ROLA AGENCJI BEZPIECZEŃSTWA WEWNĘTRZNEGO I POLICJI W ZWALCZANIU CYBERTERRORYZMU

THE ROLE OF INTERNAL SECURITY AGENCY AND THE POLICE IN COMBATING CYBERTERRORISM

Nikola CZARNOTA

Uniwersytet Rzeszowski

Abstrakt. Cyberbezpieczeństwo jest istotnym obszarem dla wszystkich sektorów bezpieczeństwa państwa. Odnosi się do bezpiecznego funkcjonowania państwa, struktur administracyjnych i obywateli w cyberprzestrzeni. Niniejszy artykuł ma na celu przedstawienie rozważań na temat cyberterroryzmu i działań Agencji Bezpieczeństwa Wewnętrznego i Policji w tej dziedzinie. Ponadto artykuł zawiera aspekty teoretyczne związane z zaprezentowaniem pojęcia cyberterroryzmu, metody działań cyberterrorystów, a także przykładowe ataki w cyberprzestrzeni w Polsce. Celem artykułu jest diagnoza zaangażowania Policji i ABW w przeciwdziałanie cyberterroryzmowi. Problem badawczy zamyka się w pytaniu: jaką rolę w zwalczaniu cyberterroryzmu pełnią Policja i Agencja Bezpieczeństwa Wewnętrznego?

Abstract. Cybersecurity is an important area for all sectors of state security. It refers to the safe functioning of the state, administrative structures and citizens in cyberspace. This article aims to present considerations on cyberterrorism and activities of the Internal Security Agency and the Police in this field. In addition, the article contains theoretical aspects related to the presented term of cyberterrorism, the method of actions of cyberterrorists, as well as exemplary attacks in cyberspace in Poland.

Słowa kluczowe: cyberterroryzm, Agencja Bezpieczeństwa Wewnętrznego, Policja, cyberbezpieczeństwo, ataki cybernetyczne.

Keywords: cyberterrorism, Internal Security Agency, Police, cybersecurity, cyber-attacks.

Wstęp

Terroryzm i powstające w ramach tego zjawiska nowe formy, ze względu na rozwój technologiczny są obecnie kluczowym aspektem poruszanym na arenie międzynarodowej. Niewątpliwie trudnością jest samo zdefiniowanie tego zjawiska oraz rozpoznawanie, przeciwdziałanie i zwalczanie skutków ataków terrorystycznych. Do jednych z najgroźniejszych zjawisk terrorystycznych, które stanowią przejaw wykorzystania technologii wbrew ich przeznaczeniu, należy z pewnością działalność przestępcza i terrorystyczna znana pod pojęciem cyberterroryzmu.

Cyberterroryzm stanowi zagrożenie dla podstawowych filarów demokratycznego państwa i praw obywatela, które są chronione przez Konstytucję. Ponadto działalność cyberterrorystów jest obecnie szeroka i obejmuje swym zakresem również infrastrukturę krytyczną państwa, co może skutkować wzrostem zagrożenia dla

procesów gospodarczych. Nie ulega wątpliwości, iż to zjawisko jest powszechne i występuje coraz częściej w związku z powszechnym korzystaniem z nowoczesnych technologii przez instytucje i obywateli Polski. Wobec tego, odpowiedzialnymi za zwalczanie i ochronę przed cyberterroryzmem są odpowiednie służby m.in. Agencja Bezpieczeństwa Wewnętrznego i Policja.

Pojęcie cyberterroryzmu

Cyberterroryzm jest zjawiskiem stosunkowo nowym i według wielu ekspertów trudnym do zdefiniowania ze względu na swoją złożoność. Zjawisko to można zdefiniować jako połączenie cyberprzestrzeni i terroryzmu, ponieważ oprócz wykorzystywania nowoczesnych technologii w cyberprzestrzeni, charakteryzuje go również działalność terrorystyczna. Cyberterroryzm to dokonywanie bezprawnych ataków w stosunku do komputerów, sieci i wszelakich informacji celem zastraszenia obywateli i rządu państwa, aby osiągnąć korzyści materialne, polityczne czy społeczne. Co więcej, aby móc mówić o ataku cyberterrorystycznym istotnym elementem jest przemoc wobec ludzi lub mienia, a także powodowanie strat w celu wywołania strachu (Oleksiewicz 2018, s. 54).

Istotny element tego zjawiska wskazał K. Liedel, który uważa, iż cyberterroryzm to uzasadniony atak na komputery, sieci, systemy teleinformacyjne mający na celu zniszczenie infrastruktury, wywołanie strachu wśród społeczeństw lub wymuszenie na władzy określonych celów o charakterze politycznym czy społecznym (Liedel 2006, s. 36). Wśród potencjalnych obszarów ataków w cyberprzestrzeni wymienia się zarówno te o charakterze militarnym, jak i cywilnym. Celami cyberterrorystów są **państwowe systemy teleinformatyczne**, które zapewniają prawidłowe funkcjonowanie (Banaś, ZSE):

- administracji państwowej,
- sił zbrojnych i innych instytucji zajmujących się obroną narodową,
- instytucji odpowiedzialnych za bezpieczeństwo wewnętrzne i zewnętrzne państwa,
- łączności i sieci telekomunikacyjnych,
- sieci zaopatrzenia w energię, wodę i gaz,
- sieci i instytucji finansowych,
- służb ratowniczych.

Współcześnie nielegalna działalność rozwija się gwałtownie w Internecie. Globalizacja i rozwój technologiczny umożliwił niezwykle szybką komunikację i przeniesienie większości działań człowieka do sieci, również tych o charakterze przestępczym. Coraz powszechniej mówi się o cyberprzestrzeni jako nowej przestrzeni społecznej, w której pojawiają się wydarzenia i problemy, które mają odzwierciedlenie w świecie rzeczywistym. Cyberprzestępczość uznaje się za nową odmianę przestępczości, wykorzystującą możliwości technologiczne.

W Polsce nie występuje legalny termin cyberterroryzmu w porządku prawnym. Mimo to, definicje cyberterroryzmu zostały ujęte w niemających charakteru normatywnego Rządowym Programie Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016 oraz w Polityce Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej. Pierwsza z nich określa cyberterroryzm jako: „cyberprzestępstwo o charakterze terrorystycznym" (RPOC, 2010). Natomiast w Polityce Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej cyberterroryzm określany jest jako: „przestępstwo o charakterze terrorystycznym popełnione w cyberprzestrzeni" (POCRP 2013).

Co istotne, 22 października 2019 roku została przyjęta Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, która obowiązuje od 31 października 2019 roku i zastępuje Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022. Strategia jest zbliżona do Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej. Głównym celem przyjęcia i wdrożenia Strategii jest podniesienie poziomu ochrony na zagrożenia w cyberprzestrzeni i informacji w sektorze publicznym, militarnym i prywatnym, a także promowanie działań mających na celu ochronę informacji obywateli (SCRP 2019).

Ponadto w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 wyróżniono pięć celów szczegółowych, mianowicie:

1. Rozwój krajowego systemu cyberbezpieczeństwa.
2. Podniesienie poziomu ochrony systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty.
3. Zwiększenie potencjału narodowego w zakresie technologii cyberbezpieczeństwa.
4. Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa.
5. Zbudowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa.

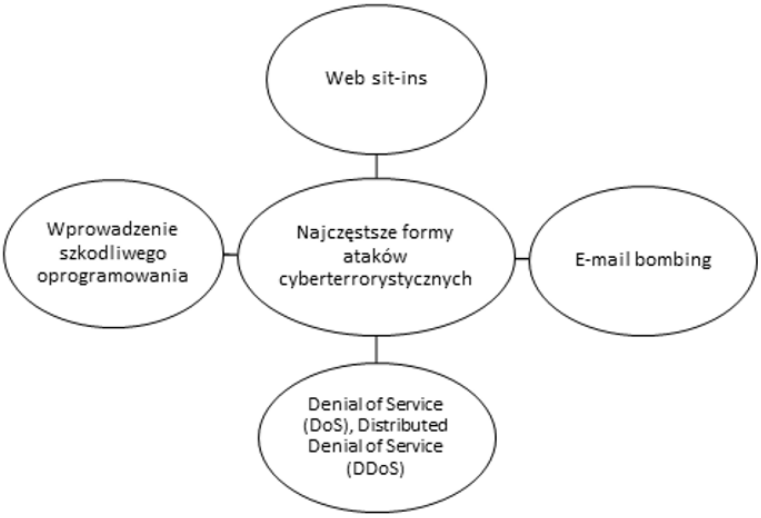
Co więcej, w obrębie każdego celu szczegółowego wyznaczone zostały priorytety działania administracji.

Analiza metod działań cyberterrorystów i ataków cyberterrorystycznych w Polsce

Cyberterroryzm stanowi istotne zagadnienie dla zapewnienia bezpieczeństwa sieci teleinformatycznych. Cyberterroryści posługują się wieloma metodami, które mogą przybierać m.in. formy zabiegów, które zmierzają do zakłócenia działania systemu, modyfikowania, kopiowania i usuwania danych czy też łamania zabezpieczeń po to, aby przejąć kontrolę nad konkretnymi elementami sieci teleinformatycznych.

Ponadto cyberterroryści posługują się nowymi technologiami i Internetem w niemalże podobny sposób, jak zorganizowanie grupy przestępcze. Wśród występujących metod działań możemy wyróżnić (Czyżak 2010, s. 48):

- włamania do obcych komputerów (*hacking*) i do systemów informatycznych (*cracking*), wykorzystywane w celu uzyskania materialnych korzyści,
- wykorzystywanie programów umożliwiających wejście do serwera z pominięciem zabezpieczeń (*back door*),
- przechwytywanie informacji przekazywanych między komputerami i pozyskiwanie tym samym haseł i loginów (*sniffing*),
- podszywanie się pod inny komputer (*IP spoofing*),
- wyłudzanie poufnych informacji, jest to najczęściej wykorzystywana metoda przez cyberterrorystów (*phishing*).



Rys. 1. Najczęściej stosowane metody przez cyberterrorystów
Źródło: Opracowanie własne na podstawie (Banaś, ZSE)

Powyższa grafika przedstawia najczęściej występujące ataki cyberterrorystyczne na instytucje publiczne. Cyberterroryści stosują metody (Banaś, ZSE):

- *web sit-ins*, która polega na masowym wchodzeniu na strony internetowe w celu ich zablokowania,
- *e-mail bombing*, dzięki któremu cyberterroryści mogą przesłać w krótkim czasie ogromną ilość elektronicznych wiadomości pocztowych, co skutkuje zablokowaniem serwera,

- *Denial of Service* (DoS), *Distributed Denial of Service* (DDoS), które polegają na przesyłaniu olbrzymich pakietów danych na konkretny komputer, co może skutkować nawet zniszczeniem go poprzez atak na różne serwery internetowe,
- wprowadzenie szkodliwego oprogramowania może powodować zniszczenie lub przechwycenie dużej ilości danych poprzez wprowadzenie różnego oprogramowania za pomocą reklam, przez zewnętrzne nośniki pamięci czy zainfekowane strony internetowe itp.

Ponadto cyberterroryści wykorzystują Internet nie tylko jako przestrzeń, w której mogą przeprowadzać ataki cyberterrorystyczne. Posługują się nią w celu rozprzestrzeniania się propagandy, idei czy też pozyskiwaniu członków do ugrupowania. W konsekwencji ataki cyberterrorystyczne dzięki wykorzystywanym metodom przez cyberterrorystów mogą doprowadzić do kradzieży istotnych informacji, często tajnych, jak i danych osobowych, uszkodzenie lub zniszczenie informacji mających kluczowe znaczenie dla państwa, paraliż instytucji publicznych, zablokowanie stron internetowych czy też zwiększenie członków w nowej organizacji i rozpowszechnienie propagandy.

CERT Polska w ostatnim swoim raporcie „Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny 2019 z działalności CERT Polska" opublikował wiele informacji na temat stanu polskiego cyberbezpieczeństwa, z których wybrane incydenty zostaną przybliżone. Nie ulega wątpliwości, iż liczba cyberataków w Polsce rośnie. W 2019 roku CERT Polska zarejestrował ich 6484, o 73% więcej niż rok wcześniej, jest to rekordowa liczba i wzrost w ujęciu rocznym. Najczęściej ataki cyberterrorystyczne dotyczyły osób fizycznych (19%) oraz sektora bankowego (16%).

Tabela 1. Incydenty obsłużone przez CERT Polska w 2019 r. w podziale na sektor gospodarki

Sektor gospodarki	**Liczba incydentów**	[%]
osoby fizyczne	1212	18,7%
bankowość	1057	16,3%
media	748	11,5%
handel hurtowy i detaliczny	624	9.6%
infrastruktura cyfrowa	550	8,5%
finanse	500	7,7%
administracja publiczna	336	5,2%
transport	61	0,9%
służba zdrowia	53	0,8%
inne	1343	20,8%
razem	6484	100%

Źródło: Opracowanie własne na podstawie (CERT, 2019)

CERT Polska odnotował rekordowy wzrost liczby obsłużonych incydentów na poziomie 73% w porównaniu do roku poprzedniego. Na pierwszym miejscu znalazły się oszustwa komputerowe, które stanowiły 63% incydentów. Na drugim miejscu pod względem liczby zarejestrowanych incydentów znalazły się zgłoszenia dotyczące złośliwego oprogramowania (14,9%). Natomiast incydenty z kategorii „obraźliwe i nielegalne treści", stanowiły 12,5 % wszystkich zarejestrowanych incydentów.

Tabela 2. Incydenty obsłużone przez CERT Polska w 2019 r. według typów

Typ incydentu	Liczba incydentów	[%]
obraźliwe i nielegalne treści	812	12,5%
złośliwe oprogramowanie	969	14,9%
gromadzenie informacji	95	1,5%
próby włamań	77	1,2%
włamania	160	2,5%
dostępność zasobów	57	0,9%
atak na bezpieczeństwo informacji	41	0,6%
oszustwa komputerowe	4086	63%
podatne usługi	102	1,6%
inne	85	1,3%
razem	6484	100%

Źródło: Opracowanie własne na podstawie (CERT, 2019)

Ponadto, raport CERT ukazuje skalę i dynamikę tego zjawiska poprzez liczbę obsłużonych incydentów na przestrzeni 10 lat, co obrazuje poniższa tabela.

Tabela 3. Liczba incydentów obsłużonych przez CERT na przestrzeni 10 lat

Rok	**Liczba incydentów**
2019	6484
2018	3739
2017	3182
2016	1926
2015	1456
2014	1282

Rok	**Liczba incydentów**
2013	1219
2012	1082
2011	605
2010	674
2009	1292

Źródło: Opracowanie własne na podstawie (CERT, 2019)

Przedstawione powyższe dane statystyczne potwierdzają, iż wraz z rozwojem działalności gospodarczej w Internecie rośnie skala przestępczości internetowej. Nie ulega wątpliwości, iż zabezpieczenie przed cyberatakami jest obecnie koniecznością, ponieważ z roku na rok wzrasta liczba cyberataków.

Działania Agencji Bezpieczeństwa Wewnętrznego i Policji na rzecz zwalczania cyberterroryzmu

W Polsce dwie służby odgrywają wiodącą rolę w działaniach na rzecz zwalczania cyberterroryzmu, jest to Agencja Bezpieczeństwa Wewnętrznego i Policja. Agencja Bezpieczeństwa Wewnętrznego jest służbą specjalną, która odpowiada za kwestie związane z ochroną bezpieczeństwa wewnętrznego państwa i jego konstytucyjnego porządku. Głównymi zadaniami Agencji Bezpieczeństwa Wewnętrznego zgodnie z ustawą o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu (Dz.U. z 2002 r. Nr 74, poz. 676) są: zwalczanie różnego rodzaju zagrożeń dla bezpieczeństwa wewnętrznego państwa i porządku konstytucyjnego, przestępstw szpiegostwa, terroryzmu, handlu narkotykami, korupcji itd. Ponadto działania pozwalające zapobiegać rozwojowi przestępczości zorganizowanej, wynikają z uprawnień operacyjno-rozpoznawczych oraz dochodzeniowo-śledczych, które służą w celu wykrywania przestępstw i ścigania jego sprawców. Natomiast czynności operacyjno-rozpoznawcze i analityczno-informacyjne wykorzystywane są w celu pozyskania informacji dla zapewnienia bezpieczeństwa państwa i porządku konstytucyjnego Polski (Oleksiewicz 2017, s. 227).

W ramach funkcjonowania Agencji Bezpieczeństwa Wewnętrznego powołano Centrum Antyterrorystyczne Bezpieczeństwa Wewnętrznego, które koordynuje i analizuje obszar związany z przeciwdziałaniem terroryzmowi i skutecznemu zwalczaniu go. Wśród głównych zadań instytucji możemy wyróżnić (Makarski 2010, s. 104-106):

- wspomaganie procesów decyzyjnych w przypadku realnego zagrożenia atakiem terrorystycznym,
- koordynowanie działań operacyjno-rozpoznawczych,
- wykonywanie czynności analityczno-informatycznych w zakresie sporządzania raportów sytuacyjnych i syntetycznych oraz przygotowanie informacji dla kierownictwa państwa,
- udział w opracowaniu i nowelizowaniu procedur związanych z zarządzaniem kryzysowym na wypadek ataku terrorystycznego,
- wspomaganie działań służb i instytucji uczestniczących w obronie antyterrorystycznej RP,
- współpracę międzynarodową z UE i NATO.

Co więcej, 1 lutego 2008 roku został powołany Rządowy Zespół Reagowania na Incydenty Komputerowe, który jest jednostką działającą w strukturach Agencji Bezpieczeństwa Wewnętrznego, w Departamencie Bezpieczeństwa Teleinformatycznego. Podstawowymi zadaniami zespołu jest nauka oraz szkolenie instytucji państwowych w Polsce w celu zapewnienia ochrony przed atakami cyberterrorystycznymi. Ponadto do jego zadań należy również koordynowanie ataków dokonujących się w sieci, ogłaszanie alarmów i zajmowanie się bieżącymi zgłoszeniami, a także przeprowadzanie badań związanych z bezpieczeństwem w sieci (CESIRT). W ramach zespołu został utworzony system ARAKIS-GOV, który wykorzystywany jest do wczesnego ostrzegania o zagrożeniach w Internecie, a także badania bezpieczeństwa stron internetowych instytucji publicznych i tym samym usuwania wszelkich nieprawidłowości, zanim zostaną wykorzystane przez cyberterrorystów (ARAKIS – GOV).

Instytucją, która zapewnia bezpieczeństwo państwa i obywateli jest Policja. Niewątpliwie widoczna jest jej obecność w związku z zagrożeniami cyberterrorystycznymi. W ramach omawianego zagadnienia powołano Biuro do Walki z Cyberprzestępczością, które zajmuje się głównie (POLICJA GOV):

- nadzorowaniem i koordynowaniem działań na rzecz zwalczania cyberterroryzmu,
- przeprowadzaniem działań operacyjno-rozpoznawczych w odniesieniu do kwestii związanych cyberatakami,
- współpracą międzynarodową i krajową z instytucjami zajmującymi się cyberterroryzmem,
- całodobową służbą i konsultacjami, w ramach koordynacji działań Policji.

Nie ulega wątpliwości, iż powyższe zadania są niezwykle istotne dla zapewnienia bezpieczeństwa w Internecie. Ponadto w wielu województwach znajdują się wydziały zajmujące się cyberterroryzmem z zadaniami zbliżonymi do powyższego Biura. Policja odgrywa istotną rolę w walce z przestępstwami w cyberprzestrzeni. Co więcej, ze względu na rozwój technologiczny zmagać się musi z coraz to nowszymi metodami i technologiami, które mogą być wykorzystywane przez cyberterrorystów (Podkarpacka Policja Gov).

Istotna w tym zakresie jest współpraca zarówno z krajowymi, jak i międzynarodowymi organami oraz instytucjami zajmującymi się działalnością na rzecz przeciwdziałania cyberterroryzmowi. Policja współpracuje z Europolem, CEPOL-em, a także z Centrum Analiz Wywiadowczych Unii Europejskiej (PE EU). Współpraca z innymi państwami, wymiana informacji oraz doświadczeń jest niezwykle istotna, aby móc skutecznie zwalczać zjawisko cyberterroryzmu. Cyberprzestrzeń jest obszarem, który nie posiada jasno określonych granic, stąd cyberterrorysta może znajdować się w zupełnie innym miejscu podczas dokonywania ataku. Stąd całodobowa

służba Policji jest istotnym czynnikiem z zakresu przeciwdziałania przestępstwom cyberprzestrzeni. Wynika to z tego, iż nie wiadomo, kiedy przestępca rozpocznie swoją działalność, więc całodobowa służba jest nieodłącznym elementem, który zabezpieczy cyberprzestrzeń.

Niewątpliwie oprócz odpowiednich organów zajmujących się przeciwdziałaniem i zwalczaniem cyberterroryzmu istotna jest też wiedza z dziedzin technicznych. Edukacja z zakresu informatyki oraz programowania i wiedza na temat sieci są kluczowe dla organów zajmujących się ochroną cyberprzestrzeni. Organy takie jak Agencja Bezpieczeństwa Wewnętrznego oraz Policja mają coraz to trudniejsze zadania w związku z ochroną cyberprzestrzeni, jak i z pozyskiwaniem informacji na temat nowych metod wykorzystywanych przez cyberterrorystów.

Podsumowanie

Podsumowując powyższe rozważania, warto zwrócić uwagę na to, iż ze względu na gwałtowny rozwój technologiczny i dostępność do Internetu następuje wzrost działalności cyberterrorystów. Ponadto posługują się coraz to nowszymi sposobami na ukrywanie swojej działalności w cyberprzestrzeni, ponieważ dysponują zarówno potencjałem finansowym, jak i doskonale przygotowaną kadrą informatyków gotowych wykorzystać swoje umiejętności po to, aby zrealizować swoje cele.

W Polsce organami, które zapewniają bezpieczeństwo i ochronę przed cyberatakami są Agencja Bezpieczeństwa Wewnętrznego i Policja. Dzięki utworzonym w ramach ich struktur organów, a także współpracy międzynarodowej z innymi państwami, istnieje realna możliwość ograniczenia działalności cyberterrorystów. Ponadto analiza badań incydentów i ataków w cyberprzestrzeni jednoznacznie wskazuje na istotę prowadzenia działań, mających na celu monitorowanie i zabezpieczanie informacji w cyberprzestrzeni. Nie należy również zapominać o aspekcie prawnym, który jest jednym z istotnych elementów przeciwdziałania cyberatakom. Stworzenie aktów prawnych z zakresu cyberprzestępczości może przysłużyć się jako skuteczne narzędzie mające na celu odstraszenie potencjalnych cyberterrorystów.

Nie ulega wątpliwości, iż oprócz działalności organów zajmujących się obszarem cyberbezpieczeństwa, szczególną uwagę powinno się zwrócić na problem bezpieczeństwa systemów informatycznych oraz edukacji użytkowników i osób decydujących o bezpieczeństwie systemów teleinformatycznych.

BIBLIOGRAFIA

[1] *Biuro do Walki z Cyberprzestępczością*, https://policja.pl/pol/kgp/bwc/33358,Biuro-do-Walki-z--Cyberprzestepczoscia.html [dostęp: 23.06.2021].

[2] *Cyberterroryzm*, https://zpe.gov.pl/a/cyberterroryzm/D4HRR86ro [dostęp: 20.06.2021].

[3] Czyżak, M., 2010. *Wybrane aspekty zjawiska cyberterroryzmu*. Telekomunikacja i Techniki Informacyjne, nr. 1-2.

[4] Liedel, K., 2006. *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń: Wyd. Adam Marszałek.

[5] Makarski, A., 2010. *Centrum Antyterrorystyczne Agencji Bezpieczeństwa Wewnętrznego. Geneza, zasady działania oraz doświadczenia po pierwszym roku funkcjonowania*. Przegląd Bezpieczeństwa Wewnętrznego, nr. 2 (2).

[6] Oleksiewicz, I., 2017. *Rola służb specjalnych w polityce zwalczania cyberterroryzmu RP*. Humanities and Social Sciences, nr. 24 (3).

[7] Oleksiewicz, I., 2018. *Cyberterroryzm jako realne zagrożenie dla Polski*. Rocznik Bezpieczeństwa Narodowego, nr. 1.

[8] Polityka Ochrony cyberprzestrzeni Rzeczypospolitej Polskiej, 2013.

[9] Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016, 2010.

[10] Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Dz.U. z 2002 r. Nr 74, poz. 676 z późn. zm.

[11] *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024,* https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024 (dostęp: 20.06.2020).

[12] *Struktura organizacyjna KWP*, http://bip.podkarpacka.policja.gov.pl/KPR/struktura-organizacyjn/30734,Struktura-organizacyjna.html (dostęp: 23.06.2021).

[13] *System ARAKIS-GOV*, https://csirt.gov.pl/cer/system-arakis-gov/310,System-ARAKIS-GOV.html (dostęp: 22.06.2020).

[14] *Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego*, https://csirt.gov.pl/ (dostęp: 22.06.2021).

[15] *Współpraca policyjna*, https://www.europarl.europa.eu/factsheets/pl/sheet/156/wspolpraca--policyjna (dostęp: 23.06.2021).