastosowanie do cyberprzestrzeni, i podkreśla, że poszanowanie prawa międzynarodowego, w szczególności Karty Narodów Zjednoczonych, ma podstawowe znaczenie dla utrzymania pokoju i stabilności. UE podkreśla, że państwom nie wolno używać serwerów proxy do popełniania czynów, które są bezprawne w świetle prawa międzynarodowego, przy stosowaniu ICT i że powinny one dążyć do zapewnienia, aby ich terytorium nie było wykorzystywane przez podmioty niepaństwowe do popełniania takich czynów(…)".

[6] Deklaracja ze Szczytu w Brukseli https://www.nato.int/cps/en/natohq/official_texts_156624.htm#20.

[7] https://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-578.pdf.

[8] Zob. wyrok Międzynarodowego Trybunału Sprawiedliwości w sprawie działalności militarnej i pozamilitarnej Stanów Zjednoczonych w Nikaragui (Nikaragua v. Stany Zjednoczone), ICJ. Rep. 1986, § 263.

[9] „Suwerenność w relacjach między państwami oznacza niepodległość. Niepodległość, odniesiona do części globu, oznacza prawo wykonywania na niej, z wyłączeniem jakiegokolwiek innego państwa, funkcji państwowych", orzeczenie arbitrażowe w sprawie wysp Las Palmas (Stany Zjednoczone v. Holandia 1928); Wyrok Międzynarodowego Trybunału Sprawiedliwości w sprawie cieśniny Korfu (Wielka Brytania v. Albania), ICJ. Rep. 1949 r. s. 19; Zob. „Pomiędzy niepodległymi państwami poszanowanie dla suwerenności terytorialnej jest niezbędnym fundamentem stosunków międzynarodowych", wyrok Międzynarodowego Trybunału Sprawiedliwości w sprawie cieśniny Korfu (Wielka Brytania v. Albania), ICJ. Rep. 1949 r., s. 35.; wyrok Międzynarodowego Trybunału Sprawiedliwości w sprawie działalności militarnej i pozamilitarnej Stanów Zjednoczonych w Nikaragui (Nikaragua v. Stany Zjednoczone), ICJ. Rep. 1986, § 251.

możliwość angażowania się w dowolne działania w cyberprzestrzeni również poza własnym terytorium, z zastrzeżeniem ograniczeń wynikających z prawa międzynarodowego. Konsekwencją suwerenności jest również zdolność państw do zawierania traktatów, w tym dotyczących cyberprzestrzeni.

Z zasady suwerenności wynika obowiązek innych państw do powstrzymania się od działań, które naruszałyby suwerenność, w szczególności obowiązek, aby nie udostępniać świadomie swojego terytorium do czynów naruszających prawa innych państw[9]. Polska uważa, że w sytuacji przeprowadzenia nieprzyjaznej operacji w cyberprzestrzeni powodującej poważne negatywne skutki na terytorium państwa, bez względu na to czy mają one charakter kinetyczny, czy ograniczają się wyłącznie do cyberprzestrzeni, takie działania należy uznać za naruszenie zasady suwerenności. Przykładem naruszenia zasady suwerenności może być zachowanie przypisywalne państwu trzeciemu i polegające na zakłócaniu działalności organów państwa np. uniemożliwienie funkcjonowania sieci, usług bądź systemów teleinformatycznych podmiotów państwowych, czy też kradzież, usunięcie bądź upublicznienie danych należących do tych podmiotów.

Państwa powinny dołożyć należytej staranności, aby infrastruktura informatyczna znajdująca się na ich terytorium nie była wykorzystywana do niedozwolonych działań wymierzonych w państwa trzecie. To samo dotyczy osób przebywających na terytorium tego państwa. Ocena tego, czy państwo dołożyło należytej staranności powinna być uzależniona od jego zaawansowania technologicznego, ekspertyzy/zasobów i wiedzy nt. działań w cyberprzestrzeni zapoczątkowanych na jego terytorium.

Działania w cyberprzestrzeni naruszające zakaz użycia siły i zasadę dotyczącą obowiązku nieinterwencji w sprawy należące do wewnętrznej jurysdykcji jakiegokolwiek państwa będą również naruszały zasadę suwerenności.

3. Działania w cyberprzestrzeni mogą stanowić niezgodną z prawem interwencję w sprawy należące do wewnętrznej jurysdykcji państwa

Interwencja w wewnętrzne lub zewnętrzne sprawy innego państwa należące do jego wewnętrznej jurysdykcji jest działaniem niezgodnym z prawem międzynarodowym[10]. Zasada nieinterwencji jest naturalną konsekwencją obowiązywania zasady suwerenności - w zakresie, w jakim państwo korzysta z wyłącznych suwerennych uprawnień, inne państwa ponoszą obowiązek ich respektowania.

Próg uznania danej operacji w cyberprzestrzeni za naruszenie zasady nieinterwencji jest wyższy, niż uznania jej wyłącznie za naruszenie zasady suwerenności. Niezgodna z prawem międzynarodowym interwencja musi zawierać element przymusu (ang. *coercion*), który ma na celu wpłynięcie na decyzje państwa należące do jego *domaine réservé*, tj. obszaru działalności państwa pozostającego - na mocy zasady suwerenności państwa - w jego wyłącznej kompetencji[11]. Zatem o naruszeniu zasady nieinterwencji możemy mówić, gdy jedno państwo

[10] Do zasady nieinterwencji odnosi się art. 2 ust. 7 Karty Narodów Zjednoczonych (w odniesieniu do relacji ONZ a państwa) oraz Deklaracja zasad prawa międzynarodowego przyjęta rezolucją Zgromadzenia Ogólnego nr 2625 z dnia 24 października 1970. (w odniesieniu do stosunków międzypaństwowych).

[11] Wyrok Międzynarodowego Trybunału Sprawiedliwości w sprawie działalności militarnej i pozamilitarnej Stanów Zjednoczonych w Nikaragui (Nikaragua v. Stany Zjednoczone), ICJ. Rep. 1986, § 205.

przy użyciu elementu przymusu ingeruje w sprawy wewnętrzne lub zewnętrzne należące do wyłącznej kompetencji innego państwa.

Nie istnieje powszechnie akceptowana definicja pojęcia „przymusu", niemniej niebudzącym wątpliwości przykładem niedozwolonej interwencji jest użycie siły.

Cyberoperacja negatywnie wpływająca na funkcjonowanie i bezpieczeństwo systemu politycznego, gospodarczego, wojskowego lub społecznego państwa, i mogąca prowadzić do zachowań, których w innych okolicznościach państwo nie podjęłoby, może zostać uznana za niedozwoloną interwencję. W szczególności naruszeniem prawa międzynarodowego w tym zakresie byłoby działanie w cyberprzestrzeni unicestwiające możliwość składania zeznań podatkowych przez Internet, czy ingerencja w systemy teleinformatyczne uniemożliwiająca rzetelne i terminowe przeprowadzenie wyborów demokratycznych. Takim naruszeniem mogłoby być również unicestwienie możliwości głosowania nad ustawą przez parlament, pracujący w trybie zdalnym, czy też modyfikacja wyników takiego głosowania. Warto również zaznaczyć, że przeprowadzana na szeroką skalę oraz ukierunkowana kampania dezinformacyjna również może być sprzeczna z zasadą nieinterwencji w szczególności, gdy prowadzi do niepokojów społecznych, wymuszających określoną reakcję państwa.

4. Działania w cyberprzestrzeni przy spełnieniu określonych warunków mogą stanowić naruszenie zakazu użycia siły

Zakaz groźby lub użycia siły wynika z art. 2 ust. 4 Karty Narodów Zjednoczonych[12] oraz z międzynarodowego prawa zwyczajowego. Zgodnie z opinią doradczą Międzynarodowego Trybunału Sprawiedliwości ws. legalności groźby lub użycia broni jądrowej[13] uznanie danego działania za użycie siły nie jest uzależnione od zastosowanego środka. Kluczowe znaczenie mają skutki podjętych działań. W konsekwencji nie można wykluczyć, że cyberatak w określonych okolicznościach osiągnie próg użycia siły. Za uznaniem cyberataku za użycie siły przemawia możliwość spowodowania przezeń analogicznych skutków, jakie wywołałby klasyczny atak zbrojny przy użyciu broni konwencjonalnej. Ocena tego, czy dana cyberoperacja osiąga próg użycia siły musi być każdorazowo analizowana przy uwzględnieniu okoliczności podjętych działań zgodnie z wymogami prawa międzynarodowego. Za użycie siły można uznać działania w cyberprzestrzeni prowadzące do: trwałego i znacznego uszkodzenia elektrowni, wyłączenia systemu obrony przeciwrakietowej, czy przejęcie kontroli nad samolotem lub statkiem pasażerskim i spowodowanie wypadku o istotnych skutkach. Nie jest to lista wyczerpująca – każdorazowo kwalifikacja prawna będzie zależała od okoliczności konkretnego ataku.

Cyberatak, który nie osiąga progu niedozwolonego użycia siły, może zostać uznany za zakazaną interwencję lub działanie naruszające zasadę suwerenności.

---

[12] Art. 2 ust. 4 Karty Narodów Zjednoczonych: *„Wszyscy członkowie powinni w swych stosunkach międzynarodowych powstrzymywać się od stosowania groźby lub użycia siły przeciwko nietykalności terytorium albo niepodległości politycznej któregokolwiek państwa, lub wszelkiego innego sposobu, niezgodnego z zasadami Narodów Zjednoczonych."*

[13] Opinia doradcza Międzynarodowego Trybunału Sprawiedliwości w sprawie legalności użycia broni jądrowej, ICJ Rep. 1996, § 39.

5. Cyberatak może zostać zakwalifikowany jako napaść zbrojna. Prawo do samoobrony ma zastosowanie do cyberprzestrzeni

Zgodnie z art. 51. Karty Narodów Zjednoczonych oraz prawem zwyczajowym państwu przysługuje prawo do samoobrony w przypadku zbrojnej napaści. W kontekście cyberprzestrzeni za zbrojną napaść można uznać cyberatak, który skutkuje śmiercią albo okaleczeniem ludzi lub uszkodzeniem albo zniszczeniem mienia znacznej wartości. W takiej sytuacji państwu, zgodnie z prawem międzynarodowym, przysługuje prawo do samoobrony, niemniej powinno ono być realizowane z poszanowaniem zasad wynikających z międzynarodowego prawa zwyczajowego tj. konieczności i proporcjonalności[14].

Samoobrona nie musi być realizowana przy użyciu tego samego środka co napaść zbrojna. W odpowiedzi na cyberatak osiągający próg napaści zbrojnej dopuszczalna jest zatem zarówno odpowiedź wyłącznie w cyberprzestrzeni, jak i przy użyciu tradycyjnie rozumianych sił zbrojnych. Pozbawienie możliwości odpowiedzi kinetycznej na cyberatak tego rodzaju mogłoby czynić prawo do samoobrony iluzorycznym w sytuacji, gdy sprawca napaści zbrojnej jest w niskim stopniu zależny od funkcjonowania cyberprzestrzeni.

Prawo do samoobrony może przysługiwać również, zgodnie z prawem międzynarodowym, w stosunku do cyberataków osiągających próg napaści zbrojnej przeprowadzonych przez podmioty niepaństwowe. Do cyberprzestrzeni stosuje się także prawo do samoobrony zbiorowej. Znajduje to potwierdzenie w deklaracji przyjętej przez przedstawicieli państw uczestniczących w posiedzeniu Rady Północnoatlantyckiej podczas walijskiego szczytu Organizacji Traktatu Północnoatlantyckiego w 2014 roku. Deklaracja stwierdza m.in. że cyberatak może osiągać próg zagrażający dobrobytowi, bezpieczeństwu oraz stabilności narodowej i euroatlantyckiej. Ich wpływ może być równie szkodliwy dla współczesnych społeczeństw, jak konwencjonalny atak. W związku z powyższym potwierdzono, że cyber-obrona jest częścią podstawowego zadania NATO w zakresie obrony zbiorowej[15].

6. Państwo ponosi odpowiedzialność za działania w cyberprzestrzeni naruszające prawo międzynarodowe

Normy międzynarodowego prawa zwyczajowego dotyczące ustalenia odpowiedzialności państwa w znacznym stopniu znajdują odzwierciedlenie w artykułach o odpowiedzialności państw za akty międzynarodowo bezprawne przyjętych w 2001 roku przez Komisję Prawa Międzynarodowego[16] (dalej „artykuły o odpowiedzialności państw").

Dokument ten przypomina, że „Każdy międzynarodowo bezprawny akt państwa powoduje odpowiedzialność międzynarodową tego państwa." (art. 1). Państwo odpowiada zarówno za działania, jak i zaniechania, które można mu przypisać zgodnie z prawem międzynarodowym i które stanowią naruszenie jego międzynarodowego zobowiązania (art. 2). Artykuły 4-11 opisują zasady przypisania odpowiedzialności państwu. Zgodnie z nimi państwo

[14] Opinia doradcza Międzynarodowego Trybunału Sprawiedliwości w sprawie legalności użycia broni jądrowej, ICJ Rep. 1996, § 41.

[15] Deklaracja ze Szczytu NATO w Walii 2014, pkt 72.

[16] Tekst załączony do rezolucji Zgromadzenia Ogólnego ONZ nr 56/83 z 12 grudnia 2001 r.

odpowiada za zachowania m.in. swoich organów; osób lub jednostek, które pomimo że nie są organami, są uprawnione do wykonywania władzy rządowej; a także osób lub grup osób zachowania są podejmowane na podstawie instrukcji i pod kierunkiem lub kontrolą państwa.

Powyższe normy mają zastosowanie również do zachowania państw w cyberprzestrzeni. Państwo może zatem ponosić odpowiedzialność za niezgodne z prawem międzynarodowym działania np. grup hakerskich lub pojedynczych hakerów, o ile wystąpią przesłanki wyrażone w artykułach o odpowiedzialności państw. Należy pamiętać równocześnie, że specyfika cyberprzestrzeni istotnie utrudnia przypisanie zachowań niezgodnych z prawem międzynarodowym państwom, czy innym podmiotom.

7. Międzynarodowe prawo praw człowieka ma zastosowanie do cyberprzestrzeni

Wysoka anonimowość, kontrola przepływu danych, oraz w dużej mierze aterytorialny charakter cyberprzestrzeni stanowią wyzwanie dla ochrony praw człowieka w sieci. Pomimo tego międzynarodowe prawo praw człowieka ma zastosowanie do zachowań w cyberprzestrzeni. Te same prawa, które jednostki posiadają poza Internetem powinny być chronione również w Internecie [17]. Na państwach ciąży obowiązek nienaruszania praw człowieka, jak również ich ochrona w przypadku naruszeń przez aktorów niepaństwowych lub inne państwa. Wskazane wyżej przykłady bezprawnych działań podmiotów zewnętrznych stanowiących naruszenie suwerenności państwa lub akt przemocy mogą jednocześnie skutkować naruszeniem praw człowieka.

Szczególnej ochrony w cyberprzestrzeni wymagają wolność słowa oraz prawo do prywatności. Jak zauważył Europejski Trybunał Praw Człowieka „Internet odgrywa istotną rolę we wzmacnianiu publicznego dostępu do wiadomości oraz umożliwieniu rozpowszechniania informacji powszechnie”[18]. Pozbawienie jednostek dostępu do Internetu lub wybranych witryn może stanowić naruszenie, gdyż, jak podkreślił Trybunał, „możliwość wyrażania opinii w Internecie stanowi bezprecedensowe narzędzie umożliwiające korzystanie z wolności wyrażania opinii” [19]. Równocześnie należy mieć na uwadze, że prawa te mogą podlegać ograniczeniom koniecznym w społeczeństwie demokratycznym, w szczególności z uwagi na interesy bezpieczeństwa publicznego, ochronę porządku publicznego, zdrowia i moralności lub ochronę praw i wolności innych osób.

Ochrona międzynarodowego prawa praw człowieka w odniesieniu do cyberprzestrzeni wymaga działań na rzecz otwartego i bezpiecznego Internetu. Poszanowanie suwerenności w cyberprzestrzeni nie może stanowić usprawiedliwienia dla naruszania międzynarodowego prawa praw człowieka. Skuteczna ochrona praw człowieka wymaga powstrzymania się przez państwo przed nieuzasadnioną ingerencją w prawa i wolności realizowane w Internecie, a w niektórych okolicznościach podejmowania działań pozytywnych celem zagwarantowania skutecznej realizacji i ochrony praw człowieka w Internecie.

[17] Rezolucja Rady Praw Człowieka ONZ “Promowanie, ochrona oraz korzystanie z Internetu” z 29.6.2012 r.
[18] Times Newspapers Ltd p. Zjednoczonemu Królestwu (nr 1 i 2), nr 3002/03 i 23676/03, wyrok Europejskiego Trybunału Praw Człowieka z 10.3.2009 r.
[19] Cengiz i Inni p. Turcji, nr 48226/10 i 14027/11, wyrok Europejskiego Trybunału Praw Człowieka z 1 grudnia 2015r., § 52.

8. Do cyberprzestrzeni stosują się normy międzynarodowego prawa humanitarnego

Normy międzynarodowego prawa humanitarnego (MPH) [20] mają zastosowanie w sytuacji istnienia konfliktu zbrojnego, międzynarodowego lub niemiędzynarodowego. Podstawowe zasady MPH to zasada humanitaryzmu, proporcjonalności, konieczności wojskowej oraz rozróżniania. Wymogi MPH znajdują zastosowanie również do działań prowadzonych w cyberprzestrzeni w trakcie konfliktu zbrojnego. Podejmując działania w cyberprzestrzeni, należy brać pod uwagę zarówno bezpośrednie, jak i pośrednie skutki takich operacji.

9. Retorsje i środki odwetowe jako instrumenty odpowiedzi na szkodliwe działania w cyberprzestrzeni

Zgodnie z prawem międzynarodowym państwo może podjąć środki w odpowiedzi na nieprzyjazne działania w cyberprzestrzeni poniżej progu napaści zbrojnej[21].

Praktyka międzynarodowa wskazuje, że państwa mogą skorzystać z wachlarza środków w celu zapewnienia przestrzegania prawa przez inne podmioty prawa międzynarodowego. W szczególności państwo będące celem ataku, w reakcji na wrogie działania może odpowiedzieć, korzystając z retorsji lub środków odwetowych.

Retorsje stanowią odpowiedź państwa w reakcji na sprzeczne z jego interesami lub wrogie działania innego państwa. Środki podjęte w ramach retorsji mogą stanowić reakcję zarówno na legalne jak i nielegalne działania innego podmiotu prawa międzynarodowego, natomiast same w sobie muszą być zgodne z prawem międzynarodowym.

Środki odwetowe stanowią reakcję państwa, którego prawnomiędzynarodowe uprawnienia zostały naruszone przez inny podmiot. Polegają one na niewykonywaniu przez określony czas międzynarodowych zobowiązań w celu nakłonienia państwa naruszającego prawo międzynarodowe do wypełnienia ciążących na nim zobowiązań oraz powstrzymania go od ponownego naruszenia prawa.

Równocześnie RP stoi na stanowisku, że ewolucja międzynarodowego prawa zwyczajowego w ostatnich dwóch dekadach pozwala uznać możliwość podejmowania przez państwa również środków odwetowych w interesie ogólnym. W szczególności możliwość podejmowania tego rodzaju środków aktualizuje się w odpowiedzi na naruszanie przez państwa norm bezwzględnie obowiązujących, jak np. zakaz agresji.

Stosując wyżej wskazane środki, państwo zobowiązane jest do działania zgodnie z zasadą proporcjonalności. Ponadto, zarówno retorsje jak i środki odwetowe nie mogą powodować naruszenia norm dotyczących podstawowych praw człowieka, zobowiązań z zakresu międzynarodowego prawa humanitarnego oraz norm bezwzględnie obowiązujących.

---

[20] Są one w szczególności wyrażone w czterech Konwencjach genewskich z 1949 r. oraz dwóch Protokołach dodatkowych z 1977 r. oraz w międzynarodowym prawie zwyczajowym.

[21] Przykładem jest decyzja Rady (WPZiB) 2019/797 z dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim, która „ustanawia ramy dla ukierunkowanych środków ograniczających służących zapobieganiu cyberatakom i reagowaniu na cyberataki, które wywołują poważne skutki i stanowią zewnętrzne zagrożenie dla Unii lub jej państw członkowskich" (akapit 7 preambuły).