Cezary Mik

Środki restrykcyjne (sankcje) wobec ataków cyfrowych jako instrument prawny dyplomacji cyfrowej Unii Europejskiej

Restrictive Measures (Sanctions) against Cyber-Attacks as a Legal Instrument of the European Union Cyber Diplomacy

European Union sanctions (restrictive measures) against cyber-attacks as a legal instrument of cyber diplomacy constitute a new legal solution created in 2019. The Union used it for the first time in 2020 against China, Russia, and the DPRK cyber-attacks. These sanctions are adopted basing on the provisions of the EU Treaty (Common Foreign and Security Policy, Art. 29) and Art. 215 of the Treaty on the Functioning of the EU. They are a part of a broader political concept for the Union, established in 2015, known as cyber diplomacy. The author explains, in the context of the general assumptions of the application of restrictive measures by the Union and its attitude to cyberspace, how cyber-attacks are understood as a premise for sanctions, what sanctions are envisaged in the event of cyber-attacks, and what are the rules and procedure for their adoption and implementation. EU regulations concerning restrictive measures in response to cyber-attacks are not an entirely satisfactory legal solution. The author concludes the article with their evaluation.

Cezary Mik

profesor nauk prawnych
Uniwersytet Kardynała Stefana Wyszyńskiego

ORCID – 0000-0002-6758-1909

Słowa kluczowe:
ataki cyfrowe, ataki cyfrowe dyplomacja cyfrowa, dyplomacja cyfrowa środki restrykcyjne, środki restrykcyjne sankcje, sankcje prawo Unii Europejskiej, prawo Unii Europejskiej wspólna polityka zagraniczna i bezpieczeństwo, wspólna polityka zagraniczna i bezpieczeństwa

Key words:
Cyber-attacks, Cyber-attacks cyber diplomacy, cyber diplomacy restrictive measures, restrictive measures sanctions, sanctions European Union law, European Union law common foreign and security policy, common foreign and security policy

https://doi.org/10.36128/priw.vi37.299

1. Wprowadzenie

W 2020 roku Unia Europejska, po raz pierwszy w swojej historii, podjęła decyzje dotyczące nałożenia środków restrykcyjnych (sankcji) w odpowiedzi na doznane ataki cyfrowe spoza Unii[1]. Ramowymi podstawami prawnymi ich zastosowania stały się decyzja Rady (WPZiB) 2019/797 z 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania ataków cyfrowych

1 EU imposes the first ever sanctions against cyber-attacks, Council of the EU, Press release, 30 July 2020; https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/. [dostęp: 3.9.2021].

zagrażających Unii lub jej państwom członkowskim (dalej: decyzja z 2019 r. lub decyzja o środkach restrykcyjnych/sankcjach)[2] oraz powiązane z nią rozporządzenie Rady (UE) 2019/796 z 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania ataków cyfrowych zagrażających Unii lub jej państwom członkowskim (dalej: rozporządzenie z 2019 r. lub rozporządzenie o środkach restrykcyjnych/sankcjach)[3]. Sankcje nałożono na podstawie decyzji Rady (WPZB) 2020/1127 z 30 lipca 2020 r., zmieniająca decyzję 2020/797[4] oraz rozporządzenia wykonawczego Rady (UE) 2020/1125 z 30.7.2020 r. (dalej odpowiednio: decyzja zmieniająca z 2020 r. i rozporządzenie wykonawcze z 2020 r.)[5].

Stosowanie środków restrykcyjnych przez Unię Europejską nie jest niczym nowym ani nadzwyczajnym. Niemniej ich użycie w przypadku ataków cyfrowych stanowi pewną nowość. Tego typu środki restrykcyjne stanowią bowiem obecnie *pars pro toto* tzw. dyplomacji cyfrowej Unii Europejskiej będącej jej odpowiedzią na wyzwania i zagrożenia wynikające z powstania globalnej przestrzeni cyfrowej, a zwłaszcza ze szkodliwej działalności cyfrowej podejmowanej w tej przestrzeni. Mając to na uwadze, warto poświęcić uwagę środkom restrykcyjnym Unii Europejskiej jako odpowiedzi na zewnętrzne ataki cyfrowe podejmowanej w ramach dyplomacji cyfrowej Unii. Kwestią interesującą jest zwłaszcza to, czym są ataki cyfrowe, czy sankcje stosowane wobec nich wykazują specyfikę w stosunku do środków ogólnie stosowanych, a także jaką pozycję posiadają w całokształcie instrumentów dyplomacji cyfrowej Unii.

---

2 Dz. Urz. UE z 17.5.2019 r., L 129I, s. 13.

3 Dz. Urz. UE z 17.5.2019 r., L 129I, s. 1. Zgodnie z art. 18, rozporządzenie stosuje się: a) na terytorium Unii, w tym w granicach jej przestrzeni powietrznej; b) na pokładach statków powietrznych lub wodnych podlegających jurysdykcji państw członkowskich; c) do każdej osoby fizycznej będącej obywatelem państwa członkowskiego i przebywającej na terytorium Unii lub poza nim; d) do każdej osoby prawnej, podmiotu lub organu, na terytorium Unii lub poza nim, zarejestrowanych lub utworzonych na mocy prawa państwa członkowskiego; e) do osób prawnych, podmiotów lub organów w odniesieniu do dowolnej działalności gospodarczej prowadzonej, w całości lub częściowo, na terytorium Unii.

4 Dz. Urz. UE z 30.7.2020 r., L 246, s. 12. Zob. też Sprostowanie do decyzji Rady (WPZiB) 2019/797 z 17.5.2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim, Dz. Urz. UE z 17.7.2020 r., L 230, s. 36.

5 Dz. Urz. UE z 30.7.2020 r., L 246, s. 4.

Uwzględniając te zadania badawcze, rozważania należy rozpocząć od wyjaśnienia pojęcia środków restrykcyjnych, ustalenia traktatowych podstaw prawnych i kompetencji Unii Europejskiej do ich stosowania oraz zasad stosowania środków restrykcyjnych przez Unię. Następnie trzeba przedstawić ogólnie stosunek Unii Europejskiej do działalności w przestrzeni cyfrowej. Będzie to tłem do omówienia miejsca środków restrykcyjnych w zestawie narzędzi dyplomacji cyfrowej Unii oraz analizy pojęcia ataków cyfrowych. Ostatnia część opracowania będzie poświęcona określeniu środków restrykcyjnych stosowanych przez Unię Europejską wobec ataków cyfrowych oraz zasadom, mechanizmowi stosowania i kontroli użycia sankcji wobec ataków cyfrowych.

2. Środki restrykcyjne w prawie i polityce Unii Europejskiej

2.1. Prawne aspekty stosowania środków restrykcyjnych przez Unię Europejską

W toku procesu integracyjnego Wspólnoty Europejskie (od 1970 do 1993 roku wraz z Europejską Współpracą Polityczną), a następnie Unia Europejska zdołały ukształtować obraz organizacji jako aktora, który nie tylko ma zadania i kompetencje w sferze integracji między państwami członkowskimi, ale także w odniesieniu do świata zewnętrznego. Współcześnie Unia stała się, zwłaszcza w sferze pozawojskowej, aktorem globalnym[6]. W wyniku Traktatu z Lizbony zdołano ujednolicić podejście Unii we wszystkich materiach mających aspekty zewnętrzne. Powstała dziedzina integracji określona mianem działania zewnętrznego Unii, scalona wspólnymi zasadami i celami oraz do pewnego stopnia instytucjonalnie (art. 3 ust. 5, art. 21 i 22 Traktatu o Unii Europejskiej, TUE)[7].

6 Zob. np. Anna Antczak, *Role międzynarodowe Unii Europejskiej. Aspekty teoretyczne* (Warszawa: WizjaPress and IT, 2012); *Dyplomacja czy siła? Unia Europejska w stosunkach międzynarodowych*, red. Stanisław Parzymies (Warszawa: Wydawnictwo Naukowe Scholar, 2009).

7 Zob. zwłaszcza Simon Duke, *Consistency, coherence and European Union external action: the path to Lisbon and beyond* oraz Marise Cremona, „Coherence in the European Union foreign relations law", [w:] *European Foreign Policy. Legal and Political Perspectives,* red. Panos Koutrakos (Cheltenham-Northampton: E. Elgar Publ., 2011), 15 i n., 55 i n. Zob. też *Polityka zagraniczna Unii Europejskiej. Prawo i praktyka*, red. Jan Galster, Anna Szczerba-Zawada (Warszawa: Instytut Wydawniczy EuroPrawo, 2016); *Le droit des relations extérieures de l'Union européenne après le Traité de Lisbonne*, red. Anne-Sophie Lamblin-Gourdin, Eric Mondielli (Éditions É. Bruylant, Bruxelles 2013); Piet Eeckhout, *EU External Relations Law* (Oxford: OUP 2011).

W ramach działania zewnętrznego zachowano wszakże znaczącą odrębność w zakresie wspólnej polityki zagranicznej i bezpieczeństwa (WPZB; art. 23 i n.), która wyraża się w istnieniu specyficznych rozwiązań kompetencyjnych (równoległość kompetencji Unii i państw członkowskich, a nie ich transfer na rzecz Unii, własna zasada lojalności – art. 24 ust. 1 i 3 TUE oraz deklaracje nr 13 i 14 włączone do Aktu końcowego Konferencji międzyrządowej z 2007 r. dotyczące WPZB, art. 4 ust. 1 i art. 5 ust. 2 TUE w związku z deklaracją nr 18 dotyczącą rozgraniczenia kompetencji), instytucjonalnych (kluczowe znaczenie organów międzyrządowych – Rady Europejskiej i Rady, ograniczenie roli Parlamentu Europejskiego i Komisji, Wysoki Przedstawiciel ds. Zagranicznych i Polityki Bezpieczeństwa, Komitet Polityczny i Bezpieczeństwa, Europejska Służba Działania Zewnętrznego – art. 26, 27, 38 TUE, organy wspólnej polityki bezpieczeństwa i obrony – art. 45 TUE) oraz prawnych (swoiste instrumenty działania i tryb ich przyjmowania wraz z zakazem uchwalania aktów legislacyjnych – art. 24, 25, 28, 29, 31 TUE, co do zasady wykluczenie kontroli Trybunału Sprawiedliwości – art. 275 Traktatu funkcjonowaniu o Unii Europejskiej, TfUE)[8].

W toku procesu integracyjnego ukształtowały się też różnorodne sposoby odpowiadania Unii na zewnętrzne zagrożenia lub działania o charakterze nieprzyjaznym czy też przynoszące jej, jej państwom członkowskim czy podmiotom do nich przynależnym szkodę. Ponadto, w związku z dążeniem do odgrywania roli aktora globalnego, Unia włączyła się w szersze działania, podejmowane głównie w ramach ONZ, w zakresie utrzymania i przywracania międzynarodowego pokoju i bezpieczeństwa (wcześniej jako Europejska Współpraca Polityczna w powiązaniu z EWG/Wspólnotą Europejską). W konsekwencji podejmuje ona działania jednostronne o charakterze autonomicznym i nieautonomicznym (zwłaszcza wykonywanie rezolucji Rady Bezpieczeństwa ONZ)[9], prewencyjnym i represyjnym. Środki te można określić mianem środków jednostronnych *sensu largo*. Zaliczyć do nich można zwłaszcza środki przyjmowane w ramach wspólnej polityki handlowej (np. środki obrony handlowej, cła antydumpingowe czy opłaty wyrównawcze), a także różnego typu środki restrykcyjne przyjmowane poza tą polityką.

8 Zob. też Jean-Claude Piris, *The Lisbon Treaty. A Legal and Political Analysis* (Cambridge: CUP 2010), 238 i n.

9 Florian Aumond, „La participation de l'Union Européenne à la préservation de la paix et de la sécurité internationales par l'adoption de mesures restrictives", [w:] *Le droit des relations extérieures*, 365 i n.

Koncepcja środków restrykcyjnych w procesie integracyjnym ewoluowała[10]. Ewolucja ta doprowadziła z jednej strony do odseparowania środków handlowych i środków kapitałowych od środków restrykcyjnych w ścisłym znaczeniu i autonomizacji tych ostatnich[11], a z drugiej do jednoznacznego politycznego i prawnego podporządkowania instrumentów sankcyjnych podejmowanych na podstawie Traktatu funkcjonowaniu o Unii Europejskiej (wcześniej ustanawiającego Wspólnotę Europejską) środkom przyjmowanym w ramach WPZB. Podporządkowanie to oznacza, że żadne środki restrykcyjne w ścisłym znaczeniu nie mogą być podejmowane wyłącznie na podstawie Traktatu funkcjonowaniu o Unii Europejskiej.

W aktualnym stanie prawnym podstawami prawnymi stosowania sankcji przez Unię Europejską są art. 29 TUE i art. 215 TfUE. Art. 29 TUE upoważnia Radę do przyjmowania decyzji (jednomyślnie, zgodnie z art. 31 ust. 1 TUE) określających „podejście Unii do danego problemu o charakterze geograficznym lub przedmiotowym". W świetle art. 25 TUE są to decyzje ustalające „stanowiska Unii", co mogłoby sugerować ich bardziej polityczny niż operacyjny charakter[12]. Art. 29 nie odnosi się też wyraźnie do środków restrykcyjnych. Niemniej, jako „sukcesor" art. 15 TUE (wspólne stanowiska Unii)[13], jest on wykorzystywany jako podstawa stosowania sankcji[14]. Art. 29 ma bardzo ogólny zakres zastosowania. Interpretowany w powiązaniu z art. 24 ust. 1 TUE, pozwala na „przyjmowanie" różnorodnych stanowisk. W rezultacie art. 29 może być podstawą dla każdego środka restrykcyjnego, w tym także ograniczającego ruch osobowy, nakładającego restrykcje gospodarcze

10 Eeckhout, *EU External Relations Law*, 503-506; Joanna Ryszka, *Sankcje gospodarcze wobec podmiotów zewnętrznych w prawie i praktyce Unii Europejskiej* (Toruń: TNOiK, 2008), 119 i n. Zob. też komentarz ogólny C. Mika do tytułu V TUE w jego wersji sprzed Traktatu z Lizbony [w:] Cezary Mik, Władysław Czapliński, *Traktat o Unii Europejskiej. Komentarz* (Warszawa: Wydawnictwo ABC, 2005), 105 i n.

11 Zob. np. Monika Niedźwiedź, „komentarz do art. 215", [w:] *Traktat o funkcjonowaniu Unii Europejskiej*, red. Andrzej Wróbel, t. II (art. 90-222), red. Krystyna Kowalik-Bańczyk, Monika Szwarc-Kuczer (Warszawa: Wolters Kluwer, 2012), 1544.

12 Por. art. 28 TUE, który dotyczy działań operacyjnych. Postanowienie to jest jednak wykorzystywane przede wszystkim do uruchamiania misji Unii.

13 Cezary Mik, „komentarz do art. 15", [w:] Mik, Czapliński, *Traktat o Unii Europejskiej*, 155 i n.

14 Rudolf Geiger, „komentarz do art. 29 TUE", [w:] *European Union Treaties. A Commentary*, red. Rudolf Geiger, Daniel-Erasmus Khan, Markus Kotzur (München-Oxford: C. H. Beck-Hart, 2015), 135-136.

lub finansowe czy embargo na broń. Chociaż art. 29 TUE milczy w tej sprawie, decyzje sankcyjne mogą być wykonywane w ramach WPZB. Wówczas przyjmowane są przez Radę większością kwalifikowaną głosów, chyba że ze względu na żywotne powody polityki krajowej którykolwiek z jej członków zgłosi weto (art. 31 ust. 2 TUE).

Decyzje sankcyjne oparte na art. 29 TUE są wprawdzie podejmowane przez Radę, ale w ramach specyficznych kompetencji Unii Europejskiej. Zgodnie z art. 24 ust. 1 TUE, kompetencje Unii Europejskiej obejmują wszelkie dziedziny z zakresu polityki zagranicznej i wszelkie kwestie dotyczące bezpieczeństwa Unii. Nie jest wszakże jasne, czy ich podstawą jest transfer kompetencji dokonany przez państwa członkowskie. Takiej interpretacji sprzeciwiają się zasada kompetencji przyznanych (art. 4 ust. 1 i art. 5 ust. 2 TUE) w powiązaniu z brakiem WPZB w wykazie kompetencji ustalonym w art. 3-6 TfUE (w art. 2 ust. 4 potwierdza jedynie, że Unia ma kompetencje[15]). Przeczą jej również deklaracje nr 13 i 14 zawarte w Akcie końcowym Konferencji międzyrządowej z 2007 r., zgodnie z którymi państwa członkowskie zachowują własne kompetencje w zakresie kształtowania i prowadzenia polityki zagranicznej, a także zakaz stosowania aktów legislacyjnych[16]. WPZB ma charakter międzyrządowy, czego skutkiem jest konieczność uzgadniania stanowisk i podejmowania decyzji w sposób jednomyślny. Jednocześnie równoległość kompetencyjna państw członkowskich nie oznacza, że nie są zobowiązane do przestrzegania i wykonania decyzji Rady dotyczących środków restrykcyjnych. Są one bowiem zobowiązane do zapewnienia zgodności swych polityk krajowych ze stanowiskami Unii (art. 29 zd. 2 TUE).

Sankcje podejmowane w ramach WPZB mogą wkraczać w sferę gospodarczą i finansową, nie mogą one być w pełni samodzielnie wykonywane przez państwa członkowskie. Te ostatnie dokonały bowiem pewnych

15 Markus Kotzur w komentarzu do art. 2 TfUE (European Union Treaties, European Union Treaties. A Commentary, 205), zauważa: „This competence is of a declaratory nature only and refers to the specific norms regulating the Common foreign and security policy (CFSP). It clarifies that acts concluded within the framework of the CFSP are not governed by the usual canon of competences but are of an inherently independent nature. […] There is a strong interest of clarification in this respect".

16 Zob. Piet Eeckhout, „The EU's Common Foreign and Security Policy after Lisbon: From Pillar Talk to Constitutionalism", [w:] *EU Law After Lisbon*, red. Andrea Biondi, Piet Eeckhout, Stefanie Ripley (Oxford: OUP, 2012), 266-268. Autor zauważa, że chociaż w literaturze kompetencje Unii w dziedzinie WPZB były charakteryzowane jako dzielone, to jednak nie zostało to przyjęte w rewizji lizbońskiej.

transferów kompetencyjnych na rzecz Unii. Do czasu wejścia w życie Traktatu z Lizbony implementacji wspólnotowej dokonywano na podstawie art. 301 i 60 TWE. W tabeli korelacji załączonej do TUE i TfUE uznano te postanowienia za równoważne art. 215 i 75 TfUE. Powstaje zatem pytanie, czy sankcje mogą być nakładane na obu podstawach prawnych. Art. 215 TfUE stanowi:

1. Jeżeli decyzja, przyjęta zgodnie z tytułem V rozdział 2 Traktatu o Unii Europejskiej, przewiduje zerwanie lub ograniczenie w całości lub w części stosunków gospodarczych i finansowych z jednym lub z większą liczbą państw trzecich, Rada przyjmuje niezbędne środki, stanowiąc większością kwalifikowaną na podstawie wspólnego projektu wysokiego przedstawiciela Unii do spraw zagranicznych i polityki bezpieczeństwa oraz Komisji. Rada informuje o tym Parlament Europejski.
2. Jeżeli przewiduje to decyzja przyjęta zgodnie z tytułem V rozdział 2 Traktatu o Unii Europejskiej, Rada może przyjąć środki restrykcyjne wobec osób fizycznych lub prawnych, grup lub podmiotów innych niż państwa, zgodnie z procedurą, o której mowa w ustępie 1.
3. Akty, o których mowa w niniejszym artykule, zawierają niezbędne przepisy w zakresie gwarancji prawnych.

Z kolei art. 75 TfUE stwierdza:

Jeżeli wymaga tego realizacja celów, o których mowa w artykule 67 [ustanowienie przestrzeni wolności, bezpieczeństwa i sprawiedliwości, a w jej ramach m.in. wysokiego poziomu bezpieczeństwa – C.M.], w odniesieniu do zapobiegania terroryzmowi i działalności powiązanej oraz zwalczania tych zjawisk, Parlament Europejski i Rada, stanowiąc w drodze rozporządzeń zgodnie ze zwykłą procedurą ustawodawczą, określają ramy środków administracyjnych dotyczących przepływu kapitału i płatności, takich jak zamrożenie funduszy, aktywów finansowych lub zysków z działalności gospodarczej, które należą do osób fizycznych lub prawnych, grup lub innych podmiotów innych niż państwa, są w ich posiadaniu lub dyspozycji.

Rada, na wniosek Komisji, przyjmuje środki w celu wdrożenia ram, o których mowa w akapicie pierwszym.

Akty, o których mowa w niniejszym artykule, zawierają niezbędne przepisy w zakresie gwarancji prawnych.

Do obu postanowień, których treść ustalono w Traktacie z Lizbony, dodano deklarację nr 25. Zgodnie z nią, gwarancje prawne, o których mowa w art. 215 i 75 TfUE oznaczają konieczność poszanowania podstawowych praw i wolności. W szczególności należy zwracać dostateczną uwagę na ochronę i poszanowanie prawa osób fizycznych lub podmiotów objętych sankcjami do korzystania z gwarancji ustawowych (ang. *due process*). W tym celu oraz w celu zagwarantowania ścisłej kontroli sądowej decyzji

nakładających sankcje muszą być oparte na jasnych i wyraźnych kryteriach, dostosowanych do specyfiki każdego środka restrykcyjnego.

Nie ulega wątpliwości, że podstawą stosowania środków restrykcyjnych jest art. 215 TfUE[17]. Jego użycie jest wszakże uzależnione od uprzedniego wydania decyzji sankcyjnej na podstawie postanowień rozdz. 2 tytułu V TUE, a zatem postanowień WPZB. Oznacza to, że nie może być on wykorzystywany samodzielnie, a jego obowiązywanie zależy od obowiązywania decyzji z zakresu WPZB[18]. Co więcej, środki restrykcyjne przyjmowane na mocy art. 215 muszą być ograniczone do „stosunków gospodarczych i finansowych". Nie mogą obejmować środków innego rodzaju, np. embarga na broń czy środków ograniczających przepływ osób[19].

Na podstawie art. 215 TfUE, w specyficznym trybie (wspólny projekt Wysokiego Przedstawiciela ds. Zagranicznych i Polityki Bezpieczeństwa i Komisji) Rada może przyjąć niezbędne środki. Przyjmuje je większością kwalifikowaną głosów, jedynie po poinformowaniu Parlamentu Europejskiego. Ma tu pewną swobodę co do formy prawnej środków. W praktyce używa się rozporządzeń. Sankcje są zasadniczo kierowane przeciwko państwom trzecim (ewentualnie ich ugrupowaniom). Jeśli jednak tak wynika z decyzji Rady przyjętej w ramach WPZB, Rada może skierować sankcje przeciwko osobom fizycznym, prawnym lub innym jeszcze podmiotom niż państwa. W ostatniej sytuacji mogą to być środki samodzielne (nie muszą być stosowane jednocześnie wobec państw trzecich). Akty nakładające środki restrykcyjne na podmioty inne niż państwa muszą zawierać gwarancje prawne (muszą chronić ich prawa i wolności, szanować uprawnienia proceduralne; sankcje muszą być oparte na wyraźnych i jasnych kryteriach, dostosowanych do specyfiki każdego przypadku, aby mogły być przedmiotem kontroli sądowej).

---

17 Zob. Monika Niedźwiedź, komentarz do art. 215 TfUE, s. 1542 i n.

18 Monika Niedźwiedź, komentarz do art. 215 TfUE, s. 1549-1550. Uzależnienie to jest jednokierunkowe, tzn. nieważność całości lub części rozporządzenia uchwalonego na mocy art. 215 nie powoduje skutków prawnych dla decyzji wydanej na podstawie art. 29 TUE.

19 Podkreśla to m.in. Eeckhout, The EU's Common Foreign and Security Policy, 506. Jednak mniej kategorycznie Trybunał Sprawiedliwości w wyroku w sprawie Bank Refah Kargaran v. Rada UE z 6.10.2020 r., C-134/19 P, ECLI:EU:C:2020:793, stwierdził, że „decyzje WPZiB i rozporządzenia oparte na art. 215 TFUE, które je wykonują, mogą nie być identyczne pod względem merytorycznym. W szczególności, co się tyczy osób fizycznych, ograniczenia wjazdu na terytorium państw członkowskich mogą być zawarte w decyzjach WPZiB, bez konieczności ich powielania w rozporządzeniach opartych na art. 215 TFUE" (pkt 41).

Kompetencje Unii Europejskiej w odniesieniu do stosowania środków restrykcyjnych w rozumieniu art. 215 TfUE nie są sprecyzowane. W szczególności tej materii nie wymienia się w art. 3-6 TfUE. Nie ulega jednak wątpliwości, że państwa członkowskie przekazały kompetencje do ich przyjmowania przez Unię. Jedynie sankcje inne niż finansowe i gospodarcze mogą być wykonywane bezpośrednio przez państwa członkowskie.

Decyzje podejmowane na podstawie art. 29 TUE nie podlegają zaskarżeniu. Natomiast zgodnie z art. 275 akapit 2 TfUE, Trybunał może kontrolować przestrzeganie art. 40 TUE (w uproszczeniu rozgraniczenie materii między wspólną polityką zagraniczną i bezpieczeństwa a materiami regulowanymi w TfUE) oraz orzekać w sprawie skarg wniesionych na podstawie art. 263 akapit czwarty TfUE (kontrola legalności decyzji sankcyjnych wobec osób fizycznych lub prawnych[20] przyjętych przez Radę na podstawie tytułu V rozdział 2 TUE). Ponadto możliwe jest dochodzenie odszkodowania od Unii Europejskiej za szkody powstałe wskutek wydania nieważnego rozporządzenia z art. 215 TfUE[21].

Gdy chodzi o art. 75 TfUE, pozwala on na podejmowanie środków autonomicznych w związku z ustanowieniem przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Chodzi jednak tutaj o środki specyficzne, zmierzające wyłącznie do zapobiegania terroryzmowi, działalności z nim związanej oraz ich zwalczania. Tryb działania odbiega od tego z art. 215, gdyż akty w formie rozporządzeń uchwala w zwykłym trybie prawodawczym Parlament Europejski i Rada, a projektodawcą jest tylko Komisja. Środków tych nie określa się zresztą mianem restrykcyjnych. Są to środki administracyjne, mimo że stanowią podstawę ograniczenia przepływu kapitału i płatności (m.in. zamrożenie funduszy, aktywów finansowych lub zysków z działalności gospodarczej), należących do „osób fizycznych lub prawnych, grup lub innych podmiotów innych niż państwa, są w ich posiadaniu lub dyspozycji".

20 Nie jest jasne, czy w świetle art. 215 akapit 2 TfUE istotnie skarga jest ograniczona tylko do tego kręgu osób (nie korzystałyby z niej inne podmioty objęte sankcjami).

21 Wyrok w sprawie Bank Refah Kargaran v. Rada UE z 6.10.2020 r., C-134/19 P, ECLI:EU:C:2020:793, pkty 30, 37, 39. W punkcie 40 stwierdza się: „zasada skutecznej ochrony sądowej osób lub podmiotów, do których skierowane są środki ograniczające, wymaga, w celu zapewnienia pełnej ochrony, aby Trybunał Sprawiedliwości Unii Europejskiej mógł orzekać w przedmiocie skargi o odszkodowanie i zadośćuczynienie wniesionej przez takie osoby lub podmioty mającej na celu uzyskanie odszkodowania za szkody i krzywdy spowodowane przez środki ograniczające przewidziane w decyzjach wspólnej polityki zagranicznej i bezpieczeństwa".

W tym wypadku także konieczne jest zapewnienie gwarancji prawnych adresatom tych środków.

Relacje zakresowe między art. 215 a art. 75 TfUE nie są w pełni jasne[22]. Niewątpliwie tylko pierwszy z nich ogólny charakter i jednoznacznie służy do stosowania środków restrykcyjnych. Drugi dotyczy jedynie środków o charakterze kapitałowym. Są to restrykcyjne środki administracyjne, które mogą być przyjmowane wyłącznie w zakresie przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Tylko środki restrykcyjne mogą być skierowane przeciwko państwom trzecim. Środki z art. 75 mogą być stosowane wyłącznie wobec aktorów niepaństwowych i tylko w związku z terroryzmem i działalnością z nim związaną[23]. Oba postanowienia zasadniczo różnią się procedurami przyjmowania aktów i znaczeniem decyzji WPZB dla wydania każdego z nich. Wspólne dla aktów jest natomiast to, że muszą obejmować gwarancje dla adresatów i mogą być wykonane przez Radę[24]. Niemniej, różnice między obu postanowieniami są na tyle fundamentalne, że nie mogą być jednocześnie podstawą jednego rozporządzenia[25]. W rezultacie jedynie art. 215 TfUE należy uznać za podstawę stosowania środków restrykcyjnych w ścisłym znaczeniu.

22 Zob. też wyrok Trybunału Sprawiedliwości w sprawie Parlament Europejski v. Rada UE z 19.7.2012 r., C-130/10, pkty 50-54, ECLI:EU:C:2012:472.

23 Jednak Trybunał Sprawiedliwości w sprawie Parlament Europejski v. Rada Unii Europejskiej z 19.7.2012 r., C-130/10, ECLI:EU:C:2012:472, pkt 63, uznał, że „Jako że terroryzm stanowi zagrożenie dla pokoju i bezpieczeństwa międzynarodowego, zwalczanie tego zjawiska może stanowić cel działań, które Unia prowadzi w ramach WPZiB, a także środków podejmowanych w celu realizacji tej polityki w ramach działań zewnętrznych Unii, w szczególności zaś środków ograniczających w rozumieniu art. 215 ust. 2 TFUE". Rozróżnienie zakresów art. 215 i 75 odbywa się zatem na poziomie dziedzin (pkt 65). W konsekwencji, według Trybunału, art. 75 stanowi *lex specialis* wobec art. 215 TfUE, co jest jednak dyskusyjne. Środki te powinny bowiem mieć charakter skorelowany z przestrzenią wolności, bezpieczeństwa i sprawiedliwości, a zatem karno-administracyjny. Zob. też podobnie Markus Kotzur, „komentarz do art. 75 TfUE", 420; Agnieszka Grzelak, „komentarz do art. 75 TfUE", [w:] Traktat o funkcjonowaniu Unii Europejskiej, red. Andrzej Wróbel, t. I (art. 1-89), red. Dawid Miąsik, Nina Półtorak (Warszawa: Wolters Kluwer, 2012), 1109-1110.

24 Zob. też trafne spostrzeżenia Monika Niedźwiedź, komentarz do art. 215 TfUE, s. 1543-1544.

25 Wyrok w sprawie Parlament Europejski v. Rada UE z 19.7.2012 r., C-130/10, ECLI:EU:C:2012:472, pkt 49.

2.2. Polityczne aspekty stosowania środków restrykcyjnych przez Unię Europejską

Stosowanie środków restrykcyjnych przez Unię Europejską jest jednym z elementów jej działania zewnętrznego. W tych ramach Unia zdołała ukształtować własną politykę podejmowania decyzji w sprawie sankcji. Pierwsze Wytyczne dotyczące sankcji Rada zatwierdziła 3 grudnia 2003 roku[26]. Niebawem (7 czerwca 2004 roku) Rada uchwaliła też Podstawowe zasady dotyczące korzystania ze środków restrykcyjnych (sankcji)[27]. Najnowszą wersję Wytycznych Rada przyjęła 4 maja 2018 roku[28] Tego dnia zaakceptowała również zaktualizowaną wersję Najlepszych praktyk UE dotyczących efektywnej implementacji środków restrykcyjnych[29].

Spośród wymienionych dokumentów podstawowe znaczenie mają obecnie Wytyczne z 2018 roku. Służą one standaryzacji korzystania z sankcji. Według nich środki restrykcyjne mają być zgodne z art. 21 TUE, precyzować cele działania zewnętrznego Unii. W zakresie wykonywania rezolucji Rady Bezpieczeństwa ONZ mają być zgodne także z nimi (Unia może jednak stosować środki bardziej restrykcyjne). Gdy przyjmuje autonomiczne środki jednostronne, Unia powinna poszukiwać dla nich szerszego wsparcia we wspólnocie międzynarodowej. Wytyczne stanowią, że celem sankcji jest doprowadzenie do „zmiany polityki lub działań kraju docelowego, części kraju, rządu, podmiotów lub osób fizycznych, zgodnie z celami określonymi w decyzji Rady". Ponadto, o ile to możliwe i zgodne ze strategią Unii wobec państwa trzeciego, środki restrykcyjne mogą zachęcać do zmiany polityki lub działalności. Cel każdego środka musi być wyraźnie sprecyzowany i zgodny ze strategią Unii w danej dziedzinie (należy to odzwierciedlić w preambule aktu Rady). Środki restrykcyjne nie powinny mieć motywacji gospodarczej.

Uznaje się też, że środki restrykcyjne określone w decyzji Rady z art. 29 TUE należy wykonać na szczeblu Unii lub krajowym. Embargo na broń i ograniczenia w przepływie osób powinny być wykonywane bezpośrednio przez państwa członkowskie, podczas gdy środki gospodarcze i finansowe powinny być implementowane przez rozporządzenia wydane w trybie art. 215 TfUE. Sankcje mogą zawierać odwołania do rezolucji Rady Bezpieczeństwa

26 Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy, doc. 15579/03. https://data.consilium.europa.eu/doc/document/ST-15579-2003-INIT/en/pdf. [dostęp: 3.9.2021].

27 Doc. 10198/1/04 REV 1. https://data.consilium.europa.eu/doc/document/ST-10198-2004-REV-1/en/pdf. [dostęp: 3.9.2021].

28 Sanctions Guidelines, doc. 5664/18. https://data.consilium.europa.eu/doc/document/ST-5664-2018-INIT/en/pdf. [dostęp: 3.9.2021].

29 Doc. 8519/18. https://data.consilium.europa.eu/doc/document/ST-8519-2018-INIT/en/pdf. [dostęp: 3.9.2021].

i innych zasad prawa międzynarodowego. Ich wykonanie musi być zgodne z prawem międzynarodowym, zwłaszcza z zobowiązaniami międzynarodowymi Unii (np. w zakresie WTO). Muszą one szanować prawa człowieka i podstawowe wolności, a zwłaszcza reguły *due process* i prawa do skutecznego środka odwoławczego. Środki muszą być proporcjonalne do ich celu. Środki celowane (*targeted measures*) uznaje się za bardziej skuteczne niż środki niedyskryminacyjne. Minimalizują one skutki w odniesieniu do osób nieponoszących odpowiedzialności za określone polityki czy działania. Do tego typu środków zalicza się m.in. „zamrożenie funduszy i zasobów gospodarczych, ograniczenia wjazdu, embargo na broń, embargo na sprzęt, który może być użyty do represji wewnętrznych, inne ograniczenia eksportowe, ograniczenia importowe i zakazy lotów", a ponadto „odstąpienie od świadczenia usług finansowych, w tym w związku z zakazami eksportu niektórych produktów, a także zakazami inwestycji" oraz „zakazy sektorowe lub środki zapobiegające niewłaściwemu wykorzystaniu sprzętu, technologii lub oprogramowania do monitorowania oraz przechwytywanie Internetu lub innych form komunikacji".

Rada przywiązuje dużą wagę do identyfikacji aktorów, wobec których należy zastosować środki restrykcyjne, i ich odróżnienia od tych, którzy takimi środkami nie powinni być dotknięci. Listy takie muszą respektować standardy ustalone przez Trybunał Sprawiedliwości (zwłaszcza prawo obrony i zasada efektywnej ochrony sądowej) i być należycie uzasadnione. Należy zapewnić możliwość wykreślenia z listy. W przypadku decyzji z art. 29 TUE dotykających osób fizycznych mogą one obejmować także członków rodziny, lecz nie dzieci poniżej 18 roku życia. W Wytycznych wskazuje się też, że akty prawne Rady nakładające środki restrykcyjne powinny zawierać „zwolnienia uwzględniające w szczególności podstawowe potrzeby osób, których dotyczy cel, opłaty prawne, wydatki nadzwyczajne lub, w stosownych przypadkach, potrzeby humanitarne lub zobowiązania międzynarodowe, w tym jako państwa przyjmujące organizacje międzynarodowe lub OBWE, w odniesieniu do różnych podjętych środków ograniczających".

Akty prawne dotyczące sankcji powinny podlegać regularnemu przeglądowi. Osiągnięcie zakładanych celów powinno też prowadzić do wygaśnięcia środków, chyba że Rada postanowi inaczej. Rada wypracowała też standardowe rozwiązania, jakie powinny być zawarte w sankcyjnych instrumentach prawnych (dotyczą one definicji, ale także poszczególnych rodzajów sankcji).

W Wytycznych Rada określiła także sposób postępowania w przypadku negocjowania w ONZ rezolucji sankcyjnych i ich wykonania za pośrednictwem sankcji unijnych. Uznała przy tym, że sankcje należy stosować tylko do sytuacji powiązanych z Unią Europejską (terytorium Unii, statki i samoloty państw członkowskich, przynależni państw członkowskich, biznes w części lub całości prowadzony w Unii). Rada podkreśliła, że Unia powinna

powstrzymać się od przyjmowania instrumentów legislacyjnych stosowanych poza terytorium Unii z naruszeniem prawa międzynarodowego. Sprecyzowała też liczne wskazówki dotyczące tego, jak państwa członkowskie mają zapewnić zgodność z przyjętymi środkami restrykcyjnymi (zwłaszcza co do zachowań aktorów niepaństwowych, na których nałożono sankcje). Ponadto w załączniku I Rada sformułowała zalecenia dotyczące stosowania sankcji autonomicznych. Zdaniem Rady powinny to być środki prewencyjne, niepunitywne. Co do zasady powinny one respektować podobne kryteria oraz środki wykonujące rezolucje Rady Bezpieczeństwa ONZ.

3. Przestrzeń cyfrowa z perspektywy Unii Europejskiej

3.1. Ogólna charakterystyka przestrzeni cyfrowej

Przestrzeń cyfrowa jest tworem względnie nowym. Jej powstanie kojarzy się z ustanowieniem światowej sieci internetowej[30]. W literaturze prawniczej nie jest jednak jasne, co obejmuje przestrzeń cyfrowa i jaki jest jej stosunek do internetu. Tak np. Nicholas Tsagourias (za L. Tobansky'm) wyróżnia trzy poziomy przestrzeni cyfrowej: 1) infrastrukturę komputerową, łącznie z urządzeniami i środkami służącymi do jej wewnętrznego powiązania i komunikacji; 2) oprogramowanie; 3) pakiety danych i elektronikę[31]. Z kolei Kristen Eichenseher (odwołując się do Y. Benklera) wywodzi, że internet, a nie przestrzeń cyfrowa, obejmuje trzy poziomy: 1) fizyczny (hardware; infrastruktura fizyczna – komputery i serwery, okablowanie itp.); 2) logiczny

30 Radosław Grabowski, „Geneza i ewolucja sieci globalnej", [w:] *Wpływ internetu na ewolucję państwa i prawa*, red. Radosław Grabowski (Rzeszów: Wydawnictwo Uniwersytetu Rzeszowskiego, 2008), 40 i n. Internet stanowił początkowo technologię wojskową (ARPAnet), następnie był stopniowo otwierany na wybrane uczelnie wyższe, potem został był wykorzystywany przez ograniczoną liczbę podmiotów (zarządzała nim Narodowa Fundacja Naukowa USA; NSFnet, 1986 r.). W 1991 r. zniesiono ograniczenia w dostępie do sieci i uchylono zakaz jej wykorzystywania do celów handlowych (42-43). Początkowo sieć wirtualna działała w oparciu o jeden komputer centralny. Obecnie ma charakter rozproszony (istnieją komputery węzłowe, których liczba rośnie). Wrażliwym miejscem sieci są jednak główne serwery przechowujące nazwy domen, określane jako DNS (Domain Name System). Zob. też Karol Dobrzeniecki, *Lex informatica* (Toruń: TNOiK, 2008), 31 i n. Autor podkreśla, że momentem przełomowym w rozwoju internetu było powstanie WWW oraz prywatyzacja sieci szkieletowej (41).

31 Nicholas Tsagourias, „The legal status of cyberspace", [w:] *Research Handbook on International Law and Cyberspace*, red. Nicholas Tsagourias, Russell Buchan (Cheltenham-Northampton: Edward Elgar Publishing, 2015), 15 (za L. Tobansky'm).

(software; oprogramowanie); 3) treściowy (content; zawartość merytoryczna). Nie kojarzy jednak przestrzeni cyfrowej z elementem fizycznym czy konkretnym miejscem[32]. Z kolei w komentarzu do reg. 1 (suwerenność w przestrzeni cyfrowej) Tallińskiego podręcznika dotyczącego stosowania prawa międzynarodowego do operacji cyfrowych, opracowanego przez dużą grupę ekspertów pod auspicjami NATO, uznaje się, że przestrzeń cyfrowa składa się z trzech warstw: 1) fizycznej (fizyczne składniki sieci, jak oprzyrządowanie i inna infrastruktura, jak kable, rutery, serwery, komputery); 2) logicznej (połączenia istniejące między urządzeniami sieciowymi, w tym aplikacje, dane, protokoły, umożliwiające wymianę danych w ramach płaszczyzny fizycznej); 3) społecznej (jednostki i grupy zaangażowane w działalność cyfrową)[33].

Bez wnikania w szczegóły można przyjąć, że przestrzeń cyfrowa ma charakter wirtualny, lecz opiera się na istniejącej fizycznie i dającej się terytorialnie zlokalizować infrastrukturze i działa dzięki niej i specjalistycznemu oprogramowaniu. Przestrzeń cyfrowa nie jest nierzeczywista. Ma charakter w pełni realny. Zarazem jest przestrzenią nieterytorialną (nie jest związana z konkretnym terytorium państwowym, przenika granice państw, działa w strefach niepodlegających suwerenności czy jurysdykcji państwa; może zostać jednak wyłączona z przestrzeni globalnej i ograniczona do określonego terytorium), zdecentralizowaną (nie ma jednego regulatora zarządzającego przestrzenią i jednego centralnego serwera) oraz globalny (sieć teoretycznie rozciąga się na cały świat; jednak działa o tyle, o ile istnieje infrastruktura internetowa oraz zasięg i dostęp do internetu).

3.2. Stosunek Unii Europejskiej do przestrzeni cyfrowej

Unia Europejska dostrzega globalny wymiar sieci i przestrzeni, a także jej wielopłaszczyznowość i zaangażowanie wielu aktorów na różnych szczeblach (Unia akceptuje w tej sprawie tzw. *multistakeholder approach*, które przyjmuje również ONZ oraz państwa Ameryki Północnej i Europy oraz ich koalicjanci). Według Unii w przestrzeni cyfrowej powinna panować wolność. Nikt nie powinien być wykluczony z dostępu do internetu i korzyści wynikających z przestrzeni cyfrowej. Każdy powinien czuć się bezpieczny w sieci.

Unia Europejska stara się kształtować swój stosunek do internetu i przestrzeni cyfrowej od wczesnych lat dziewięćdziesiątych XX wieku (początkowo w ramach koncepcji społeczeństwa informacyjnego)[34]. Dostrzega korzyści i niebezpieczeństwa związane z aktywnością w przestrzeni cyfrowej,

32 Zob. Kristen E. Eichenseher, „The Cyber-Law of Nations" *The Georgetown Law Journal*, nr 2 (2015): 322-325.

33 *Talinn Manual 2.0 on the International Law Applicable to Cyber Operations*, red. Michael N. Schmitt (Cambridge: CUP, 2017), 12.

34 Cezary Mik, *Media masowe w europejskim prawie wspólnotowym* (Toruń: TNOiK, 1999), 63-71.

wewnętrzne i międzynarodowe aspekty działalności cyfrowej[35]. Stara się formułować ogólne podejście do internetu i przestrzeni cyfrowej. Znalazło to wyraz m.in. w komunikatach pt. Polityka internetowa i rola zarządzania Europy w kształtowaniu przyszłego zarządzania internetowego z 12 lutego 2014 roku[36] czy Kształtowanie cyfrowej przyszłości Europy z lutego 2020 roku[37]

Unia uznaje w szczególności znaczenie internetu i przestrzeni cyfrowej dla rynku wewnętrznego. W związku z tym opracowała m.in. Strategię jednolitego rynku cyfrowego dla Europy z 6 maja 2015 roku[38], a także przyjęła lub proponuje liczne akty prawne uwzględniające aspekty cyfrowe w różnych dziedzinach integracji (np. ochrona danych, ochrona praw własności intelektualnej, internet rzeczy, łączność elektroniczna, sztuczna inteligencja, usługi cyfrowe).

Jednocześnie fundamentalną sprawą staje się zagadnienie bezpieczeństwa cyfrowego, które staje się częścią ogólniejszej strategii bezpieczeństwa Unii Europejskiej[39]. Wyrazem troski o bezpieczeństwo cyfrowe stała się Strategia bezpieczeństwa cyfrowego Unii Europejskiej: otwarta, bezpieczna i chroniona przestrzeń cyfrowa z 7 lutego 2013 roku[40], a obecnie Strategia UE w zakresie bezpieczeństwa cyfrowego na dekadę cyfrową z 16 grudnia 2020 roku[41] Istotne staje się bezpieczeństwo Unii, jej członków i obywateli, a z innej perspektywy bezpieczeństwo sieci i systemów informatycznych, bezpieczeństwo infrastruktury krytycznej. Pojawiają się regulacje przewidujące konieczność ustanowienia ochrony przed szkodliwą działalnością cyfrową (atakami cyfrowymi) oraz reakcje administracyjne i karne (przestępczość cyfrowa). Warto w tym miejscu wspomnieć m.in. o dyrektywie Parlamentu Europejskiego i Rady 2013/40/UE z 12 sierpnia 2013 roku dotyczącej ataków na systemy informatyczne i zastępującej decyzję ramową Rady 2005/222/

35 Zob. m.in. Ramses A. Wessel, „Towards EU cybersecurity law: Regulating a new policy field", [w:] *Research Handbook*, 403 i n.; Joanna Worona, *Cyberprzestrzeń a prawo międzynarodowe* (Warszawa: Wolters Kluwer, 2020), 177 i n.

36 COM (2014)72 final.

37 Tekst: https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf. [dostęp: 3.9.2021].

38 COM (2015)192 final, {SWD(2015)100 final}.

39 Zob. Strategię bezpieczeństwa Unii Europejskiej z 24.7.2020 r., COM(2020) 605 final.

40 Wspólny komunikat Komisji Europejskiej i Wysokiego Przedstawiciela do spraw Zagranicznej i Polityki Bezpieczeństwa, JOIN (2013) 1 final.

41 Wspólny komunikat Komisji Europejskiej i Wysokiego Przedstawiciela do spraw Zagranicznej i Polityki Bezpieczeństwa do Parlamentu Europejskiego i Rady, JOIN (2020)18 final.

WSiSW[42] i dyrektywie Parlamentu Europejskiego i Rady 2016/1148 z 6 lipca 2016 roku w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[43].

W Unii ustanowiono Agencję ds. Bezpieczeństwa Cyfrowego (ENISA)[44], a także Wspólne Przedsięwzięcie w dziedzinie Europejskich Obliczeń Wielkiej Skali[45]. W 2013 roku Europol stworzył Europejskie Centrum Przestępczości Cyfrowej[46]. W 2020 roku stworzono również Centrum Kompetencji Bezpieczeństwa Cyfrowego.

Oprócz harmonizacji przepisów krajowych dotyczących bezpieczeństwa cyfrowego i rozwiązań instytucjonalnych Unia Europejska zdołała również wypracować stanowisko i ustalić standardy dotyczące zapewnienia zewnętrznego bezpieczeństwa cyfrowego, w tym ochrony przed szkodliwą działalnością cyfrową pochodzącą spoza Unii, łącznie z atakami cyfrowymi. Zostały one ulokowane w ramach działania zewnętrznego Unii (art. 21 i n. TUE) i przyjęły postać dyplomacji cyfrowej.

42 Dz. Urz. UE z 14.8.2013 r., L 218, s. 8.

43 Dz. Urz. UE z 19.7.2016 r., L 194, s. 1. W 2020 r. Komisja przyjęła projekt nowej dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa cyfrowego na terytorium Unii, uchylającej dyrektywę (UE) 2016/1148, COM (2020) 823 final z 16.12.2020 r.

44 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z 17.4.2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Bezpieczeństwa Cyfrowego) oraz certyfikacji bezpieczeństwa cyfrowego w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o bezpieczeństwie cyfrowym), Dz. Urz. UE z 7.6.2019 r., L 151, s. 15.

45 Rozporządzenie Rady (UE) 2018/1488 z 28.9.2018 r. w sprawie ustanowienia Wspólnego Przedsięwzięcia w dziedzinie Europejskich Obliczeń Wielkiej Skali, Dz. Urz. UE z 8.10.2018 r., L 252, s. 1.

46 Zob. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3. [dostęp: 3.9.2021].

4. Miejsce środków restrykcyjnych w ramach dyplomacji cyfrowej Unii Europejskiej

Dyplomacja cyfrowa jest tworem XXI w.[47]. Jest ona formułowana i wykorzystywana w działalności państw[48], a także niektórych organizacji międzynarodowych, w tym Unii Europejskiej. Koncepcja dyplomacji cyfrowej Unii została ustalona najpierw w Konkluzjach na temat dyplomacji cyfrowej z 11 lutego 2015 roku[49]. Poruszono tu w szczególności kwestie promocji i poszanowania praw człowieka w przestrzeni cyfrowej, norm zachowania państw i stosowania istniejącego prawa międzynarodowego w sferze bezpieczeństwa międzynarodowego, zarządzania internetem, umocnienia konkurencyjności i pomyślności UE, budowy zdolności cyfrowej i rozwoju, strategicznego zaangażowania z kluczowymi partnerami i organizacjami międzynarodowymi.

Celem dyplomacji cyfrowej stało się m.in. przyczynienie się do zmniejszenia zagrożeń cyfrowych, zapobiegania konfliktom i większej stabilności w stosunkach międzynarodowych przez wykorzystanie instrumentów dyplomatycznych i prawnych. W Konkluzjach Rada wezwała Unię i jej członków do stawania czoła rosnącym zagrożeniom i wyzwaniom cyfrowym przez zwiększenie odporności krytycznej infrastruktury informacyjnej i umocnienie ścisłej współpracy i koordynacji między interesariuszami międzynarodowymi (*international stakeholders*) przez inicjatywy dotyczące rozwoju budowy zaufania, wspólnych standardów, międzynarodowych ćwiczeń cyfrowych, wzrost świadomości, szkolenia, badania i edukację, mechanizmy odpowiadania na incydenty.

Dla ukształtowania dyplomacji cyfrowej podstawowe znaczenie mają jednak Konkluzje w sprawie Ram wspólnej odpowiedzi dyplomatycznej Unii Europejskiej na szkodliwą działalność cyfrową z 19 czerwca 2017

47 Zob. np. ogólnie Katharina Ziolkowski, „E-Diplomacy and Diplomatic Law in the Internet Era", [w:] *Peacetime Regime for State Activities in Cyberspace. International Law, International relations and Diplomacy*, red. Katharina Ziolkowski (Talinn: NATO CCD COE Publ., 2013), 393 i n.; https://ccdcoe.org/uploads/2018/10/PeacetimeRegime.pdf. [dostęp: 3.9.2021], 135 i n., a w stosunku do UE: B. Piskorska, „Dyplomacja cyfrowa: instrument miękkiej siły Unii Europejskiej w stosunkach międzynarodowych", [w:] *Dyplomacja cyfrowa jako instrument polityki zagranicznej XXI* wieku, red. Marcin Kosienkowski, Beata Piskorska (Lublin: Wydawnictwo KUL, 2014), 105 i n., zwł. 134-139.

48 Zob. np. ustawę Stanów Zjednoczonych wspierającą międzynarodową dyplomację cyfrową USA i inne cele z 18.1.2018 r.

49 Council Conclusions on Cyber Diplomacy, doc. 6122/15. https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf. [dostęp: 3.9.2021].

roku[50] a także Wytyczne wykonawcze do Ram wspólnej odpowiedzi dyplomatycznej Unii Europejskiej na szkodliwą działalność cyfrowej z 9 października 2017 roku[51]. W pierwszym z dokumentów Rada ustaliła, że przestrzeń cyfrowa „oferuje znaczne możliwości, ale stwarza również stale zmieniające się wyzwania dla polityk zewnętrznych UE, w tym dla WPZB". Potwierdziła też „rosnącą potrzebę ochrony integralności i bezpieczeństwa UE, jej państw członkowskich i ich obywateli przed zagrożeniami cybernetycznymi i szkodliwymi działaniami cyfrowymi". Rada wyraziła zaniepokojenie „zwiększoną zdolnością i chęcią podmiotów państwowych i niepaństwowych do realizacji swoich celów przez podejmowanie szkodliwych działań cyfrowych o różnym zakresie, skali, czasie trwania, intensywności, złożoności, wyrafinowaniu i wpływie". Działania tego rodzaju mogą stanowić czyny międzynarodowo bezprawne. Rada podkreśliła też, że państwa nie powinny prowadzić ani świadomie wspierać działalności przy wykorzystaniu technologii informacyjno-komunikacyjnych sprzecznej z ich zobowiązaniami wynikającymi z prawa międzynarodowego. W następstwie raportem Grupy Ekspertów Rządowych ONZ z 2015 roku (GGE), Rada przyjęła, że państwa nie powinny też świadomie zezwalać na wykorzystywanie ich terytorium do czynów międzynarodowo bezprawnych popełnianych z wykorzystaniem technologii informacyjno-komunikacyjnych. W kontekście raportów GGE z lat 2010, 2013 i 2015 Rada stwierdziła, że prawo międzynarodowe ma zastosowanie do przestrzeni cyfrowej.

Rada wyraziła przekonanie, że Unia i jej członkowie są zdecydowani „aktywnie wspierać opracowywanie dobrowolnych, niewiążących norm odpowiedzialnego zachowania państwa w przestrzeni cyfrowej oraz regionalnych środków budowy zaufania uzgodnionych przez OBWE w celu zmniejszenia ryzyka konfliktów wynikających z wykorzystywania technologii informacyjno-komunikacyjnych". Dodała, że Unia pragnie angażować się w pokojowe rozstrzyganie sporów międzynarodowych w przestrzeni cyfrowej, jak również że „wszystkie wysiłki dyplomatyczne UE powinny mieć na celu w pierwszym rzędzie promowanie bezpieczeństwa i stabilności w przestrzeni cyfrowej przez zacieśnienie współpracy międzynarodowej, a także zmniejszenie ryzyka, błędnego postrzegania, eskalacji i konfliktu, które mogą wynikać z incydentów związanych z użyciem technologii informacyjno-komunikacyjnych".

50 Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), doc. 10474/17. https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf. [dostęp: 3.9.2021].

51 Doc. 13007/17. https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf. [dostęp: 3.9.2021].

Rada przyjęła również, że „wyraźne sygnalizowanie prawdopodobnych konsekwencji wspólnej reakcji dyplomatycznej UE na takie szkodliwą działalność cyfrową wpływa na zachowanie potencjalnych agresorów w przestrzeni cyfrowej, wzmacniając tym samym bezpieczeństwo UE i jej państw członkowskich". Jednocześnie Unia wskazała, że „przypisanie odpowiedzialności państwu lub podmiotowi niepaństwowemu pozostaje suwerenną decyzją polityczną opartą na danych wywiadowczych pochodzących ze wszystkich źródeł i powinno być ustalane zgodnie z prawem międzynarodowym dotyczącym odpowiedzialności państwa". W tym kontekście podkreślono, że „nie wszystkie środki wspólnej reakcji dyplomatycznej UE na złośliwe działania w przestrzeni cyfrowej wymagają przypisania odpowiedzialności państwu lub aktorowi niepaństwowemu".

Na tym tle Rada stwierdziła, że środki podejmowane w ramach WPZB, w tym sankcje, mieszczą się w ramach wspólnej reakcji dyplomatycznej Unii na szkodliwe działania cyfrowe. Powinny one „zachęcać do współpracy, ułatwiać zmniejszanie bezpośrednich i długoterminowych zagrożeń oraz wpływać na zachowanie potencjalnych agresorów w dłuższej perspektywie".

Rada postanowiła, że należy kontynuować prace nad reakcją Unii wobec szkodliwej działalności cyfrowej. Uwzględnić przy tym trzeba zasady: 1) reakcja ma służyć ochronie integralności i bezpieczeństwa UE, jej państw członkowskich i ich obywateli oraz uwzględniać szerszy kontekst stosunków zewnętrznych UE z danym państwem; 2) reakcja ma zapewnić osiągnięcie celów WPZB określonych w TUE oraz odpowiednich procedur przewidzianych do ich osiągnięcia; 3) reakcja ma opierać się na wspólnej świadomość sytuacyjnej uzgodnionej przez państwa członkowskie i odpowiadającej potrzebom konkretnej sytuacji; 4) reakcja Unii ma być proporcjonalna do zakresu, skali, czasu trwania, intensywności, złożoności, stopnia zaawansowania i wpływu działalności cyfrowej; 5) należy przestrzegać obowiązującego prawa międzynarodowego, nie wolno też naruszać podstawowych praw i wolności jednostki.

W wykonaniu konkluzji czerwcowych Rada przyjęła Wytyczne wykonawcze. Przypomniano tu, że działalność szkodliwa może pochodzić od podmiotów państwowych, niepaństwowych, a także może mieć charakter hybrydowy. Może ona polegać na działaniach przeciwko infrastrukturze, szpiegostwie cyfrowym, kradzieży własności intelektualnej, przestępczości cyfrowej lub konfliktach cyfrowych i dezinformacji przy użyciu środków cyfrowych. Rada uznała, że taka działalność wymaga podjęcia środków wykraczających poza dotychczasową politykę komunikacji i bezpieczeństwa cyfrowego. Zauważyła, że szkodliwą działalność cyfrową należy postrzegać również w kontekście prac nad odpornością (zdolnością do wytrzymywania stresu i wstrząsów, przystosowania się do nich i szybkiego powrotu do zdrowia). Rada wskazała na szereg dokumentów i rozwiązań instytucjonalnych

mających znaczenie, w tym także na współpracę Unii z NATO, zastrzegając, że współpraca ta ma odbywać się zgodnie z zasadami inkluzywności, wzajemności i autonomii procesu decyzyjnego Unii oraz zgodnie z Konkluzjami Rady wykonującymi Wspólną deklarację przewodniczącego Rady Europejskiej, Komisji Europejskiej i Sekretarza Generalnego NATO z 6 grudnia 2016 roku[52]

Rada podkreśliła też, że Ramy wspólnej odpowiedzi dyplomatycznej Unii Europejskiej powinny stanowić uzupełnienie dotychczasowych działań Unii w zakresie dyplomacji cyfrowej. Nadal mają być podejmowane wysiłki dyplomatyczne i działania operacyjne polegające na wspieraniu „szerszej zgodności (*compliance*) z istniejącym prawem międzynarodowym, w tym z Kartą Narodów Zjednoczonych" (w szczególności o przestrzeganie art. 2 pkt 4 – zakaz użycia siły, art. 33 – pokojowe rozstrzyganie sporów i art. 51 – prawo do indywidualnej lub zbiorowej samoobrony w odpowiedzi na atak zbrojny), z międzynarodowym prawem humanitarnym, czy takimi instrumentami prawnymi, jak Konwencja budapeszteńska w sprawie cyberprzestępczości, jak również ustalane wspólne stanowiska na forach międzynarodowych. Rada zapowiedziała także aktywne wspieranie GGE ONZ.

W Wytycznych wykonawczych Rada ukształtowała koncepcję środków unijnych skierowanych przeciwko szkodliwej działalności cyfrowej. Przywołano tutaj zasady określające reakcje Unii sformułowane przez Radę w Ramach wspólnej odpowiedzi dyplomatycznej. Rada przyjęła, że Ramy mają obejmować środki, które są odpowiednie do natychmiastowej reakcji na incydenty, a także „elementy, które powinny być wykorzystywane do zachęcania do współpracy, ułatwiania łagodzenia bezpośrednich i długoterminowych zagrożeń oraz wpływania na zachowanie potencjalnych agresorów w perspektywie długoterminowej". Z uwagi na zasadę równoległych kompetencji Unii i państw członkowskich w sferze WPZB środki wchodzące w zakres tej polityki, należy traktować jako „opcje do rozważenia". Nie wykluczają one działań, jakie mogą być podejmowane przez poszczególne państwa członkowskie ani działań koordynowanych między państwami członkowskimi.

Środki będące odpowiedzią Unii na szkodliwą działalność cyfrową bądź jej groźbę, które nie osiągają poziomu czynów międzynarodowo bezprawnych, ale są uznawane za działania nieprzyjazne, obejmują działania dyplomatyczne, polityczne oraz gospodarcze. Mogą być one stosowane wobec państwa lub aktora niepaństwowego bądź wobec działań pozostających w tranzycie przez terytorium państwa, jeżeli państwo to świadomie zezwala na wykorzystywanie swojego terytorium do takiej działalności lub świadomie ją wspiera.

52 Tekst: https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf. [dostęp: 03.09.2021].

Unia i jej państwa członkowskie mogą wykorzystywać pełny zestaw środków zawartych w Ramach, w tym środki restrykcyjne, w przypadku, gdy szkodliwa działalność cyfrowa jest prowadzona przez państwo, a także wówczas, gdy państwo jest uważane za odpowiedzialne za działania aktora niepaństwowego działającego pod jego kierownictwem lub kontrolą, lub jeżeli państwo to uznaje i przyjmuje zachowanie aktora niepaństwowego za własne. W przypadku państwa, które świadomie zezwala na wykorzystanie swojego terytorium do szkodliwej działalności cyfrowej, w tym czynów międzynarodowo bezprawnych z wykorzystaniem technologii informacyjno-komunikacyjnych, przeciwko państwu członkowskiemu lub Unii, środki zawarte w Ramach mogą zostać wykorzystane w celu skłonienia takiego państwa do zapewnienia, że jego terytorium nie jest wykorzystywane do takiej działalności. Przepisy dyrektywy w sprawie ataków na systemy informatyczne (2013/40/UE), w tym kary, miałyby zastosowanie również w przypadku przestępców nieposiadających znaczących powiązań ze sponsorem państwowym.

W Ramach ustalono, że Unia Europejska będzie odpowiadała na szkodliwą działalność cyfrową przy użyciu: 1) środków zapobiegawczych; 2) środków współpracy; 3) środków stabilności; 4) środków restrykcyjnych; 5) możliwego wsparcia Unii dla legalnych odpowiedzi państw członkowskich. Środki te mogą być stosowane niezależnie, sekwencyjnie lub równolegle jako część spójnego podejścia strategicznego na poziomie UE, zaprojektowanego i wdrożonego w celu wywarcia wpływu na konkretnego uczestnika, i powinny uwzględniać szerszy kontekst stosunków zewnętrznych UE oraz szersze podejście UE, które ma na celu wniesienie wkładu łagodzenia zagrożeń cyfrowych, zapobiegania konfliktom i większej stabilności w stosunkach międzynarodowych.

W odniesieniu do środków restrykcyjnych Rada stwierdziła, że Unia może je nałożyć na państwa trzecie, podmioty lub osoby fizyczne na podstawie decyzji Rady przyjętej na mocy art. 29 TUE w połączeniu z rozporządzeniem Rady uchwalonym na podstawie art. 215 TfUE. Rada zwróciła uwagę, że nałożenie sankcji ma odbywać się „zgodnie z odpowiednimi procedurami uzgodnionymi przez państwa członkowskie, określonymi w wytycznych w sprawie wdrażania i oceny środków restrykcyjnych (sankcji) w ramach WPZB". Przypomniała też, że sankcje „mają na celu spowodowanie zmiany polityki lub działań danego kraju docelowego, rządu, podmiotu lub danej osoby, zgodnie z celami określonymi w decyzji Rady". Mogą one obejmować np. zakazy podróżowania, embargo na broń, zamrożenie funduszy lub zasobów gospodarczych.

5. Ataki cyfrowe jako przesłanka stosowania sankcji Unii Europejskiej

Z punktu widzenia reagowania na ataki cyfrowe podstawowe znaczenie ma wyjaśnienie, czym one są. Tymczasem ani w analizowanych postanowieniach traktatowych dotyczących środków restrykcyjnych, ani

w dokumentach politycznych określających koncepcję dyplomacji cyfrowej nie sprecyzowano źródła cyfrowego (przyczyny) zastosowania sankcji. Uczyniła to dopiero Rada w decyzji o środkach restrykcyjnych z 2019 roku oraz tożsamym z nią w tym zakresie rozporządzeniu o sankcjach (art. 1 obu aktów). Tym niemniej w aktach tych nie definiuje się ataków cyfrowych jako takich, lecz tylko te, które powodują zastosowanie środków restrykcyjnych.

Art. 1 ust. 1 decyzji i rozporządzenia stanowią, że w polu ich działania znajdują się tylko takie ataki cyfrowe, które stanowią zewnętrzne zagrożenie dla Unii Europejskiej lub jej państw członkowskich oraz wywołują poważne skutki. Warunkowo (jeśli Rada tak postanowi) wchodzą w grę także ataki cyfrowe na państwa trzecie lub nawet organizacje międzynarodowe. Wchodzą w grę nie tylko czyny popełnione (ataki dokonane), ale także usiłowania popełnienia ataków cyfrowych. Zarazem nie są one tożsame z zagrożeniem atakami cyfrowymi.

Atakami cyfrowymi są tylko takie działania, które obejmują przynajmniej jedno z zachowań wymienionych w art. 1 ust. 3 w związku z art. 2 lit. b-d. Są to: 1) dostęp do systemów informacyjnych[53]; 2) ingerencja w systemy informacyjne („utrudnienie lub przerwanie funkcjonowania systemu informacyjnego przez wprowadzenie danych cyfrowych, przekazanie takich danych, ich uszkodzenie, usunięcie, pogorszenie ich jakości, ich zmianę lub wyeliminowanie bądź przez uczynienie ich niedostępnymi"); 3) ingerencja w dane („usunięcie, uszkodzenie, pogorszenie jakości, zmianę lub wyeliminowanie danych cyfrowych w systemie informacyjnym, bądź uczynienie ich niedostępnymi; obejmuje ona również kradzież danych, środków finansowych, zasobów gospodarczych lub praw własności intelektualnej"); 4) przechwytywanie danych („przechwycenie, za pomocą środków technicznych, niepublicznych przekazów danych cyfrowych do systemu informacyjnego, z systemu informacyjnego lub w ramach takiego systemu, w tym emisji elektromagnetycznych z systemu informacyjnego zawierających takie dane cyfrowe"). Są to zatem działania, a nie zaniechania działania (nie wchodzi w grę również przyzwolenie na działanie). W tym znaczeniu są to działania szkodliwe. Ponadto według art. 1 ust. 3 brane są pod uwagę tylko takie działania szkodliwe, które nie są prowadzone na podstawie należytego upoważnienia wydanego przez właściciela lub inny podmiot mający prawa do systemu lub

53 Według art. 2 lit. a), „systemy informacyjne" oznaczają urządzenie lub grupę wzajemnie połączonych lub powiązanych ze sobą urządzeń, z których przynajmniej jedno, zgodnie z programem, dokonuje automatycznego przetwarzania danych cyfrowych, jak również danych cyfrowych przechowywanych, przetwarzanych, wyszukiwanych lub przekazywanych przez to urządzenie lub tę grupę urządzeń, w celach eksploatacji, użycia, ochrony lub utrzymania tego urządzenia lub tej grupy urządzeń.

danych lub ich części lub nie są dozwolone na mocy prawa Unii lub danego państwa członkowskiego.

Chodzi więc jedynie o nielegalne działania szkodliwe.

W obu aktach wyjaśnia się też (ust. 2), że atakami stanowiącymi zagrożenie zewnętrzne są ataki, które:

a) zostały przygotowane poza terytorium Unii lub są przeprowadzane spoza terytorium Unii;
b) wykorzystują infrastrukturę znajdującą się poza terytorium Unii;
c) są przeprowadzane przez osobę fizyczną lub prawną, podmiot lub organ, które mają siedzibę lub prowadzą działalność poza terytorium Unii; lub
d) są przeprowadzane przy wsparciu, na zlecenie lub pod kontrolą osoby fizycznej lub prawnej, podmiotu lub organu, które prowadzą działalność poza terytorium Unii.

Przypadki te należy traktować alternatywnie, a nie kumulatywnie.

Definiując ataki cyfrowe jako przesłankę uruchomienia sankcji, decyzja i rozporządzenie rozróżniają ataki na państwa członkowskie i na Unię Europejską (ust. 4 i 5). Atak nie musi być przeprowadzany na wszystkie państwa członkowskie czy też każdy składnik struktury organizacyjnej Unii. Zarazem atakami stanowiącymi zagrożenie dla państw członkowskich są ataki na systemy informacyjne związane, między innymi, z infrastruktura krytyczną (łącznie z kablami podmorskimi oraz obiektami wystrzelonymi w przestrzeń kosmiczną) niezbędnymi do „utrzymania podstawowych funkcji społecznych lub zdrowia, bezpieczeństwa, ochrony i dobrobytu materialnego lub społecznego ludności", usługami należącymi do sektorów, które są niezbędne do utrzymania podstawowej działalności społecznej lub gospodarczej państwa (wymienia się tutaj energetykę, transport, bankowość, infrastrukturę rynków finansowych oraz zdrowia, zaopatrzenia w wodę pitną i jej dystrybucję, infrastrukturę cyfrową), bądź mają podstawowe znaczenie dla danego państwa, krytycznymi funkcjami państwa (dotyczy to zwłaszcza obrony, zarządzania instytucjami i ich funkcjonowania, procedury głosowania, funkcjonowania infrastruktury gospodarczej i cywilnej oraz bezpieczeństwa wewnętrznego lub zewnętrznego, w tym za pośrednictwem misji dyplomatycznych), przechowywaniem lub przetwarzaniem informacji niejawnych oraz rządowymi zespołami reagowania kryzysowego. Ataki stanowiące zagrożenie dla Unii Europejskiej pojmuje się jako ataki „przeciwko jej instytucjom, organom i jednostkom organizacyjnym, jej delegaturom w państwach trzecich lub w organizacjach międzynarodowych, jej operacjom i misjom w dziedzinie wspólnej polityki bezpieczeństwa i obrony (WPBiO) oraz jej specjalnym przedstawicielom".

Aby ataki cyfrowe spowodowały nałożenie sankcji muszą powodować poważne skutki. Decyzja i rozporządzenie nie wyjaśniają, o jakie skutki dokładnie chodzi, lecz dostarczają narzędzi, jak określić powagę skutków.

Art. 3 wymienia w tym zakresie siedem kryteriów, które należy traktować jako alternatywę nierozłączną. Wymienia on:

a) zakres, skalę, wpływ lub stopień spowodowanych zakłóceń m.in. działalności gospodarczej i społecznej, usług kluczowych, krytycznych funkcji państwa, porządku publicznego lub bezpieczeństwa publicznego;
b) liczbę osób fizycznych lub prawnych, podmiotów lub organów, których dotyczy atak cyfrowy;
c) liczbę państw członkowskich, których dotyczy atak cyfrowy;
d) wielkość poniesionych strat gospodarczych, na przykład w wyniku zakrojonej na szeroką skalę kradzieży środków finansowych, zasobów gospodarczych lub praw własności intelektualnej;
e) korzyść ekonomiczną odniesioną przez sprawcę dla siebie lub dla innych osób;
f) ilość lub charakter ukradzionych danych lub skalę naruszenia ochrony danych; lub
g) charakter poufnych danych handlowych, do których uzyskano dostęp.

Z wyliczenia tego można wywnioskować, że, podając kryteria określania powagi skutków ataku cyfrowego, legislator unijny przyjął zasadniczo cztery wskazówki odnoszące się do: 1) wyrządzenia szkód majątkowych lub gospodarczych/uzyskania korzyści gospodarczych; 2) skali i stopnia oddziaływania czynu; 3) liczby poszkodowanych: 4) wagi i charakteru dóbr chronionych.

6. Środki restrykcyjne jako instrument Unii Europejskiej ataki cyfrowe

Środki restrykcyjne są instrumentami służącymi zapobieganiu lub odstraszaniu ataków cyfrowych pochodzących spoza Unii Europejskiej (zewnętrzne ataki cyfrowe) skierowanych przeciwko Unii lub jej państwom członkowskim oraz reagowaniu na takie ataki. Mogą mieć zatem działanie prewencyjne i/lub represyjne.

Decyzja i rozporządzenie ustanawiające środki restrykcyjne określają też rodzaje sankcji, jakie mogą być zastosowane w razie ataku cyfrowego. Jednak inaczej niż w przypadku pojmowania ataków cyfrowych, nie są one w tym zakresie regulacją jednolitą. Decyzja obejmuje bowiem w art. 4 i 5 sankcje związane z przepływem osób fizycznych (wjazd, tranzyt przez terytoria państw członkowskich), sankcje finansowe i gospodarcze (zamrożenie środków finansowych/funduszy [ang./fr. *funds*, *fonds*] i zasobów gospodarczych). Tymczasem rozporządzenie, jako akt oparty na art. 215 TfUE, dotyczy jedynie stosowanie sankcji finansowych i gospodarczych (art. 3). Ani decyzja, ani rozporządzenie nie przewidują środków restrykcyjnych wobec państw. Regulują zatem jedynie środki celowane. W obydwu aktach, zgodnie z polityką unijną, przewiduje się różnorodne wyłączenia spod działania

sankcji. Ujęcie to nie odbiega zatem od sankcji stosowanych również w innych przypadkach niż ataki cyfrowe.

Środki restrykcyjne dotyczące wjazdu i tranzytu dotyczą jedynie osób fizycznych, w zasadzie cudzoziemców i bezpaństwowców (art. 4 ust. 2 stanowi, że nie ma obowiązku odmowy wjazdu w stosunku do własnych obywateli; rozwiązanie to może jednak budzić wątpliwości z perspektywy zakazu banicji przewidzianego w prawie międzynarodowym praw człowieka). Mają to być osoby odpowiedzialne za przeprowadzenie lub usiłowanie przeprowadzenia ataków cyfrowych oraz osoby, które „zapewniają finansowe, techniczne lub materialne wsparcie dla ataków cyfrowych lub usiłowania przeprowadzenia ataków cyfrowych, bądź też w inny sposób angażują się w takie ataki, w tym przez ich planowanie, przygotowywanie, uczestnictwo w nich, kierowanie nimi, pomoc w nich lub zachęcanie do takich ataków lub ułatwianie ich poprzez działanie lub zaniechanie", jak również osoby z nimi związane. Z sankcji tych wyłączone są jednak osoby, które korzystają z ochrony wynikającej z zobowiązań międzynarodowych państwa członkowskiego (m.in. w związku z goszczeniem organizacji międzynarodowej i OBWE, organizowaniem konferencji międzynarodowej, korzystające z międzynarodowych przywilejów i immunitetów – ust. 3 i 4; wyłączenia *ex lege*). Ponadto, państwa członkowskie mogą przyznawać wyłączenia spod działania sankcji w niektórych przypadkach (podróż uzasadniona pilną potrzebą humanitarną lub udziałem „w posiedzeniach międzyrządowych lub popieranych przez Unię lub których gospodarzem jest Unia lub dane państwo członkowskie sprawujące przewodnictwo w OBWE, gdzie prowadzony jest dialog polityczny bezpośrednio propagujący polityczne cele środków ograniczających, w tym zapewnienie bezpieczeństwa i stabilności przestrzeni cyfrowej" bądź w związku z udziałem w postępowaniu sądowym – ust. 6 i 7, wyłączenia fakultatywne[54]). W razie zastosowania wyłączenia, wjazd lub przejazd przez terytorium państwa członkowskie są ściśle ograniczone do celu ich przyznania i do osób, których dotyczą (ust. 9).

Sankcje finansowe i gospodarcze mogą być skierowane przeciwko osobom fizycznym, prawnym, jednostkom lub ciałom (ang./fr. *entities or bodies*/*entités ou organismes*), które: 1) są odpowiedzialne za przeprowadzenie lub próby przeprowadzenia ataków cyfrowych; 2) zapewniają finansowe, techniczne lub materialne wsparcie dla ataków cyfrowych lub w celu usiłowania przeprowadzenia ataków cyfrowych, bądź też w inny sposób angażują się w takie ataki (np. przez planowanie, przygotowywanie, udział, kierownictwo, pomoc

54 W ich przypadku decyzja nakazuje stosowanie procedury powiadamiania Rady. Członkowie Rady mogą jednak wnieść sprzeciw w ciągu dwóch dni roboczych od daty otrzymania powiadomienia. Wówczas decyzję ostateczną o wyłączeniu podejmuje Rada, stanowiąc większością kwalifikowaną głosów (ust. 8).

lub zachęcanie do ataków lub ułatwianie ich popełnienia przez działanie lub zaniechanie); 3) są powiązane z podmiotami, o których mowa w punktach 1 i 2 (art. 5 ust. 1 decyzji, art. 3 ust. 3 rozporządzenia).

Środki finansowe i gospodarcze przybierają postać zamrożenia funduszy i zasobów gospodarczych. Decyzja nie zawiera przy tym definicji zamrożenia funduszy i zasobów gospodarczych. Odpowiednie objaśnienia ujęto w rozporządzeniu. Przez fundusze (środki finansowe) rozumie się aktywa finansowe i wszelkiego rodzaju korzyści finansowe (np. gotówkę, czeki, roszczenia pieniężne, depozyty, długi i zobowiązania, papiery wartościowe i dłużne, odsetki, dywidendy czy inne przychody z aktywów, kredyty, gwarancje, akredytywy, konosamenty, umowy sprzedaży). Z kolei zasoby gospodarcze oznaczają „aktywa wszelkiego rodzaju, rzeczowe i niematerialne, ruchome i nieruchome, które nie są środkami pieniężnymi, ale mogą być użyte do pozyskania środków pieniężnych, towarów lub usług" (art. 1 ust. 8 lit. d, g).

Rozporządzenie odrębnie definiuje zamrożenie środków finansowych i zasobów gospodarczych. Pierwsze z nich oznacza „zapobieganie wszelkim ruchom tych środków, ich przenoszeniu, zmianom, wykorzystaniu, udostępnianiu lub dokonywaniu nimi transakcji w jakikolwiek sposób, który powodowałby jakąkolwiek zmianę ich wielkości, wartości, lokalizacji, własności, posiadania, charakteru lub przeznaczenia lub każdą inną zmianę, która umożliwiłaby korzystanie z nich, w tym zarządzanie portfelem", drugie „uniemożliwienie wykorzystania zasobów gospodarczych do uzyskiwania środków pieniężnych, towarów lub usług w jakikolwiek sposób, między innymi przez ich sprzedaż, wynajem lub obciążenie hipoteką" (ust. 8 lit. e, f). Środki i zasoby się zamraża i ich nie udostępnia bezpośrednio czy pośrednio podmiotom podlegającym restrykcjom (art. 5 ust. 2 decyzji, art. 3 ust. 2 rozporządzenia)[55]. Zamrożenie może dotyczyć tylko takich środków

55 Jak stanowią art. 5 ust. 6 decyzji i art. 7 ust. 2, zasady nieudostępniania środków lub zasobów nie stosuje się do niektórych dodatkowych kwot na zamrożonych rachunkach bankowych (odsetek i innych dochodów z rachunków, płatności należnych z tytułu umów, porozumień i zobowiązań sprzed daty nałożenia sankcji, płatności wynikających z orzeczeń sądowych, decyzji administracyjnych lub orzeczeń arbitrażowych wydanych w Unii lub w niej wykonywanych), pod warunkiem, że pozostają zamrożone. To samo dotyczy zasilania zamrożonych rachunków przez instytucje finansowe lub kredytowe, które otrzymały środki od osób trzecich (art. 7 ust. 1 rozporządzenia). Ponadto możliwe są płatności z tytułu zawartych przed datą nałożenia środków restrykcyjnych umów lub porozumień, których stroną jest podmiot obłożony sankcjami, jeśli zapewni się, że płatność nie jest dokonywana na rzecz podmiotu objętego sankcjami (art. 5 ust. 5 decyzji, art. 6 rozporządzenia; przepisy te nie są identyczne).

lub zasobów, które należą lub są własnością albo w posiadaniu lub pod kontrolą podmiotów objętych sankcjami (art. 5 ust. 1 decyzji z 2020 r., art. 3 ust. 1 rozporządzenia).

Decyzja i rozporządzenie dopuszczają odstępstwa od działania sankcji finansowych i gospodarczych. Są to wyłączenia fakultatywne, co oznacza, że państwa członkowskie mogą, lecz nie muszą ich stosować. Polegają one na odblokowaniu niektórych zamrożonych środków lub zasobów bądź na ich udostępnieniu pod warunkiem spełnienia kryteriów określonych w decyzji i rozporządzeniu (art. 5 ust. 3 decyzji, art. 4 rozporządzenia). Kryteria te są w obu aktach tożsame. A zatem odstępstwo może być przyznane, gdy środki lub zasoby są: 1) niezbędne do zaspokojenia podstawowych potrzeb podmiotów objętych sankcjami oraz członków rodzin pozostających na utrzymaniu osób fizycznych poddanych restrykcjom (np. koszty żywności, najmu lub kredytu hipotecznego, leków i leczenia, zapłata podatków, składek ubezpieczeniowych oraz opłat za usługi użyteczności publicznej); 2) służą wyłącznie pokryciu uzasadnionych kosztów honorariów lub zwrotów poniesionych wydatków związanych z usługami prawniczymi; 3) służą wyłącznie pokryciu opłat lub należności za usługi polegające na zwykłym przechowywaniu lub utrzymywaniu zamrożonych środków lub zasobów; 4) niezbędne do pokrycia nadzwyczajnych wydatków (o ile właściwy organ powiadomił właściwe organy innych państw członkowskich i Komisję o powodach, dla których uważa, że należy udzielić szczególnego zezwolenia, co najmniej dwa tygodnie przed udzieleniem); 5) wpłacone na rachunek lub wypłacone z rachunku misji dyplomatycznej lub misji konsularnej lub organizacji międzynarodowej posiadającej immunitet na mocy prawa międzynarodowego, w zakresie, jakim płatności te są przeznaczone na oficjalne cele tej misji dyplomatycznej lub misji konsularnej lub organizacji międzynarodowej.

Ponadto państwa członkowskie mogą zezwolić na odblokowanie zamrożonych środków finansowych lub zasobów gospodarczych, gdy: 1) środki lub zasoby są przedmiotem orzeczenia arbitrażowego wydanego przed datą zastosowania sankcji, bądź orzeczenia sądowego lub decyzji administracyjnej wydanych w Unii, albo orzeczenia sądowego podlegającego wykonaniu w danym państwie członkowskim, przed tą datą lub po tej dacie; 2) środki lub zasoby zostaną wykorzystane wyłącznie w celu zaspokojenia roszczeń zabezpieczonych takim orzeczeniem lub decyzją albo uznanych w nich za zasadne (jednak w granicach określonych przez mające zastosowanie przepisy prawne regulujące prawa osób, którym takie roszczenia[56] przysługują); 3) orzeczenie lub decyzja nie przynoszą korzyści podmiotowi obłożonemu sankcjami; 4) uznanie tego orzeczenia lub tej decyzji nie jest sprzeczne z porządkiem publicznym danego państwa członkowskiego. Wszystkie te przesłanki muszą

56 Zob. też art. 1 ust. 8 lit. a rozporządzenia, gdzie znajduje się definicja roszczenia.

być spełnione łącznie. W przypadku przyznania odstępstw pierwszego czy drugiego rodzaju państwa członkowskie muszą powiadamiać pozostałe państwa członkowskie i Komisję.

Zgodnie z art. 9 rozporządzenia, zakazuje się świadomego i umyślnego udziału w działaniach, których celem lub skutkiem jest obejście środków restrykcyjnych przewidzianych w tym akcie.

7. Zasady i mechanizm stosowania i wykonywania środków restrykcyjnych wobec ataków cyfrowych

W decyzji i rozporządzeniu o sankcjach określa się tryb nakładania środków restrykcyjnych. Decyzja ani rozporządzenie nie nakładają bowiem *per se* tych środków. Nałożenie sankcji odbywa się przez wpisanie danego podmiotu na listę znajdującą się w załączniku do decyzji i rozporządzenia z 2019 roku. Odbywa się to na mocy decyzji zamieniającej i rozporządzenia wykonawczego Rady przyjmowanych w obydwu przypadkach na podstawie projektu państwa członkowskiego lub Wysokiego Przedstawiciela ds. Zagranicznych i Polityki Bezpieczeństwa. To właśnie nastąpiło w 2020 roku, kiedy to Rada uchwaliła decyzję zmieniającą 2020/1127 i rozporządzenie wykonawcze 2020/1125. W tym samym trybie odbywa się zmiana środków restrykcyjnych bądź ich uchylenie. Akty nakładające sankcje ustalają przy tym jedynie treść załącznika do decyzji i rozporządzenia o środkach restrykcyjnych.

Akty nakładające sankcje precyzują w załącznikach listę podmiotów oraz uzasadnienie ich umieszczenia na liście. Załączniki zawierają informacje niezbędne do zidentyfikowania danego podmiotu (o ile są dostępne). Zgodnie z art. 7 ust. 2 decyzji i art. 14 rozporządzenia, „W przypadku osób fizycznych informacje takie mogą obejmować imiona i nazwiska, w tym pseudonimy, datę i miejsce urodzenia, obywatelstwo, numery paszportu i dokumentu tożsamości, płeć, adres, jeśli jest znany, a także stanowisko lub zawód. W przypadku osób prawnych, podmiotów lub organów informacje takie mogą obejmować nazwy, miejsce i datę wpisu do rejestru, numer w rejestrze i miejsce prowadzenia działalności".

Decyzja w sprawie nałożenia środków restrykcyjnych jest przekazywana przez Radę wraz z uzasadnieniem umieszczenia na liście podmiotom objętym sankcjami, umożliwiając im przedstawienie uwag. Jeśli takie uwagi zostaną zgłoszone lub przedstawione zostaną nowe istotne dowody Rada ma obowiązek dokonania przeglądu decyzji, informując o tym zainteresowane podmioty (art. 6 decyzji i art. 7 ust. 1-3 rozporządzenia).

Decyzja i rozporządzenie w sprawie środków restrykcyjnych wymagają działania implementacyjnego ze strony państw członkowskich. W szczególności w rozporządzeniu zobowiązuje się je do przyjmowania przepisów dotyczących sankcji i wszelkich środków koniecznych do ich implementacji. Oczekuje się, że sankcje będą skuteczne, proporcjonalne i odstraszające.

Podobnie jak dyrektywy, rozporządzenie o środkach restrykcyjnych wymaga od państw członkowskich, aby po wejściu w życie rozporządzenia notyfikowały Komisji przepisy implementujące, a później także ich zmiany mające na nie wpływ (art. 15). Zgodnie z rozporządzeniem, państwa członkowskie mają też obowiązek wskazania organów odpowiedzialnych za wykonanie rozporządzenia (art. 17; ich wykaz znajduje się w załączniku II do rozporządzenia i może być zmieniany przez Komisję – art. 13 ust. 5). Na podstawie art. 12, Komisja i państwa członkowskie informują się wzajemnie o środkach wykonujących rozporządzenie, a także wszelkich innych istotnych i dostępnych informacjach związanych z rozporządzeniem (dotyczy to zwłaszcza funduszy zamrożonych na mocy rozporządzenia oraz „naruszeń przepisów i trudności z ich egzekwowaniem oraz orzeczeń wydanych przez sądy krajowe"; ust. 1). Państwa członkowskie są też zobowiązane do niezwłocznego przekazania sobie wzajemnie oraz Komisji wszelkich innych dostępnych im istotnych informacji mogących mieć wpływ na skuteczne wykonanie rozporządzenia (ust. 2).

W przypadku, gdy sankcje finansowe i gospodarcze wykonują osoby fizyczne lub prawne, jednostki lub ciała, które działają w dobrej wierze w oparciu o przekonanie, że działanie takie jest zgodne z rozporządzeniem, nie będą one (dotyczy to także członków zarządu lub pracowników osobny prawnej, jednostki lub ciała) ponosiły odpowiedzialności jakiegokolwiek rodzaju, chyba że dokonując zamrożenia środków/zasobów dopuściły się niedbalstwa. Podmioty te nie będą odpowiedzialne, jeżeli nie wiedziały i nie miały uzasadnionego powodu do przypuszczenia, że ich działania mogą naruszyć środki określone w rozporządzeniu (art. 10). Nie zaspakaja się też roszczeń wynikających z umów lub transakcji[57], których wykonywanie zostało zakłócone, bezpośrednio lub pośrednio, w całości lub części, przez środki nałożone niniejszym rozporządzeniem, jeżeli roszczenia te zostały wniesione przez podmioty objęte sankcjami lub inne podmioty działające za pośrednictwem lub w imieniu tych podmiotów. Ciężar dowodu spoczywa na podmiocie dochodzącym roszczeń (art. 11).

Na mocy rozporządzenia zostają również nałożone pewne obowiązki informacyjne (chodzi o informacje, które ułatwiłyby zachowanie zgodności z rozporządzeniem, np. informacje dotyczące rachunków lub kwot zamrożonych) i obowiązki współpracy (z właściwymi organami państwa członkowskiego) na osoby fizyczne, prawne, jednostki i ciała. Komisja została przy tym zobowiązana do ich udostępniania państwom członkowskim (art. 8).

W decyzji dodatkowo zachęca się państwa trzecie, aby przyjmowały sankcje podobne do przewidzianych w decyzji (art. 9).

57 Zob. też art. 1 ust. 8 lit. b rozporządzenia, gdzie znajduje się definicja umów i transakcji.

Kontrola sądowa środków restrykcyjnych zwłaszcza w formie decyzji zmieniających i rozporządzeń wykonawczych odbywa się na zasadach ogólnych. Możliwe jest zatem ich zaskarżenie w trybie art. 263 TfUE (legalność aktu), a także wnoszenie skarg odszkodowawczych.

Decyzja zmieniająca i rozporządzenie wykonawcze z 2020 roku są pierwszymi aktami prawnymi Unii nakładającymi sankcje w odpowiedzi na ataki cyfrowe. U ich podłoża znalazło się szkodliwe użycie technologii informacyjno-komunikacyjnych, które miało miejsce jeszcze w latach 2015, 2016, a zwłaszcza w 2018 roku. Działalność ta nie miała charakteru jednorazowego. Jednak nie ustawała, mimo wezwań ze strony Unii Europejskiej. Polegała ona w szczególności na atakach znanych jako „WannaCry"[58], „NotPetya"[59], „Operation Cloud Hopper"[60], które, jak to się podkreśla w preambułach obu aktów, wyrządziły znaczne szkody i straty gospodarcze w Unii i poza nią. Stworzyły też niebezpieczeństwo podważenia funkcjonowania Organizacji ds. Zakazu Broni Chemicznej (OPCW) w Niderlandach. Unia uznała, że ataki te mają na celu naruszenie integralności, bezpieczeństwa i gospodarczej konkurencyjności Unii i łączą się z kradzieżą praw własności intelektualnej (identyfikuje się podmiot znany jako „Advanced Persistent

58 »WannaCry« zakłócił systemy informacyjne na całym świecie poprzez uderzenie w systemy informacyjne za pomocą oprogramowania typu ransomware i blokowanie dostępu do danych. Wpłynął on na systemy informacyjne przedsiębiorstw w Unii, w tym systemy informacyjne związane z usługami niezbędnymi do utrzymania podstawowych usług i działalności gospodarczej w państwach członkowskich. Atak ten został przeprowadzony przez podmiot znany jako „APT38" („Advanced Persistent Threat 38") lub „grupa Lazarus".

59 „NotPetya" lub „EternalPetya" spowodowały brak dostępności danych w wielu przedsiębiorstwach w Unii, szerzej w Europie i na całym świecie poprzez uderzenie w komputery za pomocą oprogramowania typu ransomware i zablokowanie dostępu do danych, co doprowadziło między innymi do znacznych strat gospodarczych. Cyberatak na ukraińską sieć elektroenergetyczną spowodował wyłączenie jej części zimą. Autorem ataku był podmiot znany jako „Sandworm"

60 „Operation Cloud Hopper" była skierowana przeciwko systemom informacyjnym przedsiębiorstw wielonarodowych na sześciu kontynentach, w tym przedsiębiorstw mających siedzibę w Unii, oraz uzyskała nieuprawniony dostęp do danych wrażliwych pod względem handlowym, powodując znaczne straty gospodarcze.

Threat 10"). Wymienione działania zostały potępione przez Radę w konkluzjach z 16 kwietnia 2018 roku[61]

Na mocy decyzji zmieniającej sankcjami objęto dwóch Chińczyków zaangażowanych w atak cyfrowy dokonany przez APT10 „Operation Cloud Hopper" (Gao Qian – powiązanie z atakiem przez użytą infrastrukturę, zatrudnienie w Huaying Haitai i powiązania z drugim Chińczykiem objętym sankcjami, Zhang Shilong – powiązanie z atakiem przez opracowanie i testowanie złośliwego oprogramowania użytego w ataku, zatrudnienie w Huaying Haitai) oraz czterech Rosjan, którzy podjęli atak cyfrowy na Organizację ds. Zakazu Broni Chemicznej (A. V. Minin, A. S. Mortenets, E. M. Serebriakov, O. M. Sotnikov – należeli do zespołu wywiadu GRU, który podjął próbę nieuprawnionego dostępu do sieci Wi-Fi w OPCW). Ponadto środki restrykcyjne zastosowano wobec kilku osób prawnych, jednostek i ciał: Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai; Chiny – powiązanie z atakami cyfrowymi przez zatrudnienie osób fizycznych objętych sankcjami), Chosun Expo (KRLD; powiązanie z atakiem „WannaCry" m.in. przez konta wykorzystywane do ataków; ponadto podmiot ten podjął atak na polską Komisję Nadzoru Finansowego i Sony Pictures Entertainment, a także dokonał kradzieży w przestrzeni cyfrowej z Bangladesh Bank i próby kradzieży z Vietnam Tien Phong Bank), Główny Ośrodek Specjalnych Technologii (GTsST) Głównego Zarządu Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GU GRU; Rosja).

Nowe sankcje związane z atakami cyfrowymi Rada przyjęła na podstawie decyzji zmieniającej 2020/1537[62] i rozporządzenia wykonawczego 2020/1536 z 22 października 2020 roku[63], dodając do dotychczasowej listy dwóch Rosjan (D. S. Badin, I. O. Kostyukov) i jedno ciało (Główny Ośrodek Służb Specjalnych (GTsSS) Głównego Zarządu Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GU GRU)) w związku z atakami na niemiecki Bundestag w kwietniu i maju 2015 roku, a także w kwietniu 2018 roku na OPCW (drugi z Rosjan i GTsSS)[64]. Atak miał wpływ na funkcjonowanie tej instytucji przez kilka dni. Skradziono dużą ilość danych; atak ten miał także wpływ na konta poczty elektronicznej kilku parlamentarzystów, w tym

61 Konkluzje w sprawie szkodliwej działalności cyfrowej, doc. 7925/18. https://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/en/pdf. [dostęp: 3.9.2021].

62 Dz. Urz. UE z 22.10.2020 r., LI 351, s. 5

63 Dz. Urz. UE z 22.10.2020 r., LI 351, s. 1.

64 Zob. Malicious cyber-attacks: EU sanctions two individuals and one body over 2015 Bundestag hack. https://www.consilium.europa.eu/en/press/press-releases/2020/10/22/malicious-cyber-attacks-eu-sanctions-two-individuals-and-one-body-over-2015-bundestag-hack/. [dostęp: 3.9.2021].

kanclerz Angeli Merkel. Wreszcie mocą decyzji zmieniającej 2020/1748[65] i rozporządzenia wykonawczego Rady (UE) 2020/1744 z 20 listopada 2020 roku[66] dokonano uściśleń związanych z sankcjami wobec Gao Qiang i Zhang Shilong.

8. Konkluzje

Unia Europejska podejmuje różnorodne odpowiedzi na szkodliwą działalność cyfrową. Są to działania z zakresu WPZB, a także spoza niej (harmonizujące odpowiednie krajowe regulacje karne bądź administracyjne). W przypadku zewnętrznych ataków cyfrowych kluczowe są środki podejmowane w ramach narzędzi dyplomacji cyfrowej. Jednym z nich są sankcje. Co do istoty środki restrykcyjne nie odbiegają przy tym od tych, które są stosowane i kontrolowane na zasadzie powszechnej. Wyróżnikiem jest zatem atak cyfrowy jako przyczyna nałożenia sankcji.

Dotychczasowa praktyka sankcyjna Unii Europejskiej w stosunku do ataków cyfrowych nie jest zbyt bogata. Trudno też jeszcze ocenić ich efektywność. Można jednak sformułować kilka ocen dotyczących ukształtowania środków restrykcyjnych stosowanych w przypadku ataku cyfrowego.

Po pierwsze, można zwrócić uwagę, że reakcja sankcyjna Unii Europejskiej została opracowana z jednej strony jako reżim tymczasowy, tzn. decyzja i rozporządzenie stanowiące podstawę nakładania restrykcji obowiązują jedynie czas określony, stosunkowo krótki, który może być jednak przedłużany. Nie sprzyja to stabilizacji stosowania sankcji. Z drugiej strony regulacje sankcyjne, a zwłaszcza decyzja z 2019 roku, stanowią swoiste obejście zakazu stanowienia aktów legislacyjnych w ramach WPZB. Nie ulega wątpliwości, że ich treść ma charakter legislacyjny. Jedynymi elementami mającymi wykluczyć kwalifikacje jako aktu legislacyjnego są czasowy charakter decyzji oraz umożliwienie uruchomienia listy indywidualizującej sankcje w załączniku (stąd decyzje są zmieniane, a nie wykonywane). Regulacji unijnych nie osadzono też wystarczająco w całokształcie reakcji na ataki cyfrowe[67].

Po drugie, rozwiązanie polegające na tym, że istnieją akty podstawowe mające faktycznie lub formalnie charakter legislacyjny, a decyzje zmieniające i rozporządzenia wykonawcze zmieniają jedynie ich załącznik I powoduje, że wbrew założeniom dyplomacji cyfrowej nie daje się zrelatywizować sankcji (bardziej ich ukierunkować) w zależności od adresata i okoliczności

65 Dz. Urz. UE z 23.11.2020 r., L 393, s. 19.

66 Dz. Urz. UE z 23.11.2020 r., L 393, s. 1.

67 Zob. Erica Moret, Patryk Pawlak, „The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?, Brief", *European Union Institute for Security Studies*, nr 24 (2017): 3. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf. [dostęp: 3.9.2021].

przypadku. Ramy wspólnej odpowiedzi dyplomatycznej i Wytyczne do nich dodane wskazują, że należy niuansować przypadki, zgodnie z zasadą proporcjonalności. Środki restrykcyjne muszą być stosowane jako całe pakiety, podczas gdy z art. 215 TfUE nie wynika jednoznacznie, że muszą one działać łącznie jako środki finansowe i gospodarcze.

Po trzecie, decyzja i rozporządzenie nie przewidują stosowania restrykcji wobec państw. Tymczasem ataki cyfrowe mogą być wynikiem ogólniejszej taktyki stosowanej przez nieprzyjazne Unii, jej członkom i sojusznikom państwa trzecie. Nie chodzi przy tym o to, że w dotychczasowej praktyce nie zaszły takie przypadki, lecz że nie wprowadzono możliwości stosowania sankcji wobec ataków cyfrowych o szerszym charakterze, zwłaszcza gdy są stosowane z inspiracji organów państwa.

Po czwarte, wątpliwe wydaje się nakładanie sankcji jedynie na jednostki lub ciała stanowiące strukturę aparatu państwowego czy nawet osoby tam zatrudnione. Najczęściej są to bowiem wykonawcy działań, o których zachowaniach zadecydowano w innym miejscu aparatu władzy. Uwaga ta nie koliduje z faktem, że zasadnie odróżnia się sankcje od ustalenia państwa odpowiedzialnego za czyn międzynarodowo bezprawny w rozumieniu prawa międzynarodowego.

Po piąte, nie jest właściwe ograniczanie sankcji finansowych i gospodarczych jedynie do zamrożenia funduszy czy zasobów gospodarczych. Te bowiem mogą być poza zasięgiem efektywnego oddziaływania Unii. Ponadto w decyzji i rozporządzeniu z 2020 roku nie uwzględnia się innych rodzajów sankcji, o których mowa np. w Wytycznych do Ram. Można też wywodzić, że z punktu widzenia efektywnego zapobiegania i reagowania na ataki cyfrowe pożądane byłoby wprowadzenie sankcji na państwa lub inne podmioty w postaci embarga na zakupy oprogramowania, które może być wykorzystywane do ataków, czy też zaawansowanych elementów infrastruktury internetowej (ewentualnie służących do ich wytwarzania), zwłaszcza gdy wchodzą w grę mocne ataki cyfrowe czy też ataki o charakterze uporczywym.

Po szóste, w decyzji i rozporządzeniu nie ma wystarczającego powiązania środków restrykcyjnych z gwarancjami proceduralnymi, o których mowa w art. 215 TfUE, a także w Ramach i Wytycznych do Ram. Owszem, mówi się o obowiązku informowania adresatów sankcji, prawie do wnoszenia uwag i obowiązku dokonania przeglądu środków restrykcyjnych, ale nie wydaje się to wystarczające, biorąc pod uwagę dotychczasowe orzecznictwo Trybunału Sprawiedliwości dotyczące kontroli poszanowania praw podstawowych w przypadku stosowania sankcji[68].

68 Zob. np. M. Niedźwiedź, komentarz do art. 215 TfUE, s. 1551 i n.; Eeckhout, *EU External Relations Law*, 511 i n.

Bibliografia

Antczak Anna, Role międzynarodowe Unii Europejskiej. Aspekty teoretyczne. Warszawa WizjaPress and IT, 2012.

Dobrzeniecki Karol, *Lex informatica*. Toruń: TNOiK, 2008.

Dyplomacja cyfrowa jako instrument polityki zagranicznej XXI wieku, red. Marcin Kosienkowski, Beata Piskorska. Lublin: Wydawnictwo KUL, 2014.

Dyplomacja czy siła? Unia Europejska w stosunkach międzynarodowych, red. Stanisław Parzymies. Warszawa: Wydawnictwo Naukowe Scholar, 2009.

Eeckhout Piet, *EU External Relations Law*. Oxford: OUP, 2011.

Eichenseher Kristen. E., „The Cyber-Law of Nations" *The Georgetown Law Journal*, nr 2 (2015): 317-380.

EU Law After Lisbon, red. Andrea Biondi, Piet Eeckhout, Stefanie Ripley. Oxford: OUP, 2012.

European Foreign Policy. Legal and Political Perspectives, red. Panos Koutrakos. Chltenham-Northampton: E. Elgar Publ., 2011.

European Union Treaties. A Commentary, red. Rudolf Geiger, Daniel-Erasmus Khan, Markus Kotzur. München-Oxford: C. H. Beck-Hart, 2015.

Le droit des relations extérieures de l'Union européenne après le Traité de Lisbonne, red. Anne-Sophie Lamblin-Gourdin, Eric Mondielli. Bruxelles : Éditions É. Bruylant, 2013.

Mik Cezary, *Media masowe w europejskim prawie wspólnotowym*. Toruń: TNOiK, 1999.

Mik Cezary, Władysław Czapliński, *Traktat o Unii Europejskiej. Komentarz*. Warszawa: Wydawnictwo ABC, 2005.

Moret Erica, Patryk Pawlak, „The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?" *Brief, European Union Institute for Security Studies*, nr 24 (2017): 1-4.

Peacetime Regime for State Activities in Cyberspace. International Law, International relations and Diplomacy, red. Katharina Ziolkowski. Talin: NATO CCD COE Publ., 2013.

Piris Jean-Claude, *The Lisbon Treaty. A Legal and Political Analysis*, Cambridge CUP, 2010.

Polityka zagraniczna Unii Europejskiej. Prawo i praktyka, red. Jan Galster, Anna Szczerba-Zawada. Warszawa: Instytut Wydawniczy EuroPrawo, 2016.

Research Handbook on International Law and Cyberspace, red. Nicholas Tsagourias, Russell Buchan. Cheltenham-Northampton: Edward Elgar Publishing, 2015.

Ryszka Joanna, *Sankcje gospodarcze wobec podmiotów zewnętrznych w prawie i praktyce Unii Europejskiej* (Toruń: TNOiK, 2008).

Talinn Manual 2.0 on the International Law Applicable to Cyber Operations, red. Michael N. Schmitt. Cambridge: CUP, 2017.

Traktat o funkcjonowaniu Unii Europejskiej, red. Andrzej Wróbel, t. I (art. 1-89), red. Dawid Miąsik, Nina Półtorak. Warszawa: Wolters Kluwer, 2012.

Traktat o funkcjonowaniu Unii Europejskiej, red. Andrzej Wróbel, t. II (art. 90-222), red. Krystyna Kowalik-Bańczyk, Monika Szwarc-Kuczer, Warszawa: Wolters Kluwer, 2012.

Worona Joanna, *Cyberprzestrzeń a prawo międzynarodowe*. Warszawa: Wolters Kluwer, 2020.

Wpływ internetu na ewolucję państwa i prawa, red. Radosław Grabowski, Rzeszów: Wydawnictwo Uniwersytetu Rzezowskiego, 2008.