Filip Radoniewicz*

Zwalczanie cyberterroryzmu w ramach UE – wybrane aspekty karnomaterialne

Streszczenie

Celem artykułu jest przedstawienie postanowień aktów prawa unijnego dotyczących prawa karnego materialnego. Cyberterroryzm nie doczekał się odrębnej regulacji. Nie oznacza to oczywiście, że unormowanie tej problematyki nie istnieje. Jest ona po prostu rozproszona i żeby odtworzyć regulację odpowiedzialności karnej za czyny, które można zakwalifikować jako cyberterroryzm, czyli przestępstw o charakterze cyberterrorystycznym, należy sięgnąć do dwóch aktów prawa unijnego: dyrektywy Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępującej decyzję ramową Rady 2002/475/WSiSW oraz zmieniającej decyzję Rady 2005/671/WSiSW oraz dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne i uchylającej decyzję ramową Rady 2005/222/WSiSW. Stąd niniejszy artykuł składa się z dwóch części: pierwszej dotyczącej dyrektywy 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu oraz drugiej, której przedmiotem jest dyrektywa 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne.

Słowa kluczowe: prawo karne, cyberprzestępczość, terroryzm, dyrektywa 2017/541, dyrektywa 2013/40

* Dr Filip Radoniewicz, Instytut Prawa, Wydział Bezpieczeństwa Narodowego, Akademia Sztuki Wojennej w Warszawie, e-mail: f.radoniewicz@akademia.mil.pl, ORCID: 0000-0002-7917-4059.

Terroryzm

Termin „terroryzm" pochodzi od łacińskiego słowa *terror*, oznaczającego „stosowanie przemocy, gwałtu, okrucieństwa w celu zastraszenia, zniszczenia przeciwnika[1]". W języku potocznym rozumiany jest jako „stosowanie terroru, zwłaszcza działalność niektórych ugrupowań ekstremistycznych, usiłujących za pomocą zabójstw politycznych, porwań zakładników, porwań samolotów i podobnych środków zwrócić uwagę opinii publicznej na wysuwane przez siebie hasła lub wymusić na rządach państw określone ustępstwa bądź świadczenia na swoją korzyść[2]". W piśmiennictwie dotyczącym terroryzmu znajdziemy wiele definicji tego pojęcia[3]. W tym miejscu warto przytoczyć jedną, która jest niezwykle syntetyczna, a jednocześnie bardzo przydatna dla dalszych rozważań zawartych w niniejszym opracowaniu, sformułowaną przez Mariana Flemminga. Zdefiniował on terroryzm jako „umyślne działania stanowiące naruszenie prawa karnego i zmierzające w drodze aktów przemocy lub zagrożenia takimi aktami do zastraszenia organów państwowych lub znaczących odłamów społeczeństwa oraz do wymuszenia określonego postępowania[4]"

Zgodnie z powyższym „czyn terrorystyczny" wypełnia znamiona przestępstwa pospolitego (np. zabójstwa, bezprawnego pozbawienia wolności, czyli „wzięcia zakładników" czy zakłócenia pracy sieci teleinformatycznej), czemu jednocześnie jednak towarzyszy zamiar spowodowania określonego efektu w postaci np. wywołania stanu zagrożenia w społeczeństwie czy określonej reakcji ze strony organów państwowych.

Pierwszym unijnym instrumentem prawnym, którego celem miało być przeciwdziałanie terroryzmowi, była decyzja ramowa Rady z dnia 13 czerwca 2002/475/WSiSW w sprawie zwalczania terroryzmu[5] (dalej jako decyzja ramowa 2002/475). Akt ten został zastąpiony dyrektywą Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępującą decyzję ramową Rady 2002/475/WSiSW oraz zmieniającą decyzję Rady 2005/671/WSiSW (dalej jako dyrektywa 2017/541), bazującą na nim, zasadniczo powtarzając jego rozwiązania (dotyczy to

1 M. Szymczak (red.), *Słownik języka polskiego*, t. III, Warszawa 1995, s. 463.
2 Ibidem.
3 Zob. szerzej: I. Resztak, *Zjawisko terroryzmu*, „Prokuratura i Prawo" 2012, nr 7–8, s. 148–152.
4 M. Flemming, *Terroryzm polityczny w międzynarodowym prawodawstwie*, „Wojskowy Przegląd Prawniczy" 1996, nr 3–4, s. 31.
5 Dz.Urz. WE 2002 L 164/3.

w zasadzie np. definicji przestępstwa terrorystycznego), jednocześnie niektóre z nich uszczegóławiając oraz dodając nowe.

Dyrektywa 2017/541 ustanawia przede wszystkim normy minimalne dotyczące definicji przestępstw i sankcji w dziedzinie przestępstw terrorystycznych[6], przestępstw dotyczących grupy terrorystycznej oraz przestępstw związanych z działalnością terrorystyczną, jak również środki ochrony i wsparcia ofiar terroryzmu i pomocy tym ofiarom. Definicja przestępstwa terrorystycznego zawarta w treści art. 3 dyrektywy 2017/541 (analogicznie jak ta sformułowana w decyzji ramowej 2002/475) ma charakter dwuelementowy: przedmiotowo-podmiotowy. By czyn zabroniony mógł zostać uznany za przestępstwo terrorystyczne musi – po pierwsze – spełniać kryterium przedmiotowe, czyli być jednym z czynów wymienionych w zamkniętym katalogu zawartym w art. 3 ust. 1 lit. a)–i)[7] lub grożeniem jego popełnienia (art. 3 ust. 1 lit. j)). Po drugie – spełniać co najmniej jedną z wymienionych w drugiej części definicji przesłanek podmiotowych w postaci celu działania sprawcy, tj. musi być popełniony w celu: 1) poważnego zastraszenia ludności, lub 2) bezprawnego zmuszenia rządu lub organizacji międzynarodowej do podjęcia

6 W decyzji ramowej 2002/475 oraz dyrektywie 2017/541 mowa jest o „przestępstwach terrorystycznych" (ang. *terroristic offences*), natomiast w polskim kodeksie karnym z dnia 6 czerwca 1997 r. (t.j. Dz.U. z 2016 r., poz. 1137 ze zm., dalej jako k.k.) użyto pojęcia „przestępstwo o charakterze terrorystycznym".

7 Wskazano w niej następujące zachowania: a) ataki na życie ludzkie, które mogą powodować śmierć; b) ataki na integralność fizyczną osoby; c) porwania lub branie zakładników; d) spowodowanie rozległych zniszczeń obiektów rządowych lub obiektów użyteczności publicznej, systemu transportowego, infrastruktury, w tym systemu informacyjnego, stałych platform umieszczonych na szelfie kontynentalnym, miejsca publicznego lub mienia prywatnego – jeżeli zniszczenia te mogą zagrozić życiu ludzkiemu lub spowodować poważne straty gospodarcze; e) zajęcie statku powietrznego, statku wodnego lub innego środka transportu publicznego lub towarowego; f) wytwarzanie, posiadanie, nabywanie, przewożenie, dostarczanie lub używanie materiałów wybuchowych lub broni, w tym broni chemicznej, biologicznej, radiologicznej lub jądrowej, jak również badania nad taką bronią i rozwój broni chemicznej, biologicznej, radiologicznej lub jądrowej; g) uwalnianie substancji niebezpiecznych lub powodowanie pożarów, powodzi lub wybuchów, czego rezultatem jest zagrożenie życia ludzkiego; h) zakłócanie lub przerywanie dostaw wody, energii elektrycznej lub wszelkich innych podstawowych zasobów naturalnych, czego rezultatem jest zagrożenie życia ludzkiego; i) niezgodna z prawem ingerencja w systemy, o której mowa w art. 4 dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne i uchylającej decyzję ramową Rady 2005/222/WSiSW, w przypadkach gdy zastosowanie ma art. 9 ust. 3 lub art. 9 ust. 4 lit. b) lub c) tej dyrektywy, oraz niezgodna z prawem ingerencja w dane, o której mowa w art. 5 tej dyrektywy, w przypadkach gdy zastosowanie ma art. 9 ust. 4 lit. c) tej dyrektywy (zob. dalsze uwagi).

lub zaniechania jakiegoś działania, lub 3) poważnej destabilizacji lub zniszczenia podstawowych politycznych, konstytucyjnych, gospodarczych lub społecznych struktur danego państwa lub danej organizacji międzynarodowej[8].

Natomiast w art. 4 dyrektywy 2017/541 zobowiązano państwa członkowskie do kryminalizacji kierowania grupą terrorystyczną[9] oraz uczestnictwa w działaniach takiej grupy. Wskazano, że pod tym ostatnim pojęciem rozumieć należy również dostarczanie informacji lub zasobów materialnych oraz wszelkiego rodzaju finansowanie działań takiej grupy, ze świadomością, że takie uczestnictwo będzie stanowiło wkład w działalność przestępczą grupy terrorystycznej.

8 Wspomnianą decyzję ramową 2002/475 do polskiego porządku prawnego implementowano ustawą z dnia 16 kwietnia 2004 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz.U. z 2004 r. nr 93, poz. 889). Jak wspominano jej postanowienia są zbliżone do zawartych w dyrektywie, a definicja przestępstwa terrorystycznego ma podobny kształt. Polski ustawodawca nie zdecydował się na dosłowną jej transpozycję. Stworzył własną, znacznie bardziej syntetyczną (art. 115 § 20 k.k.). Położono w niej nacisk na kryterium celu działania sprawcy, wskazując w przepisie – tak jak ma to miejsce w treści art. 1 ust. 1 decyzji ramowej 2002/475 oraz art. 3 ust. 2 dyrektywy 2017/541– alternatywnie jako cel działania sprawcy: 1) poważne zastraszenie wielu osób; 2) zmuszenie organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności; 3) wywołanie poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej. Drugi element definicji z art. 115 § 20 k.k. został skonstruowany odmiennie niż w pierwowzorze z decyzji ramowej 2002/475 (a co za tym idzie – odmiennie niż w dyrektywie 2017/541). Katalog przestępstw, które w przypadku popełnienia, w którymś ze wskazanych w definicji celów, są uznawane za mające charakter terrorystyczny został zastąpiony kryterium formalnym – wymogiem, aby czyn zabroniony zagrożony był karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat. Przepis ten nie tworzy zatem *delictum sui generis* lecz powoduje, iż przestępstwem o charakterze terrorystycznym będzie każde przestępstwo (każda zbrodnia i poważniejszy występek zagrożony karą pozbawienia wolności, której górna granica przekracza 5 lat) popełnione w którymś ze wskazanych w pierwszej części definicji celu. Stosownie do postanowień decyzji ramowej 2002/475, przestępstwem terrorystycznym jest również groźba popełnienia takiego czynu (art. 115 § 20 *in fine*) [w:] J. Giezek (red.), *Kodeks karny. Część ogólna*, Warszawa 2012, s. 738. Zob. szerzej: F. Radoniewicz, *Techniki implementacji do polskiego porządku prawnego postanowień decyzji ramowych Rady Unii Europejskiej dotyczących prawa karnego materialnego*, „Przegląd Prawa Konstytucyjnego" 2015, nr 3, s. 192–196.

9 Stosownie do definicji zawartej w art. 2 pkt 3) dyrektywy 2017/541 pod pojęciem tym należy rozumieć „grupę zorganizowaną złożoną z więcej niż dwóch osób, ustanowioną na pewien czas i działającą w uzgodniony sposób w celu popełniania przestępstw terrorystycznych". Natomiast „grupą zorganizowaną" – zgodnie z definicją zawartą w dalszej części cytowanego przepisu – jest grupa, która „nie jest przypadkowo sformowana w celu natychmiastowego popełnienia przestępstwa oraz w której nie ma potrzeby formalnego określenia ról członków grupy, ciągłości członkostwa lub rozwiniętej struktury".

W kolejnych artykułach dyrektywy 2017/541 nałożono na państwa członkowskie obowiązek kryminalizacji „przestępstw związanych z działalnością terrorystyczną", polegających na pewnych czynnościach, które nie stanowią same w sobie aktów terroru, ale mogą stanowić czynności przygotowawcze do ich popełnienia[10].

W świetle art. 15 ust. 1 dyrektywy 2017/541 przestępstwa, o których w niej mowa powinny podlegać skutecznym, proporcjonalnym i odstraszającym sankcjom karnym, które mogą pociągać za sobą wydanie lub ekstradycję.

Przestępstwa terrorystyczne, o których mowa w art. 3 dyrektywy 2017/541, oraz przestępstwa, o których mowa w jej art. 14 (podżeganie i pomocnictwo do przestępstw wskazanych w dyrektywie oraz ich usiłowanie)[11], powinny podlegać karom pozbawienia wolności w wymiarze wyższym niż orzekane na mocy prawa krajowego za takie przestępstwa, gdy nie przyświeca im „cel terrorystyczny" (art. 15 ust. 2).

Czyny wymienione w art. 4 dyrektywy 2017/541 powinny być zagrożone karą pozbawienia wolności w wymiarze maksymalnym nie niższym niż 15 lat w przypadku przestępstwa, o którym mowa w art. 4 lit. a), oraz w wymiarze maksymalnym nie mniejszym niż osiem lat w przypadku przestępstw wymienionych w art. 4 lit. b) (art. 15 ust. 3).

Natomiast w przypadku, gdy przestępstwo, o którym mowa w art. 6 lub 7 dyrektywy 2017/541, dotyczy dziecka, okoliczność ta powinna, zgodnie z prawem krajowym, być uwzględniana przy osądzaniu sprawców (art. 15 ust. 4).

10 Są to następujące przestępstwa: publiczne nawoływanie do popełnienia przestępstwa terrorystycznego (art. 5), werbowanie na rzecz terroryzmu (art. 6), prowadzenie szkolenia na potrzeby terroryzmu (art. 7), odbywanie szkolenia na potrzeby terroryzmu (art. 8), podróżowanie w celach terrorystycznych (art. 9), organizowanie lub ułatwianie w inny sposób podróżowania w celach terrorystycznych (art. 10), finansowanie terroryzmu (art. 11), a także „inne przestępstwa związane z działalnością terrorystyczną", wymienione w art. 12: a) kradzież kwalifikowana dokonana w celu popełnienia jednego z przestępstw wymienionych w art. 3; b) wymuszenie dokonane z zamiarem popełnienia jednego z przestępstw wymienionych w art. 3; c) sporządzanie lub korzystanie z fałszywych dokumentów urzędowych dokonane z zamiarem popełnienia jednego z przestępstw wymienionych w art. 3 ust. 1 lit. a)–i), w art. 4 lit. b) oraz w art. 9.

11 Za przestępstwo powinno zostać uznane pomocnictwo do popełnienia jednego z przestępstw, o których mowa w art. 3–8, 11 i 12 (art. 14 ust. 1), podżeganie do popełnienia jednego z przestępstw, o których mowa w art. 3–12 (art. 14 ust. 2) oraz usiłowanie popełnienia jednego z przestępstw, o których mowa w art. 3, 6, 7, art. 9 ust. 1 i art. 9 ust. 2 lit. a) oraz art. 11 i 12, z wyjątkiem posiadania, o którym mowa w art. 3 ust. 1 lit. f), oraz przestępstwa, o którym mowa w art. 3 ust. 1 lit. j) (art. 14 ust. 3).

Cyberterroryzm, czyli terroryzm w cyberprzestrzeni

Pojęcie cyberprzestrzeni (ang. *cyberspace*, słowo powstałe z połączenia dwóch angielskich słów: *cybernetics* i *space*, oznacza przestrzeń cybernetyczną) pojawiło się w latach 80. Za jego autora uważa się kanadyjskiego pisarza Williama Gibsona, który go użył w wydanej w 1984 r. powieści *Neuromancer* na określenie rzeczywistości wirtualnych, generowanych przez komputer, w których znajdowali się jego bohaterowie. Termin ten przeniknął do kultury masowej i obecnie określa się nim przede wszystkim wirtualną przestrzeń, czyli przestrzeń komunikacji za pomocą sieci komputerowych[12]. Często używa się tego pojęcia jako synonimu internetu[13].

Definicji cyberterroryzmu, podobnie jak terroryzmu, znajdziemy w literaturze znaczną ilość[14]. Z uwagi na ograniczoną objętość niniejszego opracowania, ograniczę się – analogicznie jak w przypadku terroryzmu – do przytoczenia dwóch (poniekąd skrajnych) jednej, niezwykle zwięzłej, a w związku z tym ogólnej i syntetycznej, sformułowanej przez Susan Brenner, która przyjęła, że cyberterroryzm jest to terroryzm planowany, dokonywany i koordynowany za pomocą komputerów i sieci komputerowych[15].

Druga, najczęściej zresztą przytaczana, definicja cyberterroryzmu, sformułowana przez D. Denning, jest znacznie węższa. Zdaniem tej autorki

12 W polskim prawie definicję cyberprzestrzeni znajdziemy m.in. w art. 2 ust.1a ustawy z dnia 21 czerwca 2002 r. o stanie wyjątkowym (t.j. Dz.U. z 2016 r., poz. 886 ze zm.), art. 3 ust. 1 pkt 4 ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (t.j. Dz.U. z 2014 r., poz. 333 ze zm.) oraz art. 2 ust. 1b ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (t.j. Dz.U. z 2016 r., poz. 851 ze zm.), zgodnie z którymi należy przez to pojęcie rozumieć „przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2014 r., poz. 1114), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami". Zob. szerzej: J. Kosiński, *Cyberprzestępczość* [w:] W. Jasiński, W. Mądrzejowski, K. Wiciak (red.), *Przestępczość zorganizowana. Fenomen. Współczesne zagrożenia. Zwalczanie. Ujęcie praktyczne*, Szczytno 2013, s. 462–463.

13 Por. K. Liderman, *Bezpieczeństwo informacyjne*, Warszawa 2012, s. 62–63; D. Wall, *Cybercrime. The Transformation of Crime in the Information Age*, Malden 2013, s. 10–11.

14 Zob. szerzej: M.F. Gawrycki [w:] A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 63–73.

15 S.W. Brenner [w:] *Cybercrime and the Law. Challenges. Issues, and Outcomes*, Boston 2012, s. 16. Por. M. Terlikowski, *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe. Haking, haktywizm i cyberterroryzm* [w:] M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009, s. 111–112.

cyberterroryzm jest połączeniem terroryzmu i cyberprzestrzeni. Generalnie rozumie się, że oznacza on bezprawne ataki i groźby ataku komputerów, sieci i informacji tam zgromadzonych w celu zastraszenia lub zmuszenia rządu lub jego mieszkańców do realizacji celów politycznych lub społecznych. Ponadto w celu zakwalifikowania jako cyberterroryzm, atak powinien skutkować przemocą wobec osób lub majątku lub przynajmniej spowodować wystarczającą szkodę, aby wywołać strach. Przykładami mogą być ataki, które prowadzą do śmierci lub uszkodzenia ciała, eksplozji, katastrof samolotów, zanieczyszczenia wody lub dotkliwych strat gospodarczych. Poważne ataki na infrastrukturę krytyczną mogą być atakami cyberterrorystycznymi w zależności od ich skutków. Do takich nie można zaliczyć ataków, które zakłócają nieistotne usługi lub powodują głównie kłopoty finansowe[16]".

Pierwszym wiążącym unijnym aktem prawnym dotyczącym zamachów na bezpieczeństwo w cyberprzestrzeni była decyzja ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne[17] (dalej jako decyzja ramowa 2005/222). Prace nad nią rozpoczęły się już w 2001 r. w następstwie ogłoszenia przez Komisję Europejską w 2001 r. tzw. komunikatu o cyberprzestępczości[18], zawierającego pewne propozycje przepisów materialnych i proceduralnych, mających służyć zwalczaniu przestępstw komputerowych, zarówno na poziomie krajowym, jak i wspólnotowym. Efektem podjętych wówczas działań był m.in. projekt wskazanej wyżej decyzji ramowej[19].

W preambule decyzji ramowej 2005/222 wskazano, że jej celem jest usprawnienie współpracy między organami sądowymi i organami ścigania państw członkowskich poprzez zbliżanie przepisów prawa karnego w tych państwach w dziedzinie ataków na systemy informatyczne. Podjęcie działań legislacyjnych na poziomie unijnym uzasadniano koniecznością przeciwdziałania atakom na systemy informatyczne, z uwagi na możliwe związki między tego typu przestępstwami a działalnością zorganizowanych grup przestępczych

16 Cyt. za: D. Verton, *Black Ice. Niewidzialna groźba cyberterroryzmu*, Gliwice 2004, s. 20.
17 Dz.Urz. UE 2005 L 69/67.
18 Komunikat Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów COM(2000)890 w sprawie tworzenia bezpiecznego społeczeństwa informacyjnego poprzez zwiększenie bezpieczeństwa struktur informacyjnych i zwalczanie przestępczości komputerowej z dnia 26 stycznia 2001 r.
19 Projekt decyzji ramowej Rady w sprawie ataków na systemy informatyczne (*Proposal for a Council Framework Decision on attacks against information systems*), COM (2002) 0173.

oraz atakami terrorystycznymi na systemy informatyczne stanowiące część infrastruktury państw członkowskich.

W decyzji ramowej 2005/222 przede wszystkim zdefiniowano najistotniejsze pojęcia („systemu informatycznego", „danych komputerowych", „osoby prawnej", „bezprawności"), zobowiązano państwa członkowskie do stypizowania przestępstw uzyskania bezprawnego dostępu, bezprawnej ingerencji w system informatyczny oraz bezprawnej ingerencji w dane komputerowe, odniesiono się do kwestii odpowiedzialności osób prawnych, jurysdykcji oraz wykorzystania sieci operacyjnych punktów kontaktowych dostępnych 24 godziny na dobę oraz przez siedem dni w tygodniu w celu wymiany informacji dotyczących ataków na systemy informatyczne.

Ograniczona liczba przestępstw określonych w decyzji ramowej 2005/222, konieczność uwzględnienia nowych zagrożeń, a także chęć dostosowania regulacji do nowych inicjatyw Unii Europejskiej w dziedzinie cyberbezpieczeństwa i uzupełnienia ich w celu stworzenia całościowej regulacji tej materii doprowadziła do decyzji o podjęciu prac nad nowym instrumentem prawnym w dziedzinie cyberprzestępczości. Ich efektem jest dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i uchylająca decyzję ramową Rady 2005/222/WSiSW[20] (dalej jako dyrektywa 2013/40).

W preambule tego aktu podkreślono m.in., że ataki na systemy informatyczne, w szczególności ze względu na zagrożenie ze strony przestępczości zorganizowanej oraz możliwość powiązania z działaniami o charakterze terrorystycznym lub mającymi podłoże polityczne, są coraz bardziej niebezpieczne. Zwłaszcza że mogą stworzyć realne zagrożenie dla systemów informatycznych stanowiących element infrastruktury krytycznej państw członkowskich i Unii.

W treści dyrektywy 2013/40 zasadniczo powtórzono postanowienia z decyzji ramowej, jednocześnie przewidując pewne nowe rozwiązania (nowe typy czynów zabronionych – nielegalne przechwytywanie danych komputerowych oraz przestępstwa dotyczące „narzędzi hackerskich" – oraz określono dodatkowe okoliczności, których wystąpienie powinno skutkować zaostrzeniem odpowiedzialności karnej.

Dla potrzeb dyrektywy 2013/40 (a wcześniej decyzji ramowej 2005/222) przyjęto, że „systemem informatycznym" (ang. *information system*) jest urządzenie lub grupa wzajemnie połączonych lub powiązanych ze sobą urządzeń,

20 Dz.Urz. UE 2013 L 218/8.

z których jedno lub więcej, zgodnie z programem, dokonuje automatycznego przetwarzania danych komputerowych, jak również danych komputerowych przechowywanych, przetwarzanych, odzyskanych lub przekazanych przez to urządzenie lub tę grupę urządzeń, w celach ich eksploatacji, użycia, ochrony lub utrzymania (art. 2 lit. a).

Powyższa definicja ma szeroki zakres przedmiotowy. Pod pojęciem systemu informatycznego należy bowiem rozumieć zarówno pojedyncze urządzenie przetwarzające dane (np. komputer czy smartfon), jak i sieć komputerową, zarówno małą (np. sieć LAN[21]), obejmującą kilka komputerów, jak i wielką strukturę, składającą się z połączonych ze sobą sieci (np. tzw. sieć MAN[22])[23].

W art. 2 lit. b dyrektywy 2013/40 zdefiniowano „dane komputerowe" jako „przedstawienie faktów, informacji lub pojęć w formie nadającej się do przetwarzania w systemie informatycznym, włącznie z programem umożliwiającym wykonanie funkcji przez system informatyczny".

Natomiast w świetle art. 2 lit. d) dyrektywy 2013/40 za bezprawne uważa się działanie, o którym w niej mowa, w tym dostęp, ingerencję lub przechwycenie, na które właściciel lub inny podmiot uprawniony do systemu lub jego części nie udzielił zgody, lub które nie jest dozwolone na mocy prawa krajowego.

W art. 3 dyrektywy 2013/40 nałożono na państwa członkowskie obowiązek kryminalizacji umyślnego i bezprawnego uzyskania dostępu do całości lub jakiejkolwiek części systemu informatycznego, jeżeli wiąże się to z naruszeniem przez sprawcę środków bezpieczeństwa. Przez uzyskanie dostępu do systemu informatycznego należy rozumieć zdobycie możliwości korzystania z jego zasobów (czyli przechowywanych w nim danych oraz używanie sprzętu, co w zasadzie sprowadza się również do dostępu do danych – oprogramowania nim sterującego).

Kolejnym przestępstwem określonym w dyrektywie 2013/40 jest ingerencja w system informatyczny, polegająca na umyślnym, bezprawnym i poważnym utrudnieniu lub zakłóceniu funkcjonowania systemu informatycznego poprzez wprowadzenie, przekazywanie, uszkadzanie, usuwanie, pogarszanie,

21 Sieć LAN (ang. *local area network*) – sieć lokalna.

22 Sieć MAN (ang. *metropolitan area network*) – sieć miejska, składająca się z wielu połączonych sieci lokalnych. Sieci tego typu tworzone są przez instytucje państwowe, uczelnie (sieci akademickie), czy podmioty prywatne (np. przedsiębiorstwa).

23 Z uwagi na ograniczenia objętościowe niniejszego opracowania, szczegółowe rozważania dotyczące tej kwestii zostaną pominięte. Zob. szerzej: F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016, s. 244–249.

zmienianie lub eliminowanie danych komputerowych lub czynienie ich niedostępnymi (art. 4 dyrektywy 2013/40). Chodzi zatem przede wszystkim o działania o charakterze logicznym skierowane przeciw systemom informatycznym, mające na celu utrudnienie lub uniemożliwienie działania systemu poprzez oddziaływanie na przetwarzane przez system dane komputerowe lub oprogramowanie odpowiadające za jego funkcjonowanie.

Natomiast w art. 5 dyrektywy 2013/40 zobowiązano państwa członkowskie do kryminalizacji ataków logicznych, których przedmiotem są dane komputerowe. Określono w nim przestępstwo nielegalnej ingerencji w dane, jako usuwanie, uszkadzanie, pogarszanie, zmienianie lub eliminowanie danych komputerowych w systemie informatycznym lub czynienie ich niedostępnymi. Taką ingerencją jest np. zarówno kasowanie danych, jak i instalacja przez sprawcę w zaatakowanym komputerze programu, umożliwiającego podjęcie przy jego użyciu dalszych działań (np. kradzieży danych) czy – poprzez włączenie zaatakowanego komputera przy jego pomocy w botnet – przeprowadzenie rozproszonego ataku odmowy usługi (dDoS – ang. *Distributed Denial of Service*).

Pierwszym „nowym" (w stosunku do decyzji ramowej 2005/222) typem czynu zabronionego jest określone w treści art. 6 dyrektywy 2013/40 przestępstwo nielegalnego przechwytywania (ang. *illegal interception*), polegające na umyślnym przechwytywaniu środkami technicznymi niepublicznych przekazów danych komputerowych do, z lub w ramach systemu informatycznego, w tym emisji elektromagnetycznych wytwarzanych przez system informatyczny zawierający takie dane komputerowe.

W art. 7 dyrektywy 2013/40 przewidziano drugi typ przestępstwa, którego nie przewidywała decyzja ramowa 2005/222. W przepisie tym zobowiązano państwa członkowskie do kryminalizacji bezprawnego i umyślnego wytwarzania, sprzedaży, dostarczania, przywozu, posiadania, rozpowszechniania lub udostępniania w inny sposób narzędzia służącego do popełnienia wskazanych w art. 3–6 dyrektywy 2013/40 przestępstw (potocznie „narzędzia hackerskiego"), w przypadkach, w których czyn ten dokonany był w celu popełnienia któregokolwiek z określonych w dyrektywie przestępstw. Przez „narzędzie" rozumie się: 1) program komputerowy zaprojektowany lub przystosowany głównie dla celów popełniania przestępstw, o których mowa w art. 3–6; 2) hasło komputerowe, kod dostępu lub podobne dane umożliwiające dostęp do całości lub części systemu informatycznego.

W art. 9 ust. 1 dyrektywy 2013/40 wskazano, że przewidziane w niej czyny (łącznie z pomocnictwem i podżeganiem do nich oraz usiłowaniem popełnienia przestępstw z art. 4 i 5 – zob. art. 8 ust. 1 i 2) powinny być zagrożone

skutecznymi, proporcjonalnymi i odstraszającymi sankcjami o charakterze karnym. Jednocześnie jednak zastrzeżono, by czyny określone w art. 3–7 dyrektywy 2013/40 (co oznacza, że nie dotyczy to usiłowania ich popełnienia oraz pomocnictwa i podżegania do nich) podlegały karze w maksymalnym wymiarze nie mniejszym niż dwa lata pozbawienia wolności co najmniej w przypadkach, które nie są przypadkami mniejszej wagi (art. 9 ust. 2).

Ponadto w art. 9 dyrektywy 2013/40 przewidziano szereg okoliczności, których wystąpienie powinno skutkować zaostrzeniem odpowiedzialności karnej. Dotyczą one jednak jedynie czynów określonych w art. 4 i 5 (tj. bezprawnej ingerencji w system informatyczny oraz bezprawnej ingerencji w dane komputerowe). Pierwszą jest wykorzystanie do jego popełnienia jednego z narzędzi, o których mowa w art. 7 dyrektywy 2013/40, zaprojektowanego lub dostosowanego głównie do tego celu, i umyślne spowodowanie skutku w postaci oddziaływania na znaczną liczbę systemów informatycznych. Sprawca powinien w takim wypadku podlegać karze, której górna granica powinna wynosić co najmniej trzy lata pozbawienia wolności (art. 9 ust. 3 dyrektywy 2013/40).

W art. 9 ust. 4 dyrektywy 2013/40 – jako okoliczności obciążające, których wystąpienie skutkować powinno możliwością orzeczenia kary pozbawienia wolności w wymiarze co najmniej pięciu lat wskazano popełnienie czynu w ramach organizacji przestępczej określonej w decyzji ramowej 2008/841 z dnia 24 października 2008 r. w sprawie zwalczania przestępczości zorganizowanej[24], spowodowanie znacznej szkody, popełnienie przestępstwa przeciwko systemowi informatycznemu o charakterze infrastruktury krytycznej[25].

24 Dz.Urz. UE 2008 L 300/42. Zgodnie z art. 1 pkt 1 tejże decyzji jest to zorganizowana grupa, istniejąca przez pewien czas, składająca się z więcej niż dwóch osób, działających wspólnie w celu popełnienia przestępstw, których maksymalne zagrożenie karą wynosi co najmniej cztery lata pozbawienia wolności lub aresztu lub które podlegają surowszej karze, w celu osiągnięcia, bezpośrednio lub pośrednio, korzyści finansowej lub innej korzyści materialnej. „Zorganizowaną grupą" jest grupa, która nie jest przypadkowo utworzona w celu natychmiastowego popełnienia przestępstwa, ale której członkowie nie muszą mieć formalnie określonych ról, w której nie musi istnieć ciągłość członkostwa ani rozwinięta struktura (art. 1 pkt 2 decyzji ramowej 2008/841). W dyrektywie 2013/40 przyjęto rozwiązanie analogiczne, jak wcześniej w decyzji ramowej 2005/222, uniezależniając uznanie zorganizowanej grupy za organizację przestępczą od wysokości sankcji, grożącej za przestępstwo popełnione przez osoby działające w jej ramach.

25 Zgodnie z art. 2 lit. a) dyrektywy Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz.Urz. UE 2008 L 345/75) – pod pojęciem tym rozumie się składnik, system lub część infrastruktury zlokalizowane na terytorium państw

Natomiast jako ostatnią okoliczność zaostrzającą odpowiedzialność karną (art. 9 ust. 5) przewidziano posłużenie się przez sprawcę w celu popełnienia przestępstwa określonego w art. 4 lub 5, tożsamością osoby trzeciej (tzw. kradzież tożsamości).

Obecnie jednak powyższe zastrzeżenia należy uznać za nieaktualne. Rozważając bowiem kwestię zaostrzenia odpowiedzialności karnej w przypadku terrorystycznego charakteru czynu sprawcy, należy mieć na względzie regulację zawartą w dyrektywie 2017/541. Zgodnie bowiem z art. 3 ust. 1 lit. i) w zw. z art. 3 ust. 2 tej dyrektywy (zob. wcześniejsze uwagi), niezgodna z prawem ingerencja w systemy, o której mowa w art. 4 dyrektywy, w przypadkach gdy zastosowanie ma art. 9 ust. 3 lub art. 9 ust. 4 lit. b) lub c) tej dyrektywy, oraz niezgodna z prawem ingerencja w dane, o której mowa w art. 5 tej dyrektywy, w przypadkach, gdy zastosowanie ma art. 9 ust. 4 lit. c) tej dyrektywy. Oznacza to, że za przestępstwa terrorystyczne powinny zostać uznane czyny polegające na nielegalnej ingerencji w systemy informatyczne popełnione w celu określonym w art. 3 ust. 2 dyrektywy 2017/541, w przypadku, gdy do ich dokonania wykorzystano jedno z narzędzi, o których mowa w art. 7 dyrektywy 2013/40, zaprojektowanego lub dostosowanego głównie do tego celu, i umyślne spowodowanie skutku w postaci oddziaływania na znaczną liczbę systemów informatycznych lub spowodowano znaczną szkodę. Ponadto czyn z art. 5 powinien zostać uznany za takowy, gdy skierowany był przeciwko systemowi informatycznemu o charakterze infrastruktury krytycznej.

Bibliografia

Bógdał-Brzezińska A., Gawrycki M.F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003.

Flemming M., *Terroryzm polityczny w międzynarodowym prawodawstwie*, „Wojskowy Przegląd Prawniczy" 1996, nr 3–4.

Giezek J. (red.), *Kodeks karny. Część ogólna*, Warszawa 2012.

Kosiński J., *Cyberprzestępczość* [w:] W. Jasiński, W. Mądrzejowski, K. Wiciak (red.), *Przestępczość zorganizowana. Fenomen. Współczesne zagrożenia. Zwalczanie. Ujęcie praktyczne*, Szczytno 2013.

Liderman K., *Bezpieczeństwo informacyjne*, Warszawa 2012.

Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016.

członkowskich, które mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego ludności oraz których zakłócenie lub zniszczenie miałoby istotny wpływ na dane państwo członkowskie w wyniku utracenia tych funkcji.

Radoniewicz F., *Techniki implementacji do polskiego porządku prawnego postanowień decyzji ramowych Rady Unii Europejskiej dotyczących prawa karnego materialnego*, „Przegląd Prawa Konstytucyjnego" 2015, nr 3.
Resztak I., *Zjawisko terroryzmu*, „Prokuratura i Prawo" 2012, nr 7–8.
Szymczak M. (red.), *Słownik języka polskiego*, t. III, Warszawa 1995.
Terlikowski M., *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe. Haking, haktywizm i cyberterroryzm* [w:] M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009.
Verton D., *Black Ice. Niewidzialna groźba cyberterroryzmu*, Gliwice 2004.
Wall D., *Cybercrime. The Transformation of Crime in the Information Age*, Malden 2013.

Combating cyberterrorism in the EU – selected substantive criminal law aspects

Abstract

The purpose of the article is to present EU law provisions on substantive criminal law. Cyber terrorism is not regulated independently. This, of course, does not mean that there is no regulation for this problem. It is scattered and to decode the regulation of criminal liability for acts that can be classified as cyberterrorism, i.e. cyber-terrorist offences, two EU legal acts should be refered: Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017. Combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA and Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and repeals Council Framework Decision 2005/222/JHA. This article therefore consists of two parts: the first on Directive 2017/541 of 15 March 2017 on the fight against terrorism and the second on Directive 2013/40/EU of 12 August 2013 on attacks against information systems.

Key words: criminal law, cybercrime, terrorism, directive 2017/541, directive 2013/40