Studia z zakresu nauka prawnoustrojowych.
Miscellanea 2023, Tom XIII

KRYMINALNE ZAGROŻENIA W SIECI DLA BEZPIECZEŃSTWA PUBLICZNEGO – PROFILAKTYKA I REAGOWANIE

Dr Katarzyna Lenczowska-Soboń
Uniwersytet Marii Curie-Skłodowskiej, Prokuratura Okręgowa w Lublinie
e-mail: lenczowska@wp.pl, https://orcid.org/0000-0002-1888-1665

Asp. szt. dr Kamil Samiczak
Zakład Służby Kryminalnej Szkoły Policji w Katowicach
e-mail: kamil_samiczak@op.pl, https://orcid.org/0000-0002-9486-6168

Streszczenie: Niezależnie od wielu zalet, które wynikają z rozwoju cyberprzestrzeni, z uwagą analizować też trzeba zagrożenia z tym obszarem związane. Jak wskazano we wstępie artykułu środowisko cyberprzestrzeni jest idealnym miejscem dla przestępców internetowych czy hakerów, którzy wraz z postępem technologii są coraz bardziej efektywni i posiadają dostęp do coraz pilniej strzeżonych informacji. Cyberprzestrzeń jest też źródłem wielu zagrożeń dla bezpieczeństwa zewnętrznego, jaki i wewnętrznego państwa. Użytkownicy końcowi, administratorzy, osoby odpowiadające za bezpieczeństwo powinny zatem szczególnie pamiętać o podstawowych regułach związanych z utrzymaniem bezpieczeństwa. Między innymi o aktualizowaniu systemu operacyjnego, dbaniu o poprawną konfigurację antywirusowego oprogramowania.

Dla zapewnienia bezpieczeństwa funkcjonowania systemu informatycznego ważne jest nie tylko rozpoznanie zagrożenia czy redukowanie potencjalnych możliwości ataku, ale również ochron istotnych z perspektywy państwa systemów informatycznych. Autorzy wskazują także na potrzebę wyspecjalizowania podmiotów zajmujących się konkretnymi badaniami i analizami z obszaru cyberprzestępczości. Laboratoria, które będą miały dostęp do najnowszych instrumentów informatycznych, zatrudniając ekspertów w swoich specjalizacjach, realizując ściśle normy certyfikujące, świadomie współpracując ze sobą – na wzór sieci ENFSI - są w stanie nadążyć za nowymi sposobami działania przestępców. Zadaniem informatyki kryminalistycznej jest wprowadzenie jak również rozpowszechnienie zasad dotyczących procesu identyfikacji w zakresie dowodu cyfrowego, opracowanie na tym polu dobrych praktyk oraz szerokie rozpowszechnienie ich w procesie edukacji kadr wymiaru sprawiedliwości ale także kształcenia społeczeństwa już na etapie szkolnictwa podstawowego oraz średniego. Bez rozpowszechnienia się wiedzy informatycznej nie ma możliwości na przeprowadzenie szybkiego, skutecznego i zakończonego sukcesem postępowania karnego w sprawach związanych z dowodem cyfrowym.

Z uwagi na globalny charakter Internetu niezbędne wydaje się opracowanie aktów prawnych regulujących aspekty prawne obszarów związanych z cyberbezpieczeństwem w taki sposób, aby stosowny organ mógł monitować na bieżąco wszelkie pojawiające się nieprawidłowości, które mogą zagrozić nie tylko państwu, ale też pojedynczemu użytkownikowi.

W celu zwiększenia bezpieczeństwa w cyberprzestrzeni państwo polskie, jak się wydaje, powinno zwiększyć nacisk nie tylko na profilaktykę korzystania z Internetu, ale także powinno zadbać o uświadomienie społeczeństwa na każdym etapie rozwoju w kwestii zagrożeń w sieci, na które jest ono narażone. Z uwagi na ciągły progres technologii niezbędne jest szkolenie większej liczby specjalistów zajmujących się bezpieczeństwem teleinformatycznym, po to, by byli oni w stanie na bieżąco rozpoznawać nowe rodzaje zagrożeń i reagować na nie możliwie ja najszybciej. Ważna jest również dbałość o ochronę najważniejszych systemów teleinformatycznych Polski. Powinno się także realizować ćwiczenia sprawdzające odporność polskiej infrastruktury na ataki cybernetyczne zwłaszcza te o charakterze militarnym.

W Stanach Zjednoczonych Ameryki trwają prace nad tworzeniem poziomów prywatności dostępu użytkowników do danych w sieci. Być może tego typu rozwiązania mogłyby także przyczynić się do poprawy bezpieczeństwa osób korzystających z sieci w Rzeczpospolitej Polskiej.

Słowa kluczowe: cyberprzestępczość, cyberbezpieczeństwo, kryminalne zagrożenie, profilaktyka, internet.

W językach słowiańskich słowo „zagrożenie" związane jest ze słowem „groza", które oznacza to co powoduje lęk, strach, trwogę. Od tego też słowa pochodzą określenia: grozić, groźba, zagrażać, zagrożenie, które pozostają antytezą do słowa bezpieczeństwo[1]. W języku polskim termin ten jest charakteryzowany następująco jako zagrożenie, sytuacja lub stan, które komuś zagrażają lub w których ktoś czuje się zagrożony; też: ktoś, kto stwarza taką sytuację, natomiast czasownik, „zagrozić — zagrażać" oznacza postraszyć kogoś, aby zmusić go do określonego zachowania lub stać się dla kogoś lub czegoś realnym niebezpieczeństwem[2]. To rozumienie stało się podstawą do przeanalizowania tego terminu na przykładzie zagrożeń w sieci, które mogą mieć wpływ na bezpieczeństwo publiczne.

W oparciu o wnikliwą analizę licznych opracowań naukowych można przyjąć, że bezpieczeństwo, w odniesieniu do jednostki, to stan wewnętrzny, indywidualnie konfigurowany, dający poczucie pewności istnienia i gwarancje jego zachowania oraz szanse na jego doskonalenie[3]. Poczucie bezpieczeństwa to jedna z podstawowych potrzeb, jakimi kieruje się człowiekiem, a tym samym jest jedną z zasadniczych wartości pożądanych przez państwa, grupy społeczne oraz jednostki. Wyraża się to chociażby w Konstytucji w art. 5, która na poziomie państwa, wskazuje na konieczność zapewnienia bezpieczeństwa obywatelom[4]. Bez-

1 J. Olchowski, *Zagrożenia bezpieczeństwa*, [w:] Polska w systemie bezpieczeństwa międzynarodowego, Warszawa 2016, s. 43.

2 https://sjp.pwn.pl/szukaj/zagro%C5%BCenie.html [29.12.2022].

3 Por. L. F. Korzeniowski, *Podstawy nauk o bezpieczeństwie*, Warszawa 2012, s. 76.

4 Konstytucja RP, Dz.U. 1997 poz. 483 z późn. zm.

pieczeństwo ma także wymiar społeczny. Życie społeczne to nieustanne tworzenie warunków bezpieczeństwa, przeciwdziałania jego zagrożeniom, poszukiwanie poczucia bezpieczeństwa. Jest to zauważalne tym bardziej, że we współczesnej, coraz bardziej złożonej i zmiennej rzeczywistości społecznej, bezpieczeństwo jest dynamicznym, podlegającym złożoności oraz zmianie, procesem. Zmianie podlegają przede wszystkim jego zagrożenia ściśle związane z bezpieczeństwem[5]. Obok zagrożeń tzw. tradycyjnych (militarnych), tj. zagrożenia granic państwa czy ataku ze strony innego państwa, pojawiły się zagrożenia pozamilitarne o charakterze ekologicznym, surowcowo-energetycznym itp[6]. Już kilkadziesiąt lat temu przestano je utożsamiać tylko i wyłącznie ze zbrojnym atakiem jednego państwa na drugie[7]. Bezpieczeństwo jest naczelną potrzebą nie tylko jednostki, ale także grupy społecznej. Jest również naczelnym celem działań państw i systemów międzynarodowych[8].

Jednym z istotniejszych zagrożeń we współczesnym świecie wydaje się zagrożenie dla bezpieczeństwa informacyjnego i telekomunikacyjnego (teleinformatycznego) Polski. Dokonującym się przemianom w naszym kraju towarzyszyła popularyzacja komputerów osobistych (PC), zarówno wśród indywidualnych użytkowników, jak i w strukturach administracji państwowej różnych szczebli. W drugiej połowie lat dziewięćdziesiątych dwudziestego wieku, w sieci pojawiły się także pierwsze portale informacyjne, a z nimi różnego rodzaje wirusy komputerowe[9].

Jednym z pierwszych bardzo poważnych (ze względu na skalę reperkusji) naruszeń w obszarze bezpieczeństwa dla działania komputerów oraz systemów komputerowych było pojawienie się wirusa komputerowego o nazwie Cornell virus. Działanie jego okazało się tak niszczące, że zagrażało zasobom nie tylko najważniejszych uniwersytetów w Stanach Zjednoczonych Ameryki, ale też wynikom badań prowadzonych w NASA (National Aeronautics and Space Administration), co w rezultacie przyniosło negatywne konsekwencje w obszarze gospodarki narodowej USA. W pewnym momencie doszło też do tego, że wirusami komputerowymi zostały zagrożone systemy komputerowe armii amerykańskiej. Uaktywnienie się tego typu zagrożeń w sieci w trakcie kryzysów militarnych mogłoby spowodować porażenie centralnych ośrodków dowodzenia[10].

5 Por. A. Włodkowska-Bagan, *Wymiar polityczny i militarny bezpieczeństwa Polski*, [w:] Polska w systemie bezpieczeństwa międzynarodowego..., op. cit., s. 77-97.

6 J. Olchowski, *Zagrożenia bezpieczeństwa*, [w:] Polska w systemie bezpieczeństwa międzynarodowego..., op. cit., s. 41.
Por. T. Młynarski, *Wymiar energetyczny bezpieczeństwa Polski*, [w:] Polska w systemie bezpieczeństwa międzynarodowego..., op. cit., s. 117-131.

7 M. Pietraś, K. A. Wojtaszczyk (red.), *Polska w systemie bezpieczeństwa międzynarodowego*, Warszawa 2016, s. 7.

8 Ż. Ściborek, B. Wiśniewski, R. B. Kuc, A. Dawidczyk, *Bezpieczeństwo Wewnętrzne Podręcznik Akademicki*, Wydawnictwo Adam Marszałek, Toruń 2015, s. 24.

9 M. Lakomy, *Wymiar informacyjny i telekomunikacyjny bezpieczeństwa Polski*, [w:] Polska w systemie bezpieczeństwa międzynarodowego..., op. cit., s. 134-138.

10 M. Białkowski, *Ocena prawna i kryminalistyczna przestępczości komputerowej*, Wydanie I, Warszawa 2016, s. 26.

W czasach postępującej globalizacji, cyfryzacji i komunikacji przy wykorzystaniu sieci teleinformatycznych obszar bezpieczeństwa systemów IT przestaje być wyłącznie przedmiotem zainteresowania specjalistów w tym zakresie. Internet jest jednym z podstawowych kanałów komunikacyjnych i informacyjnych na świecie. Rozwój tego obszaru życia, spowodował, że coraz więcej czynności wykonywanych jest przy użyciu internetu. Stosowanie podpisów elektronicznych, korzystanie przez użytkowników z portali rozrywkowych, społecznościowych, posiadanie kont bankowych w sieci, wizualizacja rzeczywistości, sztuczna inteligencja czy ogólnoświatowa wymiana informacji – to wszystko nie jest dla przeciętnego człowieka czymś zaskakującym, korzystamy bowiem z tych dóbr niemalże każdego dnia. Wraz z rozwojem technologii informatycznych oraz cyfryzacji zaczęło się rozwijać środowisko hakerów i cracerów. O ile hakerzy uważają się za osoby dla których naczelną zasadą jest wolność. Wolność w trzech wymiarach: tworzenia, dostępu do wiedzy i wolności dzielenia się nią[11]. Cracerzy zaś to osoby odpowiedzialne za tworzenie szkodliwego oprogramowania, wymierzonego w integralność i poufność informacji oraz ciągłość działania systemów informatycznych. To zaowocowało powstaniem nowego rodzaju przestępczości tzw. cyberprzestępczości, w szerokim rozumieniu tego pojęcia. Pojęcia te jednak w praktyce są traktowane synonimicznie.

Z perspektywy informatycznej na zagrożenia teleinformatyczne można spojrzeć przede wszystkim przez pryzmat stosowanych metod i technik ataków komputerowych. Do stosowanych najczęściej ataków przez cracerów można zaliczyć m. in.:

1. Wkorzystywanie oprogramowania złośliwego (wirusy komputerowe, trojany, robaki, rootkity i inne).
2. Dentail of Service/ Distributed Denial of Service (odmowa dostępu).
3. Ataki sieciowe (network attacs).
4. Wykorzystywanie sieci bonet.
5. Ataki socjotechniczne (social engineering),
6. Ataki na hasła (np. ataki typu bruteforce),
7. Wstrzyknięcie polecenia SQL aplikacji internetowej (SQL injection).

Biorąc pod uwagę motywacje sprawców można wymienić także inne zagrożenia, tj. :

1. Cyberprzestępczość.
2. Cyberterroryzm.
3. Haking.
4. Haktywizm.
5. Cyberszpiegostwo.
6. Różnego rodzaju operacje o charakterze zbrojnym w cyberprzestrzeni[12].

To spowodowało konieczność podjęcia radykalnych działań zarówno na szczeblu międzynarodowym jak i krajowym. Aby przeciwdziałać ingerencji w funkcjonowanie systemów informatycznych, zarówno sektor rządowy, jak i prywatny, wprowadza coraz większą liczbę zabezpieczeń. Firmy zajmujące się oprogramowaniem

11 K. Piotrowicz, *Etyka hakera. Wyzwanie dla konsumeryzmu*, [w:] T. Szlendak, K. Piotrowicz (red.), Na pokaz. O konsumeryzmie w kapitalizmie bez kapitału, Toruń 2001, s. 203-204.

12 Zob. M. Lakomy, *Zagrożenia dla bezpieczeństwa teleinformatycznego państw - przyczynek do typologii*, „e-Politikon" 2013, nr 6.

antywirusowym oferują coraz to nowsze i efektywniejsze aktualizacje stworzonych przez siebie programów. Ponadto, o czym szerzej traktować będą kolejne części artykułu, szczególnie istotne wydaje się informowanie o zagrożeniach, na które narażają się użytkownicy Internetu, przez różnego rodzaju kanały przepływu informacji np. portale społecznościowe, blogi eksperckie, telewizję cyfrową i prasę itp.[13], a także powołane ku temu instytucje jak przykładowo Cert Polska. Niezabezpieczona lub źle zabezpieczona sieć bezprzewodowa umożliwia podłączenie się do niej osobom nieupoważnionym, a tym samym otwiera dostęp do naszych danych, a co gorsze – pozwala na popełnianie czynów karalnych przy użyciu naszych kont. Co więcej sieci bezprzewodowe są używane do wykonywania min: przelewów internetowych, przesyłania danych firmowych, przesyłania danych zawierających dane osobowe oraz wielu innych czynności, w trakcie których posługujemy się istotnymi poufnymi informacjami. Warto wiedzieć, że wszystkie te informacje mogą być wykorzystane przeciwko nam, co może mieć nieprzyjemne dla nas konsekwencje. Aby zapobiec tego typu sytuacjom i przejęciu naszych danych przez podmiot do tego nieuprawniony, należy wykonać kilka prostych czynności. Po zakupie nowego komputera czy routera/przełącznika, użytkownik powinien od razu zmienić hasło na routerze: dokonać zmiany domyślnego loginu i hasła punktu dostępowego. Kolejno powinno zarządzać się punktem dostępowym za pomocą kabla: ograniczenie możliwości konfigurowania punktu dostępowego za pomocą kabla znacznie ogranicza możliwości ataku na nasz system. Moc nadawania powiązana jest z umiejscowieniem urządzenia: punkt dostępu powinien być umiejscowiony w centralnym punkcie mieszkania/domu. Szyfrowanie danych to jedno z podstawowych zabezpieczeń, które należy zastosować w naszej sieci. Brak szyfrowania sprawia, że nasze dane są przesyłane w sieci w sposób niemalże jawny. Uważać trzeba także przy zmianie nazwy sieci. Wpisując nową nazwę sieci, nie należy pomagać jej w identyfikacji, na przykład stosując imię/nazwisko właściciela. Filtrowanie adresów karty nie stanowi wystarczającego zabezpieczenia przed atakiem[14].

Tematyka związana z cyberprzestępczością staje się centrum zainteresowania nie tylko wśród prywatnych pracodawców, ale także administracji publicznej czy gospodarki korzystającej ze współczesnych technologii informatycznych, ułatwiających przedsiębiorcom uruchamianie nowych kanałów generowania dochodów, a także docierania do nowych rynków zbytu. Dlatego też istotne jest diagnozowanie sieci w zakresie zapewnienia bezpieczeństwa wskazanym wcześniej podmiotom. Warto także nadmienić, że użytkownikami sieci mogą być osoby niepełnoletnie, dlatego też idąc śladem małopolskiej Policji zasadnym jest edukowanie najmłodszych już w pierwszych klasach szkoły podstawowej co do grożących w Internecie niebezpieczeństw. Projekt „Zagrożenia w Sieci – profilaktyka**,** reagowanie" powstał jako odzew na zapotrzebowanie zgłaszane przez nauczycieli i rodziców,

13 A. Waloch, *Współczesne zagrożenia dla bezpieczeństwa państwa polskiego w cyberprzestrzeni*, „Studia de Securitate. Annales Universitas Paedagogicae Cracoviensis" 2019, 9(4), s. 1.

14 T. Pawlicki, *Bezpieczeństwo sieci Wi-Fi*, [w:] J. Czapska, A. Okrasa, Bezpieczeństwo - policja - kryminalistyka, Wydanie I, Kraków 2015, s. 291-293.

którzy dostrzegają problemy, z jakimi spotykają się dzieci – już na etapie szkolenia podstawowego. Dzięki zaangażowaniu i wsparciu Urzędu Marszałkowskiego Województwa Małopolskiego opracowano i wdrożono projekt szkoleniowy. Od samego początku w jego realizację jako partnerzy – oprócz Policji – włączyło się Kuratorium Oświaty w Krakowie oraz przedstawiciele Naukowej i Akademickiej Sieci Komputerowej (NASK). Prowadzone działania edukacyjne i informacyjne związane były z tematyką cyberzagrożeń, Obejmowały one edukowanie dzieci z klas czwartych, piątych i szóstych wszystkich szkół podstawowych województwa małopolskiego oraz nauczycieli pracujących z tymi uczniami, a także rodziców uczniów.

W trakcie prowadzonych spotkań z dziećmi policjanci omawiali następujące zagadnienia:
Czym jest Internet i do czego służy?
Jak bezpiecznie korzystać z Internetu przy użyciu wyszukiwarek internetowych?
Do czego służy poczta internetowa i jak z niej korzystać?
Co to jest i jak działa internetowe forum?
W jaki sposób korzystać z czatów i komunikatorów internetowych?
Z jakimi zagrożeniami można się spotkać w sieci i jak się zachować w takiej sytuacji?
Z kim niezwłocznie należy się wtedy skontaktować?[15].

Kolejny projekt edukacyjny „Przystań w sieci" skierowany został zarówno do nauczycieli, jak i uczniów w całym kraju. Twórcami projektu byli Facebook, NASK i UNICEF Polska. Zadaniem zasadniczym tego projektu było zwrócenie uwagi na zagrożenia, jakie mogą pojawić się w sytuacji pracy w trybie „online"[16]. Uczniowie i nauczyciele, jak również pedagodzy, psychologowie oraz bibliotekarze, na platformie e-learningowej mogli zapoznać się z takimi modułami edukacyjnymi jak: cyberzagrożenia, cyberprzemoc, prywatność w sieci, szkodliwe i niebezpieczne treści, ślady cyfrowe i reputacja online, a także informacje fałszywe. Szkolenia te obejmowały zagadnienia dotyczące świadomego i bezpiecznego korzystania z mediów społecznościowych oraz Internetu.

Projekty tego typu są istotne, gdyż wiedza dotycząca cyberbezpieczeństwa trafia do coraz większej dzięki nim jakąś część społeczeństwa, przede wszystkim zaś młodych obywateli państwa – być może także tych, którzy w przyszłości zasilą szeregi organów ścigania i wymiaru sprawiedliwości.

Rozwój Internetu zapoczątkował wiele zmian społeczno-ekonomicznych oraz politycznych we współczesnym świecie. Jego dynamizacja, a także całej sfery informatycznej, sprawia, że jest najszybciej rozwijającym się segmentem życia społecznego[17]. Oprócz wielu zalet, jakie posiada, jego rozwój stanowi też jedną z podstawowych przyczyn wzrostu zagrożenia cyberprzestępczością. Stosowanie

15 https://malopolska.policja.gov.pl/krk/dziala/prewencja/projek/zagrozenia-w-sieci/1275,Zagrozenia-w-Sieci-profilaktyka-reagowanie.html [03.10.2022].

16 https://akademia.nask.pl/przystan-w-sieci--cyberbezpieczenstwo-przede-wszystkim.html [12.10.2022].

17 B. Hołyst, K. Jałoszyński, A. Letkiewicz, *Wojna z terroryzmem w XXI wieku*, Szczytno 2009, s. 109.

zwyczajowych rozwiązań prawnych do cyberprzestrzeni okazało się niemożliwe, a granice, w których działały organy państwowe są niewystarczająco szerokie i nie obejmują wszystkich zagrożeń. Nadużycia komputerowe stanowią zagrożenie nie tylko dla bezpieczeństwa krajowego, lecz również międzynarodowego. Skutki tych nadużyć widoczne są zwłaszcza od kilku miesięcy w przekazie informacji medialnych (w tym także w internecie), a dotyczącą konfliktu zbrojnego pomiędzy Rosją a Ukrainą.

W takiej sytuacji konieczna jest szczególna dbałość o samoświadomość i pełną edukację wśród służb zajmujących się bezpieczeństwem wewnętrznym i zewnętrznym kraju.

W przeprowadzonych badaniach[18] – w tym dotyczących Polski – ujawniono, że podstawowymi źródłami wiedzy dla policjantów w tym zakresie pozostają Internet oraz koledzy i znajomi. Jest to zjawisko niepokojące, świadczy bowiem o braku usystematyzowanej wiedzy na temat problemu, z którym badani spotykają się coraz częściej i do którego zwalczania powinni być profesjonalnie przygotowani. Specyfika przestępstw popełnianych w cyberprzestrzeni powoduje, że wiele czynów tego typu pozostaje niewykrytych lub nie jest poprawnie identyfikowana jako przestępstwo. Przyczyną takiej sytuacji często staje się właśnie brak technicznej świadomości samego użytkownika komputera lub innego urządzenia, na temat tego, że padł właśnie ofiarą cyberprzestępcy. Jeśli policjantowi zabraknie wiedzy w tym zakresie, nie będzie w stanie określić czy doszło do przestępstwa, jakiego jest rodzaju ani w jaki sposób prawidłowo go penalizować [19], a w konsekwencji przeprowadzić skutecznego postępowania wykrywczego.

Ze względu na transgraniczny charakter omawianego zjawiska bezpieczeństwo cyfrowe stało się przedmiotem zainteresowania wszystkich członków społeczeństwa informacyjnego. Cyberprzestępczość[20] uznano za jeden z najpoważniejszych problemów, z którym aktualnie zmierzyć się muszą organy ścigania. Rozwój – poprzez pierwotne sieci typu ARPANET – do stopniowego konstytuowania się sieci lokalnych to był dopiero początek rozkwitu nowej przestrzeni społecznej, jaką powoli stawał się Internet. Około 30 lat temu znacząco wzrosło użycie komputerów osobistych, a firmy telekomunikacyjne zaczęły przejawiać zainteresowanie usługami sieciowymi. Wzrost znaczenia sieci był związany z rozszerzeniem jej zasięgu,

18 T. Pączkowski, *Cyberprzestępczość w województwie śląskim. Studium z socjologii ryzyka – rozważania na temat świadomości policjantów*, przedmiotem pracy było ustalenie źródeł wiedzy badanych policjantów na temat cyberprzestępczości. praca doktorska zasoby Uniwersytetu Śląskiego w Katowicach, Katowice 2019.

19 T. Pączkowski, *Cyberprzestępczość...*, op. cit., s. 260-261. Zob. R. Balkowski, *Bezpieczeństwo systemów teleinformatycznych - zmiany, trendy i zasady*, [w:] Poradnik Klienta Usług Finansowych, Wyd. Komisja Nadzoru Finansowego, Warszawa 2018, s. 7.

20 Cyberpczestępczość jest formą zagrożeń teleinformatycznych. W zasadzie każde działanie w cyberprzestrzeni, które łamie obowiązujące prawo, można szerzej rozumieć jako cyberprzestępczość. Świadczą o tym np. uregulowania Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej z 2013 r., gdzie zdefiniowano ten termin jako czyn zabroniony popełniony w obszarze cyberprzestrzeni. por. Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej z 2013 r.

w związku z czym nie stawiano też żadnych przeszkód przed dołączającymi się sieciami. Nadzór nad Internetem amerykańskiego Departamentu Obrony skończył się w momencie, gdy udział cywilnych użytkowników zaczął stwarzać realne niebezpieczeństwo dla tajności projektu. Komercjalizacja Internetu stała się faktem[21]. Tak samo jak powszechność i dostępność do Internetu.

Statystyki CERT Polska działającego przy NASK jednoznacznie pokazują, że z roku na rok rośnie liczba cyberataków. W 2018 r. liczba zarejestrowanych incydentów była o 17,5% większa w stosunku do 2017 r., a w 2016 r. aż o 32% większa niż w 2015 r.[22]. Zgodnie z informacjami prasowymi, które pojawiły się w połowie 2018 r., średnio 700 razy na godzinę podejmowane są próby cyberataków na Polskę[23]. Statystyki dotyczące zgłaszanych incydentów w 2021 to łącznie 29 483 unikalne incydenty cyberbezpieczeństwa. Jest to wzrost o 182% w stosunku do roku poprzedniego. Najczęstszym typem incydentu wciąż jest phishing[24].

Odpowiedzią na coraz większą liczbę zagrożeń w Internecie są inicjatywy prawodawcze z zakresu cyberbezpieczeństwa w ramach Unii Europejskiej, takie jak uchwalona 6.7.2016 r. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, zwana Dyrektywą NIS (ang. *Directive on security of network and information systems, NIS Directive)*. Przyjmując Dyrektywę NIS, UE nie powiedziała ostatniego słowa w zakresie ram prawnych cyberbezpieczeństwa. We wrześniu 2017 r. został przedstawiony tzw. pakiet cyberbezpieczeństwa, elementem którego był Komunikat KE „Odporność, prewencja i obrona: Budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej" oraz projekt Cybersecurity Act. Cybersecurity Act składa się z dwóch części: nowego, permanentnego mandatu dla Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA), której rola została znacznie wzmocniona, a także rozporządzenia tworzącego europejskie ramy certyfikacji cyberbezpieczeństwa dla produktów i usług ICT. Jest to druga, po dyrektywie NIS, regulacja prawna w zakresie cyberbezpieczeństwa na poziomie europejskim.

Stworzenie spójnego systemu mającego zapewnić cyberbezpieczeństwo Rzeczypospolitej Polskiej było celem Ustawy z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa**,** która implementuje dyrektywę NIS i ma charakter przełomowy, gdyż po raz pierwszy tworzy w Polsce całościowy prewencyjny system cyberbezpieczeństwa, obejmujący m.in.: dostawców usług cyfrowych, operatorów usług kluczowych, podmioty publiczne, podmioty świadczące usługi z zakresu cyberbezpieczeństwa, organy właściwe do spraw cyberbezpieczeństwa, powołano trzy Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego działające na poziomie krajowym (CSIRT GOV, CSIRT NASK i CSIRT MON) oraz sektorowe zespoły cyberbezpieczeństwa. Ustawa powołuje do życia Pojedynczy Punkt Kon-

21 I. Jaroszewska, *Wybrane aspekty przestępczości w cyberprzestrzeni Studium prawno karne i kryminologiczne*, KPP Monografie, Kortowski Przegląd Prawniczy Monografie, Olsztyn 2017, s. 2.

22 https://www.cert.pl/tag/statystyki /, [20.5.2019].

23 https://antyweb.pl/polska-cyberataki-dane/, [20.5.2019].

24 https://cyberpolicy.nask.pl/aktualnosci/raport-cert-polska-za-2021r/ [20.01.2023].

taktowy, Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa oraz Kolegium do Spraw Cyberbezpieczeństwa. Implementując dyrektywę NIS, zobowiązuje Radę Ministrów do przyjęcia krajowej strategii w zakresie bezpieczeństwa sieci i systemów informatycznych, określającej cele strategiczne oraz odpowiednie środki polityczne i regulacyjne, mające na celu osiągnięcie i utrzymanie wysokiego poziomu cyberbezpieczeństwa[25]. Nowe wyzwania prawne powodują również konieczność zmian w prawie, wprowadzając min nowe rozwiązania jak dokumenty eletroniczne, elektroniczny KRS i wiele innych, w ramach których wiele czynności prawnych i zdarzeń może odbywać się za pośrednictwem sieci internet.

Zagrożenia w cyberprzestrzeni można podzielić według kilku kategorii. Najbardziej dotkliwymi dla społeczeństwa są te, które dotykają bezpośrednio użytkowników sieci. Do tych, które są najbardziej dotkliwe, należą:

a. kradzieże tożsamości (identity theft),
b. wyłudzenia,
c. niszczenie i modyfikacje danych osobowych,
d. ataki przy wykorzystaniu szkodliwego oprogramowania, tj. robaki, trojany, wirusy, keyloggery czy malware.

Wśród powodów wzrostu zagrożenia przestępczością tzw. komputerową w doktrynie przedmiotu najczęściej wymienia się brak stosowanej wiedzy na temat nadużyć komputerowych, a także właściwego oprogramowania, które mogłoby wykryć potencjalne zagrożenie (np. złośliwe oprogramowanie, które działa często w ukryciu, wykorzystując luki w podstawowym oprogramowaniu bądź aktywuje się po jakimś czasie, jak wirusy, trojany czy bomby logiczne itp.). Cechą charakterystyczną tej stosunkowo nowej przestępczości jest niewielka gotowość ofiar przestępstw do angażowania Policji w ich ściganie, mimo iż szkody poniesione w wyniku tych czynów są relatywnie wysokie. Kolejną cechą charakterystyczną jest tzw. ciemna liczba incydentów, niskie prawdopodobieństwo wykrycia sprawcy oraz lekceważenie przez pokrzywdzonych zasad bezpieczeństwa[26].

Przyczyną braku składania zawiadomień do Policji o pokrzywdzeniu przestępstwami komputerowymi jest najczęściej chęć uniknięcia niepożądanego rozgłosu czy też obawa przed utratą zaufania społecznego, a czasami brak wiary w wykrycie sprawcy, szczególnie gdzy przestępstwo dotyka instytucji bądź podmiotu gospodarczego.

Blokowanie dostępu do usług, działania o charakterze socjotechnicznym

Częstym obiektem ataków cyberprzestępców są systemy IT należące do firm[27]. Nierzadko dochodzi tutaj do kradzieży cennych informacji (tajemnicy produkcji, danych osobowych pracowników). Zdarzenia te mogą zaszkodzić firmie nie tylko na

25 A. Besiekierska, *Komentarz do Ustawy o Krajowym Systemie Cyberbezpieczeństwa*, Legalis, www.sip.legalis.pl
26 M. Siwicki, *Cyberprzestępczość*, Wydawnictwo C. H. Beck, Warszawa 2013, s. 77.
27 C. Banasiński, M. Rojszczak, *Cyberbezpieczeństwo*, Warszawa 2020, s. 103.

polu finansowym, ale także wizerunkowym czy prawnym. Pamiętać trzeba, że działania ukierunkowane są na te ogniwa w łańcuchu bezpieczeństwa, które są z reguły najsłabsze. Dlatego też, żeby przeciwdziałać cyberprzestępczości, należy uwzględnić kompetencje, strukturę i umiejętności użytkowników, a także ich zdolność do postrzegania zmian.

Coraz częściej do ataków dochodzi również na różnego rodzaju organizacje publiczne, punkty strategiczne państwa. Działania te są o tyle niebezpieczne, że mogą zdestabilizować funkcjonowanie ważnych obszarów z punktu widzenia funkcjonowania podstawowych sektorów w państwie. Sprawcy włamują się do urządzeń sieciowych i modyfikują listy kontroli dostępu (access control list – ACL) po to, aby uzyskać w ten sposób dostęp do chronionych obszarów. Twórcy złośliwego oprogramowania coraz częściej stosują różnego rodzaju metody maskujące, czynią to, aby ukrywać się w środowiskach wirtualnych, w celu uniemożliwienia wykrycia ich programów za pomocą metod śledczych i analizy antywirusowej. Postępowanie takie nie jest przy tym wyzwaniem dla sprawców, gdyż znają oni metody stosowane przez organy ścigania, dlatego też stosują taktykę polegającą na skrywaniu swoich działań wśród uprawnionych operacji systemowych i sieciowych (tzw. antyforensics)[28].

Kluczowe jest w tym przypadku wprowadzanie nowych rozwiązań właśnie w celu przeciwdziałania atakom komputerowym, gdyż systemy komputerowe dysponują coraz większą pojemnością danych, a zatem wykonywanie bitowych obrazów podejrzanych systemów przy uwzględnieniu dużego incydentu może się okazać nie tylko utrudnione, ale też bardzo czasochłonne. Dlatego też, aby działania były efektywne, muszą włączyć się w nie środowiska nie tylko działów IT i bezpieczeństwa, ale także prawnicze, ekonomiczne, marketingowe, jak również pracownicy działów HR.

Stanowisko Unii Europejskiej wobec bezpieczeństwa w cyberprzestrzeni

Sieci oraz systemy i usługi informatyczne pełnią bardzo istotną rolę w społeczeństwie. Ich niezawodność oraz bezpieczeństwo to kwestie istotne dla działalności zarówno społecznej, jak i gospodarczej, a w szczególności dla prawidłowego funkcjonowania rynku wewnętrznego.

Dyrektywa Parlamentu Europejskiego i Rady Unii Europejskiej z dnia 6 lipca 2016 r. (2016/1148) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dz. Urz. UE L 194) została uchwalona, by możliwe było osiągnięcie wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii Europejskiej. Dlatego też wskazano na środki mające to bezpieczeństwo zapewnić. W tym celu ustanowiono obowiązki dla wszystkich państw należących do UE dotyczące przyjęcia krajo-

28 J. Luttgens, M. Pepe, K. Mandia, *Incydenty bezpieczeństwa. Metody reagowania w informatyce śledczej*, Gliwice 2014, s. 28.

wej strategii bezpieczeństwa sieci i systemów informatycznych. Stworzono grupę współpracy, która miałaby ułatwiać i wspierać współpracę strategiczną, a także wymianę informacji pomiędzy państwami członkowskimi. Zaprojektowano również sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego CSIRT. Ustalone zostały wymogi zgłaszania incydentów dla operatorów usług kluczowych i dostawców usług cyfrowych. Wskazano też kierunki postępowania dla państw członkowskich dotyczące wyznaczania właściwych organów krajowych, pojedynczych punktów kontaktowych oraz CSIRT, wykonujących zadania związane z bezpieczeństwem sieci, jak i systemów informatycznych[29]. Omawiana tu dyrektywa wydaje się korzystnie wpływać na działania podejmowane przez państwa członkowskie, ukierunkowane na zagwarantowanie obywatelom ich zasadniczych potrzeb, tj. na ochronę bezpieczeństwa narodowego, działań na rzecz ochrony informacji, utrzymania porządku publicznego.

Program bezpieczeństwa cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2017 – 2022

Kluczowym warunkiem zapewnienia bezpieczeństwa systemów teleinformatycznych jest dostęp do informacji o napływających zagrożeniach oraz dzielenie się informacjami o występujących lub mogących nastąpić atakach. W tym też celu trwa udoskonalanie systemu bieżącego zarządzania bezpieczeństwem cyberprzestrzeni. W oparciu o przeprowadzone analizy przekazywane będą do zainteresowanych stron ostrzeżenia na temat zagrożeń, z zachowaniem tajemnicy przedsiębiorstwa, którego dane zgłoszenie dotyczy. Natomiast w celu ochrony indywidualnych użytkowników zostanie utworzony dodatkowy system chroniący przed skutkami zidentyfikowanych zagrożeń.

Celem rządu RP, jaki stawia sobie w najbliższym czasie, jest inwestowanie nie tylko w zasoby przemysłowe, ale i technologiczne, poprzez stwarzanie warunków dla rozwoju przedsiębiorstw, ośrodków naukowo-badawczych, jak i start-upów, których zadaniem będzie udoskonalanie przyjętych i wdrażanie nowych rozwiązań. Strategia wyżej opisana jest uchwalana na okres 5 lat, a jej koordynatorem jest minister właściwy do spraw informatyzacji[30].

Zagrożenia dla bezpieczeństwa współczesnych sieci teleinformatycznych

Zagrożenia dla bezpieczeństwa w sieci można sklasyfikować w różny sposób. Podstawą klasyfikacji może być podział dotyczący rodzajów zagrożeń, jakie mogą wystąpić. Możliwe jest także uporządkowanie ich według przyczyn, miejsca powstania zagrożenia, występujących czynników socjologicznych (np. oszustwa w sieci), charakteru zagrożenia.

29 B. Hołyst, *Kryminalistyka*, Warszawa 2018, s. 1320.
30 Ibidem

Do zagrożeń sklasyfikowanych według przyczyn można zaliczyć: świadomą, celową, szkodliwą działalność człowieka, tj. terroryzm, szpiegostwo, wandalizm, sabotaż, szantaż, źle rozumiane ambicje hakerów czy cracerów. Może być to także niecelowa i nieświadoma działalność użytkownika, np. błędy w użytkowaniu, nieprzestrzeganie procedur itp. Do wspomnianej grupy zagrożeń zaliczają się także wydarzenia losowe, tj. klęski żywiołowe, wyładowania atmosferyczne, katastrofy, pożar, powodzie, zalanie wodą, awarie sprzętu i wszelkiego rodzaju wady oprogramowania. Zagrożenia związane z miejscem jego powstawania mogą mieć charakter zewnętrzny bądź wewnętrzny. Te pierwsze powstają w sieci publicznej, są to np. próby włamania do sieci internetowej przy zastosowaniu wirusów, robaków, związane z popełnieniem oszustwa, piractwa czy hackingu.

We współczesnym świecie technika jest istotnym bodźcem napędowym cywilizacji. Współczesne osiągnięcia naukowe usprawniają codzienne funkcjonowanie w społeczeństwie, ale również niosą ze sobą zagrożenia, czego rezultatem może być odczuwanie niepokoju. Nowe wynalazki i technologie mogą z jednej strony ułatwiać, z drugiej zaś utrudniać nasze życie, wpływać znacząco na stan bezpieczeństwa, naruszać równowagę ekologiczną biosfery, oddziaływać na kształt życia społecznego. Musimy mierzyć się z zagrożeniami cywilizacyjnymi. Jednym z najbardziej spektakularnych zagrożeń dla współczesnych państw jest terroryzm, którego skutkiem mogą być zarówno choroby zakaźne, skażenia środowiska, jak również zniszczenia obiektów budowlanych oraz różnego rodzaju urządzeń. Szczególnie podatne na działania terrorystyczne bywają urządzenia i obiekty infrastruktury gospodarczej, przemysłowej, kulturalnej czy komunalnej. Terroryzm jest to forma przemocy polegająca na przemyślanej akcji zastraszenia rządzących lub określonych grup społecznych w celach politycznych, ekonomicznych lub innych. Stawia sobie zwykle za cel wpływanie na władzę poprzez popełnianie przestępstw z użyciem przemocy lub groźby jej użycia. Ofiary są wybierane mniej czy bardziej przypadkowo, zazwyczaj mają znaczenie symboliczne[31].

W Polsce do wyłonienia obiektów i obszarów istotnych dla społeczności lokalnych – w celu zapewnienia odpowiedniego poziomu ich ochrony – niezbędna jest współpraca następujących organów:

- wójta, burmistrza lub prezydenta miasta (ustalenie stopnia ważności obiektu dla społeczności lokalnej, zwłaszcza w obszarze aglomeracji miejskich),
- szefa Agencji Bezpieczeństwa Wewnętrznego (określenie poziomu wrażliwości obiektu na ewentualny zamach terrorystyczny),
- wojewody (wydanie decyzji administracyjnych zawierających wykaz obiektów, które podlegają ochronie),
- komendanta wojewódzkiego Policji (zatwierdzenie planu ochrony obiektu, nadzór nad prawidłowym funkcjonowaniem służb ochrony)[32].

31 B. Bronisława, *Współczesne zagrożenia dla bezpieczeństwa publicznego*, „Zeszyty naukowe WSEI seria: ADMINISTRACJA" 2012, nr 2, s. 121.

32 W. Skomra, *Kompleksowe podejście do wyłaniania i ochrony infrastruktury krytycznej*, „Cyberbezpieczeństwo, „Kwartalnik policyjny" 2017, nr 4(43), s. 9.

Warto dodać, że zarówno ochrona fizyczna, jak i ochrona teleinformatyczna (jak i wszystkie pozostałe) muszą być traktowane równorzędnie, jako element zarządzania bezpieczeństwem[33].

Bezpieczeństwo publiczne jest wartością konstytucyjną, dla której ochrony możliwe jest ograniczenie korzystania przez obywateli z ich konstytucyjnych wolności i praw. Innymi wartościami konstytucyjnymi, które mogą być ograniczane, są m.in. porządek publiczny, ochrona środowiska, zdrowie czy moralność publiczna[34].

Wydaje się, że rozwinięcie współpracy instytucjonalnej, a także lepsze i wydajniejsze sposoby finansowania zadań związanych z cyberbezpieczeństwem powinny przynieść zamierzone efekty w postaci lepszej wydajności ochrony sieci. Jest to cel, do którego instytucje rządowe dążą, choć aktualnie nie zastosowano w pełni rozwiązań, które tworzyłyby instytucjonalną sieć systemową dla kompleksowej ochrony cyberprzestrzeni RP. Forma ataku hybrydowego, nacisków, paraliżowania systemów administracji w cyberprzestrzeni jest w tej chwili częściej stosowana niż działania konwencjonalnych armii. Warto również nadmienić, że aktywność podmiotów niepaństwowych przybrała na sile. Zwłaszcza takich jak korporacje międzynarodowe, transnarodowe grupy wywierające presję na działania rządów bądź też zorganizowane grupy o charakterze przestępczym oraz organizacje terrorystyczne. Podważona została w związku z powyższym zasada gwarantowanego wzajemnego zniszczenia w ataku jądrowym. Istotnym jest fakt, że przejęcie kontroli nad bronią jądrową przez terrorystyczne organizacje mogłoby doprowadzić do zagłady znacznej populacji ludzkości. Katalog zagrożeń ciągle się rozwija, co stanowić może poważny problem dla prawidłowego, sprawnego i efektywnego funkcjonowania instytucji, jak i indywidualnych użytkowników sieci internetowej[35].

Wybrane działania mające zapewnić bezpieczeństwo cyberprzestrzeni w Polsce

Badania przeprowadzone już kilkanaście lat temu w Polsce wykazywały, że wśród aż 40% respondentów istnieje obawa przed handlem danymi osobowymi. Natomiast około 30 % badanych sygnalizowało, że boi się rozsyłania wirusów komputerowych oraz kradzieży haseł, kodów dostępu itp.[36]. Użytkownicy końcowi, administratorzy, osoby odpowiadające za bezpieczeństwo powinny zatem szczególnie pamiętać o podstawowych regułach związanych z utrzymaniem bezpieczeństwa. Między innymi o aktualizowaniu systemu operacyjnego, dbaniu o poprawną konfigurację antywirusowego oprogramowania[37].

33 Ibidem, s. 12.

34 Art. 31 ust.3 ustawy z dnia 2 kwietnia 1997 r. *Konstytucja Rzeczypospolitej Polskiej*, Dz. U. z 1997 r., Nr 78, poz. 483, ze zm.

35 S. Szamol, *Ochrona Cyberprzestrzeni Rzeczypospolitej Polskiej w wymiarze strategicznym*, „Cyberbezpieczeństwo. Kwartalnik policyjny" 2018, nr 3(46), s. 99-100.

36 E. M. Guzik-Makaruk, *Poczucie Bezpieczeństwa obywateli w Polsce. Identyfikacja i przeciwdziałanie współczesnym zagrożeniom*, Warszawa 2011, s. 194.

37 J. Sordyl, *Ransomware - wymuszanie okupu w sieci*, „Cyberbezpieczeństwo. Kwartalnik policyjny" 2017, nr 4(43), s. 48.

Dla zapewnienia bezpieczeństwa funkcjonowania systemu informatycznego istotne są nie tylko rozpoznanie zagrożenia czy redukowanie potencjalnych możliwości ataku (tak jak wcześniej wspomnieliśmy, poprzez instalowanie lepszych systemów zabezpieczeń), ale również poprzez ochronę zwłaszcza tych istotnych z perspektywy państwa systemów informatycznych[38]. Zasadne wydawałoby się wyspecjalizowanie podmiotów zajmujących się konkretnymi badaniami i analizami z obszaru cyberprzestępczości, w tym jednostek analitycznych zajmujących się prewencją oraz podmiotów zajmujących się analizą postincydentalną. Laboratoria, które będą miały dostęp do najnowszych instrumentów informatycznych, zatrudniając ekspertów w swoich specjalizacjach, realizując ściśle normy certyfikujące, świadomie współpracując ze sobą (na wzór sieci ENFSI), są w stanie nadążyć za nowymi sposobami działania przestępców. W zakresie podmiotów zajmujących się analizą incydentalną i informatyką kryminalistyczną[39] zasadne jest wprowadzenie oraz zasad dotyczących procesu identyfikacji w zakresie dowodu cyfrowego, opracowanie na tym polu dobrych praktyk oraz szerokie rozpowszechnienie ich w procesie edukacji kadr wymiaru sprawiedliwości. Bez rozpropagowania się wiedzy informatycznej, w szczególności w służbach zajmujących się bezpieczeństwem wewnętrznym kraju, nie ma możliwości na przeprowadzenie szybkiego, skutecznego i zakończonego sukcesem postępowania karnego w sprawach związanych z dowodem cyfrowym[40].

Z uwagi na globalny charakter Internetu niezbędne wydaje się opracowanie aktów prawnych regulujących aspekty prawne obszarów związanych z cyberbezpieczeństwem w taki sposób, aby stosowny organ mógł monitować na bieżąco wszelkie pojawiające się nieprawidłowości, które mogą zagrozić nie tylko państwu, ale też pojedynczemu obywatelowi. Przykładowo, w literaturze postuluje się *de lege ferenda* wprowadzenie nowych przepisów prawnych w ustawie o Agencji Bezpieczeństwa Wewnętrznego, które umożliwiałyby śledzenie transferów elektronicznych środków płatniczych (np. bitcoinów, lightcoinów i innych kryptowalut) w czasie rzeczywistym, czyli nową formę czynności operacyjno-rozpoznawczych[41].

W celu zwiększenia bezpieczeństwa w cyberprzestrzeni państwo polskie, jak się wydaje, powinno zwiększyć nacisk nie tylko na profilaktykę korzystania z Internetu, ale także powinno w szczególności zadbać o uświadomienie społeczeństwa w kwestii zagrożeń w sieci, na które jest ono narażone (w tym zakresie można by podążać śladem opisanym wcześniej działań, podejmowanych przez przedstawicieli władz województwa małopolskiego). Z uwagi na ciągły progres technologii niezbędne jest szkolenie

38 M. Zubańska, Z. Mikołajczyk, M. Fałdowski, *Systemowe Ujęcie Bezpieczeństwa Wewnętrznego Tom 2 Zagadnienia praktyki policyjnej*, Szczytno 2019, s. 559.

39 Według dostępnych źródeł termin „informatyka kryminalistyczna" użyty został po raz pierwszy [w:] Z. Czeczot, T. Tomaszewski, *Kryminalistyka ogólna*, Toruń 1996, s. 432-438.

40 M. Szymczak, *Współczesne wyzwania informatyki kryminalistycznej w kontekście rozwijającej się cyberprzestępczości. Księga Pamiątkowa Profesora T. Widły* (przyjęte do druku), Katowice 2021, s. 13-14.

41 P. Opitek, *Kontrola transferów pieniądza bezgotówkowego w czasie rzeczywistym jako nowa forma czynności operacyjno-rozpoznawczych na przykładzie ustawy o Agencji Bezpieczeństwa Wewnętrznego (postulaty de lege ferenda)*, „Prokuratura i Prawo" 2021, nr 2, s. 154.

większej liczby specjalistów zajmujących się bezpieczeństwem teleinformatycznym, po to, by byli oni w stanie na bieżąco rozpoznawać nowe rodzaje zagrożeń i reagować na nie możliwie ja najszybciej i jak najskuteczniej. Wyszkoleni w ten sposób specjaliści powinni zajmować miejsce na każdym szczeblu struktury organizacyjnej stosownych służb, umożliwiając pełną konsultację w przypadku wystąpienia incydentu teleinformatycznego o charakterze przestępczym. Istotna jest również dbałość o ochronę najważniejszych systemów teleinformatycznych Rzeczpospolitej Polskiej. Prowadzone powinny być również ćwiczenia sprawdzające odporność polskiej infrastruktury na ataki cybernetyczne. Działania takie powinny kierować się logiką rozwoju technologii i co za tym idzie dostosowania otoczenia prawnego do nowej sytuacji.

Jedną z jednostek organizacyjnych utworzonych m.in. do ochrony systemów informatycznych jest Centralne Biuro Zwalczania Cyberprzestępczości. Zgodnie z ustawą z dnia 17 grudnia 2021 r. o utworzeniu Centralnego Biura Zwalczania Cyberprzestępczości stworzono nową jednostkę organizacyjną Policji właściwą do rozpoznawania i zwalczania przestępstw popełnianych przy użyciu systemu informatycznego, systemu teleinformatycznego, zapobiegania tym przestępstwom, jak również wykrywania oraz ścigania ich sprawców[42]. Odpowiada to założeniom nakreślonym w Strategii Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z roku 2022, w ramach której wskazano, że szczególnym wyzwaniem dla bezpieczeństwa Polski, podobnie jak pozostałych Państw wysokorozwiniętych, w tym naszych bliskich sojuszników i partnerów, będą negatywne oddziaływania w cyberprzestrzeni, wynikające z celowego lub nieumyślnego działania człowieka bądź wywołane awarią albo nieszczęśliwym wypadkiem, zakłóceniem funkcjonowania infrastruktury teleinformatycznej[43]. Według Komendy Głównej Policji zagrożenie w związku z przestępczością przy wykorzystaniu Internetu i pozostałych dróg elektronicznych jest coraz większe, co w rezultacie doprowadziło do utworzenia nowej struktury w ramach Komendy Głównej Policji – od dnia 12 stycznia 2022 roku funkcjonuje Centralne Biuro Zwalczania Cyberprzestępczości[44]. Biuro do Walki z Cyberprzestępczością realizuje zadania związane z tworzeniem warunków do efektywnego wykrywania sprawców przestępstw popełnionych przy użyciu nowoczesnych technologii teleinformatycznych. Do zadań Biura do Walki z Cyberprzestępczością należą w szczególności:

1. Nadzorowanie, koordynowanie i wspieranie ukierunkowanych na zwalczanie cyberprzestępczości działań prowadzonych przez komendy wojewódzkie (Sto-

42 Poza CBZC, które funkcjonuje od 12 stycznia 2022 r., 8 lutego b.r. podczas konferencji w Wojskowej Akademii Technicznej minister obrony narodowej M. Błaszczak, ogłosił powołanie nowego komponentu Sił Zbrojnych Rzeczypospolitej Polskiej - Wojska Obrony Cyberprzestrzeni. Są one przeznaczone do przeprowadzenia w cyberprzestrzeni działań o charakterze obronnym oraz, w razie potrzeby, działań ofensywnych. Mają one przyczynić się do zapewnienia wyższego poziomu bezpieczeństwa w cyberprzestrzeni, której obrona należy do podstawowych zadań kolektywnej obrony NATO, co potwierdzono podczas szczytu NATO w Warszawie w 2016 r. por. https://www.gov.pl/web/obrona-narodowa/wojska-obrony-cyberprzestrzeni-rozpoczynaja-dzialalnosc.

43 Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z roku 2022, s. 33.

44 Portal internetowy polskiej policji, *Centralne Biuro Zwalczania Cyberprzestępczości – nowy rodzaj służby w Policji*, www.policja.pl/pol/cbzc, [10.05.2022].

łeczną) Policji w zakresie czynności operacyjno-rozpoznawczych oraz współdziałanie z Centralnym Biurem Śledczym Policji w tym zakresie.
2. Prowadzenie czynności operacyjno-rozpoznawczych pozostających we właściwości biura.
3. Inicjowanie i prowadzenie współpracy z organami administracji rządowej, sądami, prokuraturami, instytucjami państwowymi, a także podmiotami prywatnymi w zakresie zadań pozostających we właściwości biura.
4. Prowadzenie współpracy międzynarodowej oraz współdziałanie z Biurem Międzynarodowej Współpracy Policji w zakresie zadań pozostających we właściwości biura.
5. Prowadzenie całodobowej służby mającej na celu koordynowanie działań Policji w zakresie zagrożeń przestępstwami w sieci Internet, ich zwalczania oraz współdziałania jednostek organizacyjnych Policji z krajowymi i zagranicznymi organami i podmiotami pozapolicyjnymi.
6. Prowadzenie konsultacji technicznych, inicjowanie i wspieranie badań oraz projektów, a także współpraca z podmiotami krajowymi i zagranicznymi zmierzająca do rozpoznawania i implementowania nowoczesnych rozwiązań w walce z cyberprzestępczością[45].

Służba ta, której stan etatowy docelowo wynosił będzie około 1800 etatów policyjnych, zajmuje się ujawnianiem i zwalczaniem cyberprzestępczości[46] niezależnie od sposobu działania sprawców lub organizacji. Zatrudnieni funkcjonariusze Policji mają posiadać kompetencje z zakresu bezpieczeństwa informatycznego (*computer forensic*) oraz zwalczania przestępczości komputerowej[47] lub przestępczości w sieciach komputerowych. Przedmiotowy zakres działania CBZC został określony za pomocą konkretnych kategorii przestępstw (przestępstw komputerowych) oraz sposobu działania sprawców tych czynów zabronionych. W przypadku ujawnienia działań cyberterrorystycznych podstawowe działania zostaną wykonane przez pracowników i specjalistów tego Biura, a następnie zgodnie z właściwością rzeczową przekazane do odpowiedniej jednostki kontrterrorystycznej. Zauważyć należy, że w polskim kodeksie karnym zdefiniowane zostało przestępstwo o charakterze terro-

45 https://policja.pl/pol/kgp/bwc/33358,Biuro-do-Walki-z-Cyberprzestepczoscia.html, [28.01.2022]. Por. art 5d. Ustawy o Policji z dnia 6 kwietnia 1990 r. z późn. zm. (t.j. Dz. U. z 2021 r. poz. 1882 z późn. zm.), https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19900300179/U/D19900179Lj.pdf, [23.01.2023].

46 Nowa generacja cyberprzestępstw to zautomatyzowane, rozproszone ataki przeprowadzone z wykorzystaniem nadpisanego w tym celu oprogramowania. Rosnący zakres działań cyberprzestępców pokazują skuteczne ataki na globalne spółki, systemy bankowe czy dokonane pod koniec 2016 r. włamania do instytucji finansowych i podmiotów publicznych na całym świecie, w tym także w Polsce. Ataki mogą być ukierunkowane nie tylko na osiągnięcie zysku przez sprawców, ale także na pozyskanie informacji, wpływanie na decyzje o charakterze strategicznym lub nastroje społeczne oraz co ważne mogą spowodować destabilizację zarówno w politycznym oraz w gospodarczym sektorze funkcjonowania państwa. Szerzej na ten temat: A. Gryszczyńska, G. Szpor (red.), *Internet Strategie Bezpieczeństwa*, Warszawa 2017, s. 1-32.

47 Szerzej o regulacjach związanych z zwalczaniem cyberprzestępczości w Polsce i UE zob. [w:] I. Wilk, *Regulacje polityki zwalczania cyberprzestępczości w Polsce i w Unii Europejskiej*, [w:] G. Szpor, A. Gryszczyńska, Internet. Strategie Bezpieczeństwa, Warszawa 2017, s. 187-194.

rystycznym. Jednakże w tej definicji legalnej brak jest wskazania sposobu działania sprawców, co powoduje, że możliwe jest zakwalifikowanie czynu przestępstwa komputerowego jako przestępstwa o charakterze terrorystycznym (art. 115 §20 k.k.)[48]. Oznacza to, że przestępstwa takie jak naruszenie ochrony danych informatycznych dla bezpieczeństwa kraju lub wywołanie uszkodzeń w bazach danych stanowić będą przestępstwa terrorystyczne[49]. Utworzenie jednostek organizacyjnych na szczeblu centralnym w Prokuraturze Krajowej, takich jak: Departamenty do zwalczania Przestępczości Zorganizowanej i Korupcji, a także nowo powstałego Centralnego Biura do walki z Cyberprzestępczością i ścisła współpraca pomiędzy nimi pozwoli efektywniej realizować funkcje wykrywacze nie tylko w zwalczaniu terroryzmu dostrzegalnego „gołym okiem", ale także w zwalczaniu cyberterroryzmu. Cyberterroryzmu, który coraz to skuteczniej zbiera swoje żniwo w wielu państwach na świecie, zakłócając i paraliżując infrastrukturę o istotnym znaczeniu dla gospodarki, ale też dla obronności atakowanego kraju, czego najlepszym przykładem aktualnie jest wcześniej już wspomniana Ukraina i jej konflikt zbrojny z Rosją.

Mimo wysokiej skuteczności służb w RP i instytucji odpowiedzialnych za cyberbezpieczeństwo skala zagrożeń pojawiających się w cyberprzestrzeni będzie w przyszłości zdecydowanie wzrastać.

Jednym z zagrożeń niebezpiecznych dla prawidłowego funkcjonowania państwa jest podszywanie się przez hakerów pod organ administracji. W ostatnim czasie głośnym wydarzeniem było rozsyłanie maili i podszywanie się pod Komendanta Głównego Policji i jego Zastępców oraz wykorzystywanie wizerunku Centralnego Biura Zwalczania Cyberprzestępczości, a także innych jednostek Policji.

Z treści przesyłanych wiadomości niejednokrotnie wynikało, że wobec osoby, która ją otrzymała, toczy się postępowanie karne w związku z popełnieniem przestępstwa i powinna ona zapoznać się z zarzutami, które opisane są w załączniku do tej wiadomości. W załącznik należało kliknąć i pobrać go na swoje urządzenie cyfrowe. W rzeczywistości mogło to być złośliwe oprogramowanie, za pomocą którego internetowi oszuści chcieli wykraść nasze dane. W celu uwiarygodnienia swojej wiadomości przestępcy podpisywali się także w imieniu Komendanta Centralnego Biura Zwalczania Cyberprzestępczości nadinsp. Adama Cieślaka.

Oszuści czasami podszywają się również pod Komendanta Głównego Policji generalnego inspektora Jarosława Szymczaka i wysyłają maile z załącznikiem rozpoznawanym jako dokument w formacie „pdf". Z treści tych wiadomości wynikało, że wobec osoby prowadzone jest postępowanie karne dotyczące przestępstw z kategorii wolności seksualnej i obyczajności. Przestępcy zalecają jako formę kontaktu korespondencję mailową i w tej sprawie, i ostrzegają przed skierowaniem sprawy prokuratorowi.

48 G. Ocieczek, K. Samiczak, *Działalność prokuratury i Policji w zakresie przeciwdziałania terroryzmowi w kontekście dynamicznie zmieniającej się sytuacji militarnej na świecie*, „Wojskowy Przegląd Prawniczy Kwartalnik" 2022, Kwiecień-Czerwiec, s. 25-27.

49 S. Dziwisz, *Odpowiedzialność karna za przestępstwa o charakterze terrorystycznym popełnione w cyberprzestrzeni*, [w:] A. Podraza, P. Potakowski, K. Wiak, Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna, Warszawa 2013, s. 279.

Warto wiedzieć, że załącznik do takiej wiadomości może zawierać szkodliwe oprogramowanie, a całość korespondencji w rzeczywistości jest próbą oszustwa i zastraszenia społeczeństwa. Jej celem jest przede wszystkim kradzież środków płatniczych.

Jeżeli nawet ktoś dopuścił się czynu karalnego, to Policja w żadnym wypadku nie kontaktuje się z nim poprzez pocztę elektroniczną.

W przypadku otrzymania podobnej wiadomości na swoją skrzynkę pocztową warto bezpośrednio zgłosić ten fakt na specjalnie do tego celu utworzonej stronie internetowej https://www.cert.pl/

Wnioski

Mimo wielu zalet, które wynikają z rozwoju cyberprzestrzeni, z uwagą należy analizować coraz to nowsze zagrożenia z tym obszarem związane. Jak wskazano we wstępie artykułu, środowisko cyberprzestrzeni jest doskonałym miejscem dla przestępców internetowych czy hakerów, którzy wraz z rozwojem technologii są coraz bardziej efektywni i posiadają dostęp do coraz pilniej strzeżonych informacji. Cyberprzestrzeń jest też źródłem wielu zagrożeń dla bezpieczeństwa zewnętrznego, jaki i wewnętrznego państwa. Przeciwdziałanie takim zagrożeniom, jak się wydaje, powinno być w związku z tym priorytetem zarówno dla sektora państwowego jak i prywatnego.

Uwzględniając stały wzrost cyberprzestępczości należy bowiem oczekiwać, że także Polska będzie stawała się celem najbardziej kompetentnych podmiotów państwowych i pozapaństwowych działających w tym środowisku, co generuje potrzebę stałej aktualizacji i inwestycji w system reagowania na incydenty komputerowe, jak również wzmożonej współpracy z partnerami w ramach projektu Północnoatlantyckiego.

W USA trwają prace nad tworzeniem poziomów prywatności dostępu użytkowników do danych w sieci[50]. Prace wskazane wyżej realizuje także rząd francuski[51]. Być może tego typu rozwiązania przyczyniłyby się również do poprawy bezpieczeństwa osób korzystających bezpieczeństwa korzystających z sieci w Polsce i w innych państwach[52]. Postulowane działania miałyby istotny wpływ na podwyższenie bezpieczeństwa informatycznego, zwłaszcza w obszarze funkcjonowania najważniejszych państwowych struktur.

50 Tworzenie takiej struktury informatycznej musi być zgodne z przestrzeganiem podstawowych konstytucyjnych praw człowieka i obywatela.

51 Defénse et sécurité des systemèsd'information. Stratégie de la France - Obrona oraz bezpieczeństwo systemów informacyjnych. Strategia dla Francji.

52 W. Halboob, R. Mahmod, N. Udzir Izura, M. Taufik Abdullah, *Privacy Levels for Computer Forensic: Toward a More Efficient Privacy-preserving Investigation*, Procedia Computer Science 56 (2015) Elsevier. International Workshop on Cyber Security and Digital Investigation (CSDI 2015), p. 375.

Piśmiennictwo

- Balkowski R., *Bezpieczeństwo systemów teleinformatycznych - zmiany, trendy i zasady,* [w:] Poradnik Klienta Usług Finansowych, Warszawa 2018.
- Banasiński C., Rojszczak M., *Cyberbezpieczeństwo*, Warszawa 2020.
- Besiekierska A., *Komentarz do Ustawy o Krajowym Systemie Cyberbezpieczeństwa*, Legalis, www.sip.legalis.pl
- Białkowski M., *Ocena prawna i kryminalistyczna przestępczości komputerowej*, Wydanie I, Warszawa 2016.
- Bonisławska B., *Współczesne zagrożenia dla bezpieczeństwa publicznego*, Lublin 2012.
- Czeczot Z., Tomaszewski T., *Kryminalistyka ogólna*, Toruń 1996.
- Dziwisz S., *Odpowiedzialność karna za przestępstwa o charakterze terrorystycznym popełnione w cyberprzestrzeni,* [w:] Podraza A., Potakowski P., Wiak K. (red.), Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna, Warszawa 2013.
- Gryszczyńska A., Szpor G. (red.), *Internet Strategie Bezpieczeństwa*, Warszawa 2017.
- Guzik-Makaruk E. M., *Poczucie Bezpieczeństwa obywateli w Polsce. Identyfikacja i przeciwdziałanie współczesnym zagrożeniom*, Warszawa 2011.
- Halboob W., Mahmod R., Udzir Izura N., Taufik Abdullah M., *Privacy Levels for Computer Forensic: Toward a More Efficient Privacy-preserving Investigation*, Procedia Computer Science 56 (2015) Elsevier. International Workshop on Cyber Security and Digital Investigation (CSDI 2015), 2015.
- Hołyst B., Jałoszyński K., Letkiewicz A., *Wojna z terroryzmem w XXI wieku*, Szczytno 2009.
- Hołyst B., *Kryminalistyka*, wyd. 13, Warszawa 2018.
- Jaroszewska I., *Wybrane aspekty przestępczości w cyberprzestrzeni Studium prawno karne i kryminologiczne*, Olsztyn 2017.
- Korzeniowski L. F., *Podstawy nauk o bezpieczeństwie*, Warszawa 2012.
- Lakomy M., *Wymiar informacyjny i telekomunikacyjny bezpieczeństwa Polski*, [w:] Pietraś M., Wojtaszczyk K. A. (red.), Polska w systemie bezpieczeństwa międzynarodowego,Warszawa 2016.
- Lakomy M., *Zagrożenia dla bezpieczeństwa teleinformatycznego państw - przyczynek do typologii*, „e-Politikon" 2013, nr 6.
- Luttgens J., Pepe M., Mandia K*., Incydenty bezpieczeństwa. Metody reagowania w informatyce śledczej*, Gliwice 2014.
- Młynarski T., *Wymiar energetyczny bezpieczeństwa Polski*, [w:] Pietraś M., Wojtaszczyk K. A. (red.), Polska w systemie bezpieczeństwa międzynarodowego, Warszawa 2016.
- Ocieczek G., Samiczak K., *Działalność prokuratury i Policji w zakresie przeciwdziałania terroryzmowi w kontekście dynamicznie zmieniającej się sytuacji militarnej na świecie,* Warszawa 2022.

- Olchowski J., *Zagrożenia bezpieczeństwa,* [w:] Pietraś M., Wojtaszczyk K. A. (red.), Polska w systemie bezpieczeństwa międzynarodowego, Warszawa 2016.
- Opitek P., *Kontrola transferów pieniądza bezgotówkowego w czasie rzeczywistym jako nowa forma czynności operacyjno-rozpoznawczych na przykładzie ustawy o Agencji Bezpieczeństwa Wewnętrznego (postulaty de lege ferenda*, Warszawa 2021.
- Pawlicki T., *Bezpieczeństwo sieci Wi-Fi*, [w:] Czapska J., Okrasa A. (red.), Bezpieczeństwo - policja - kryminalistyka, Wydanie I, Kraków 2015.
- Pączkowski T., *Cyberprzestępczość w województwie śląskim. Studium z socjologii ryzyka – rozważania na temat świadomości policjantów*, Katowice 2019,
- Pietraś M., Wojtaszczyk K. A. (red.), *Polska w systemie bezpieczeństwa międzynarodowego*, Warszawa 2016.
- Piotrowicz K., *Etyka hakera. Wyzwanie dla konsumeryzmu*, [w:] Szlendak T., Piotrowicz K. (red.), Na pokaz. O konsumeryzmie w kapitalizmie bez kapitału, Toruń 2001.
- Siwicki M., *Cyberprzestępczość*, Warszawa 2013.
- Skomra W., *Kompleksowe podejście do wyłaniania i ochrony infrastruktury krytycznej,* „Cyberbezpieczeństwo" 2017, nr 4(43).
- Sordyl J., *Ransomware - wymuszanie okupu w sieci*, „Cyberbezpieczeństwo" 2017, nr 4(43).
- Szamol S., *Ochrona Cyberprzestrzeni Rzeczypospolitej Polskiej w wymiarze strategicznym,* „Cyberbezpieczeństwo. Kwartalnik policyjny" 2018, nr 3(46).
- Szymczak M., *Współczesne wyzwania informatyki kryminalistycznej w kontekście rozwijającej się cyberprzestępczości*. *Księga Pamiątkowa dedykowana Profesorowi T. Widle*, Toruń 2021.
- Ściborek Z., Wiśniewski B., Kuc R.B., Dawidczyk A., *Bezpieczeństwo Wewnętrzne Podręcznik Akademicki*, Toruń 2015.
- Waloch A., *Współczesne zagrożenia dla bezpieczeństwa państwa polskiego w cyberprzestrzeni*, „Studia de Securitate. Annales Universitas Paedagogicae Cracoviensis" 2019, 9(4).
- Wilk I., *Regulacje polityki zwalczania cyberprzestępczości w Polsce i w Unii Europejskiej,* [w:] Szpor G., Gryszczyńska A. (red.), Internet. Strategie Bezpieczeństwa, Warszawa 2017.
- Włodkowska-Bagan A., *Wymiar polityczny i militarny bezpieczeństwa Polski*, [w:] Pietraś M., Wojtaszczyk K. A. (red.), Polska w systemie bezpieczeństwa międzynarodowego, Warszawa 2016.
- Zubańska M., Mikołajczyk Z., Fałdowski M., *Systemowe Ujęcie Bezpieczeństwa Wewnętrznego Tom 2 Zagadnienia praktyki policyjnej*, Szczytno 2019.

CRYMINAL ONLINE THREATS FOR PUBLIC SAFETY – PRENETION AND RESPONSE

Summary: Regardless of the many advantages that result from the development of cyberspace, the threats associated with this area must also be carefully analysed. As indicated in the introduction of the article, the cyberspace environment is an ideal place for Internet criminals or hackers who, along with the progress of technology, are more and more effective and have access to more and more closely guarded information.

Cyberspace is also a source of many threats to the external and internal security of the state. End users, administrators, persons responsible for security should, therefore, especially remember about the basic rules related to maintaining security. Among other things, about updating the operating system, taking care of the correct configuration of anti-virus software.

To ensure the security of the functioning of the IT system, it is important not only to identify the threat or reduce the potential for attack, but also to protect the IT systems that are important from the perspective of the state. The authors also point to the need to specialize entities dealing with specific research and analysis in the area of cybercrime. Laboratories that will have access to the latest IT instruments, employing experts in their specializations, strictly implementing certification standards, consciously cooperating with each other - like the ENFSI network - are able to keep up with the new ways criminals operate. The task of forensic computer science is to introduce as well as disseminate the rules regarding the identification process in the field of digital evidence, to develop good practices in this field and to widely disseminate them in the process of educating judiciary personnel, but also educating the public at the stage of primary and secondary education. Without the dissemination of IT knowledge, there is no possibility to conduct quick, effective and successful criminal proceedings in cases related to digital evidence.

Due to the global nature of the Internet, it seems necessary to develop legal acts regulating the legal aspects of areas related to cybersecurity in such a way that the relevant authority can prompt any irregularities that may occur that may threaten not only the state, but also a single user.

In order to increase security in cyberspace, it seems that the Polish state should increase the emphasis not only on preventing the use of the Internet, but should also ensure that the society is made aware of the online threats to which it is exposed at every stage of development. Due to the continuous progress of technology, it is necessary to train more IT security specialists so that they are able to recognize new types of threats on an ongoing basis and react to them as quickly as possible. It is also important to care for the protection of Poland's most important ICT systems. Exercises should also be carried out to check the resistance of Polish infrastructure to cyber attacks, especially those of a military nature.

In the United States of America, work is underway to create privacy levels for users' access to data on the web. Perhaps such solutions could also contribute to improving the safety of people using the network in the Republic of Poland.

Key words: cybercrime, cybersecurity, criminal threat, prevention, internet.