Konrad Snopkiewicz
Wojskowa Akademia Techniczna

Przegląd zagrożeń w cyberprzestrzeni

Streszczenie

Przestrzeń cybernetyczna nabrała znaczenia powszechnego w niezwykle dynamicznym tempie. W obecnych czasach trudno wyobrazić sobie funkcjonowanie bez możliwości zalogowania się do sieci. Surfowanie po Internecie stało się codziennością, można stwierdzić, że jest to jedna z kluczowych potrzeb człowieka. Niegdyś nowe, a dziś już wszystkim obyte środowisko internetowe zrodziło nowe poważne zagrożenie, jakim jest cyberprzestępczość. Cyberataki są jednymi z największych zagrożeń XXI wieku. Zdecydowanie łatwiej dokonuje się przestępstw z wykorzystaniem maski anonimowości działania. Cyberprzestępczość wpływa na stabilność instytucji państwa, a także system polityczny i gospodarczy. W niniejszym opracowaniu przedstawiono przegląd zagrożeń występujących w cyberprzestrzeni od tych najbardziej powszechnych do najgroźniejszych oddziałujących na funkcjonowanie państwa i ludzi.

Słowa kluczowe: cyberprzestrzeń, zagrożenia, bezpieczeństwo

Wstęp

Współcześnie korzystanie z sieci odbywa się na prawie każdej płaszczyźnie życia, przykładowo: robiąc zakupy internetowe, przelewając pieniądze z konta bankowego za rachunki gazowe, pokazując zdjęcia z wakacji na Malediwach oraz komunikując się ze sobą za pomocą kamerki wbudowanej w laptopie. Człowiek korzysta z wymienionych udogodnień każdego dnia, nie zdając sobie coraz częściej sprawy, że jego prywatność jest ograniczona i każde jego działanie w tej informatycznej przestrzeni pozostawia ślady. Większości rzeczy pozostawionych w Internecie nigdy nie zostanie usunięta, co często doprowadza „sprytnych cyberprzestępców" do podejmowania coraz odważniejszych działań na szkodę innego człowieka[1].

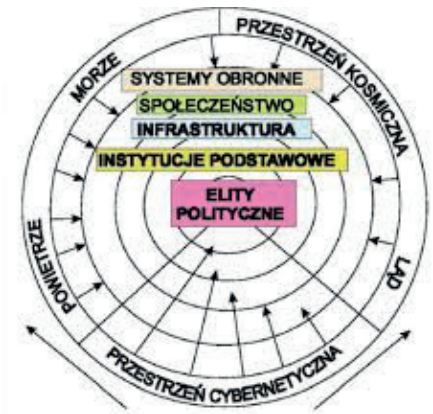
[1] K. Snopkiewicz, *Cyberbezpieczeństwo w polskich realiach*, [w:] G. Skrobotowicz, *Cyberbezpieczeństwo w polskich realiach*, Lublin 2019, s. 36-37.

1. Podstawowa terminologia

Określenie „cyberprzestrzeń" (z ang. *cyberspace*) po raz pierwszy zastosowano w literaturze w 1982 r. Jego twórcą był W. Gibson – autor wielu powieści *science fiction*, który definiował cyberprzestrzeń w następujący sposób: „Konsensualna halucynacja doświadczana każdego dnia przez miliardy uprawionych użytkowników we wszystkich krajach. […] Graficzne odwzorowanie danych pobieranych z banków wszystkich komputerów świata. Niewyobrażalna złożoność… Świetlne linie przebiegały bezprzestrzeń umysłu, skupiska i konstelacje danych"[2].

Najbardziej popularna definicja cyberprzestrzeni została stworzona przez Departament Obrony Stanów Zjednoczonych w brzmieniu: „globalna domena środowiska informacyjnego składająca się ze współzależnych sieci infrastruktury technologii informacyjnej i zawartych w nich danych, z uwzględnieniem Internetu, sieci telekomunikacyjnych, systemów komputerowych oraz osadzonych w nich procesów i kontrolerów"[3,4].

Z kolei P. Sienkiewicz przytacza tzw. model Wardena z lat 90. XX w. traktujący przestrzeń cybernetyczną jako „piąty wymiar walki" (Rysunek 1.). Przedstawia on bardzo istotne aspekty odnoszące się do bezpieczeństwa i walki w jej obszarze na pięciu płaszczyznach: na lądzie, na morzu, w powietrzu, w przestrzeni kosmicznej i właśnie w przestrzeni cybernetycznej[5].



Rysunek 1. Model „pięciu wymiarów" walki Wardena

Źródło: opracowane na podstawie: J. Warden, *The Enemy as System, Airpower Journal*, wiosna 1995, 26.08.2020, s. 374-375, [za:] R. Białoskórski, *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku Zarys Problematyki*, Warszawa 2011, s. 13.

[2] W. Gibson, *Neuromancer*, Warszawa 2001, za: K. Gawkowski, *Cyberkolonializm*, Gliwice 2018, s. 13.

[3] Ang. *A global domain within the information environment consisting of the interdependent Network of information technology infrastructures and resident data, includng the Interent, telecomunications networks, computer systems, and embedded processors and controllers*.

[4] K. Gawkowski, *Cyberkolonializm*, Gliwice 2018, s. 13.

[5] P. Sienkiewicz, http://winntbg.bg.agh.edu.pl/skrypty2/0095/373378, 26.08.2020 [dostęp: 20.05.2020].

Współcześnie w znaczeniu ogólnym cyberprzestrzeń oznacza świat informacji, tworzony przy pomocy Internetu lub inaczej przestrzeń komunikacyjną tworzoną przez system powiązań internetowych[6]. Definicja słownika PWN precyzuje cyberprzestrzeń jako: „przestrzeń wirtualną, w której odbywa się komunikacja między komputerami połączonymi siecią internetową"[7]. Jedną z najbardziej znanych w Polsce definicji cyberprzestrzeni jest pochodząca z Doktryny Cyberbezpieczeństwa Rzeczypospolitej Polskiej z 2015 r., określająca cyberprzestrzeń jako „przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami"[8]. Według programu rządowego cyberprzestrzeń to cyfrowa mapa przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z uczestnikiem[9]. Na specyfikę cyberprzestrzeni wskazuje wielu nie tylko polskich, lecz także zagranicznych badaczy zajmujących się tą problematyką[10]. W literaturze spotkać możemy co najmniej cztery ujęcia definicyjne pojęcia „cyberprzestrzeń", w których określana jest jako[11]:

1) przestrzeń otwartego komunikowania się za pośrednictwem Internetu lub innych sieci, tworząca system powiązań informatycznych ułatwiających użytkownikom kontakty, w tym kontakty w czasie rzeczywistym (w kontekście tej definicji cyberprzestrzeń postrzegana jest jako kanał wymiany informacji),
2) przestrzeń tworzona przez grafikę komputerową w komputerach osobistych,
3) rzeczywistość wirtualna (przyjmuje się tu zamienność tych dwóch określeń),
4) środowisko stwarzające warunki do współdziałania różnych mediów, umożliwiające konstruowanie dzieła sztuki (jest to całościowy zestaw danych do kreowania dzieła).

---

[6] R. Białoskórski, *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku Zarys Problematyki*, Warszawa 2011, s. 14.

[7] https://sjp.pwn.pl/sjp/cyberprzestrze%C5%84;2553915, 26.08.2020 [dostęp: 20.05.2020].

[8] Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej, 2015, s. 7.

[9] D. Lisiak-Felicka, *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, Kraków 2016, s. 48-50.

[10] G. Penkowska, *Człowiek i komputer. Zbiór esejów*, Gdańsk 2005.

[11] B. Siemieniecki, *Rzeczywistość wirtualna a edukacja*, [w:] *Cyberprzestrzeń i edukacja*, red. T. Lewowicki, B. Siemieniecki, Toruń 2012, s. 12-14.

Cyberprzestrzeń charakteryzuje się pewnymi cechami technicznymi[12]:

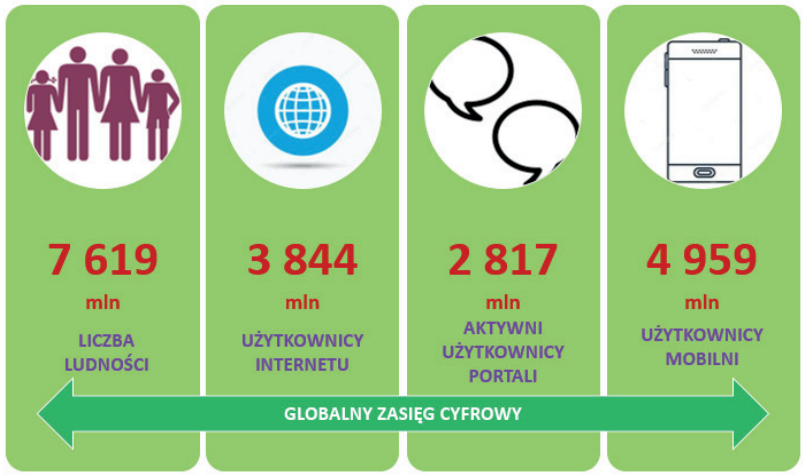
- otwarta architektura – nie ma żadnego centrum, jej najważniejszą składową jest Internet;
- ageograficzność – nie istnieją żadne fizyczne granice;
- niematerialność – choć jest uzależniona od istniejącej struktury informatycznej;
- pole magnetyczne.

Cyberprzestrzeń w tym kontekście stanowi zatem pewną kategorię zbiorczą urządzeń elektronicznych wspólnie ze sobą działających. Przestrzeń informatyczna wywarła ogromny wpływ na funkcjonowanie systemu bezpieczeństwa w państwach. Luki oraz błędy w architekturze teleinformatycznej mogą być przyczyną poważnych zakłóceń wszystkich systemów w obszarze szeroko pojętego bezpieczeństwa oraz licznych awarii. Obecnie przyjmuje się, że przestrzeń cybernetyczna może ulegać przekształceniu w pewnego rodzaju bezpieczeństwo międzynarodowe, które mają kilka wspólnych cech. Wyróżnia się tutaj przede wszystkim wcześniej wspomniana ageograficzność czy aterytorialność i niematerialność domeny, co może znacznie utrudnić rozwiązywanie incydentów informatycznych. Ogromną trudność rodzi również identyfikacja sprawców cyberataków. Cyberprzestrzeń zapewnia bowiem większą wolność i anonimowość. Z kolei stworzenie optymalnego systemu przeciwdziałania rodzącym zagrożeniom jest niezwykle trudne i kosztowne, przez co angażują się w nią wszystkie organizacje międzynarodowe i państwa na całym świecie. Ten właśnie aspekt posłużył do wyodrębnienia kolejnego rodzaju bezpieczeństwa przedmiotowego, jakim jest cyberbezpieczeństwo[13].

2. Zcyfryzowanie społeczeństwa

Świat Internetu w bardzo dynamicznym tempie rozwija się. Przybywa znaczna ilość użytkowników globalnej sieci (Rysunek 2.). Nawet twórcy Internetu zapewne nie przewidywali, że wzrost sięgnie 4 miliardów użytkowników na całym świecie (2018). Z danych Internet Live Stats wynika, iż ponad połowa mieszkańców globu w 2018 r. miała dostęp do Internetu. Aktywnych stron internetowych było już ponad 1,2 mld (co sekundę wylicza się, że przybywa kolejne 8). Aktywne konto na portalu społecznościowym ma już co 3 osoba na świecie, a użytkowników mobilnych jest już prawie 5 mld[14].

[12] R. Zięba, *Bezpieczeństwo międzynarodowe w XXI wieku*, Warszawa 2018, s. 56.
[13] Ibidem, s. 56-57.
[14] Internet Live Stats, 2018 r. [online], https://www.internetlivestats.com/ [dostęp: 26.08.2020].



Rysunek 2. Globalny świat cyfrowy w 2018 r.

Źródło: opracowanie własne na podstawie danych Internet Live Stats, 2018 [online], https://www.internetlivestats.com/ [dostęp: 26.08.2020].

Na potwierdzenie słuszności, iż społeczeństwo stało się informacyjne świadczą wyniki badań według raportu Digital in 2018: *World's internet users pass the 4 billion mark*[15]. Ukazują one dostęp do Internetu według poszczególnych kontynentów:

- Antarktyda – 98% (stacje badawcze),
- Ameryka Północna – 88%,
- Europa – 80%,
- Australia i Oceania – 69%,
- Ameryka Południowa – 68%,
- Azja – 50%,
- Afryka – 34%.

Raport również przedstawia kraje o najszerszym dostępie do Internetu. Na świecie są to mieszkańcy Kataru i Zjednoczonych Emiratów Arabskich (99%), w Europie z kolei Luksemburg, Islandia i Norwegia (98%). W UE dostęp do sieci globalnej ma średnio 90% obywateli, z kolei w Polsce 86%. Szacuje się, że około 78% użytkowników polskich korzysta z Internetu każdego dnia. Obecnie aż 76% polskich internautów łączy się z siecią za pomocą urządzeń mobilnych[16].

[15] WeAreSocial UK – Digital in 2018: *World's internet users pass the 4 billion mark* [online], https://wearesocial.com/uk/blog/2018/01/global-digital-report-2018 [dostęp: 25.08.2020].
[16] Ibidem.

3. Wybrane rodzaje zagrożeń w cyberprzestrzeni

Nowoczesne technologie są niezwykle ważne dla człowieka i niosą za sobą wiele korzyści. Obecnie ciężko jest wyobrazić sobie życie bez Internetu czy komputera. Niestety wiąże się to również z licznymi zagrożeniami. Cyberprzestrzeń jest polem, na którym rozgrywa się wiele ludzkich, a nawet państwowych dramatów. Cyberzagrożenia dotyczą każdego człowieka, w szczególności dzieci. Są one niezwykle groźne dla państwa oraz całego globu jako narzędzie w rękach terrorystów i hakerów.

W zależności od klasyfikacji i przyjętego toku myślenia zagrożeń w cyberprzestrzeni jest bardzo duża ilość, które ciągle dynamicznie się rozrastają. Wiążą się one z wielkimi stratami finansowymi, moralnymi, a nawet życiowymi. Cyberzagrożenia można podzielić na trzy grupy (Rysunek 3.). Do pierwszej z nich należą przede wszystkim uzależnienia, problemy z komunikacją międzyludzką oraz relacjami. Drugą grupę tworzą zaniedbania w tworzeniu systemów informatycznych, jak również awarie i lekkomyślność ludzka. Z kolei trzecia grupa to cyberprzestępstwa na drobną skalę, np.: hejt w Internecie aż po działania cyberterrorystyczne i cyberwojenne[17].

Rysunek 3. Grupy cyberzagrożeń
Źródło: opracowanie własne.

Zagrożenie jest potencjalnym powodem niepożądanego wydarzenia dla bezpieczeństwa systemu. P. Sienkiewicz wyróżnia trzy główne kategorie zagrożeń bezpieczeństwa cyberprzestrzeni oraz ich wiele wariantów[18]:

[17] K. Gawkowski, *Cyberkolonializm*..., op. cit., s. 51.
[18] http://winntbg.bg.agh.edu.pl/skrypty2/0095/373378, s. 374-375 [dostęp: 25.08.2020].

1) techniczne – niezawodność systemów technicznych, awarie lub nieprawidłowości w oprogramowaniu;
2) społeczne:
   – polityczne,
   – losowe,
   – umyślne;
3) naturalne – katastrofy naturalne.

Do zagrożeń politycznych można zaliczyć cyberterroryzm, cyberataki, cyberprotesty czy cyberwalkę polityczną. Zdarzenia losowe to takie, które z reguły nie mają złych intencji natomiast zagrożenia umyślne to m.in.: hacking, cyberprzemoc, kradzieże tożsamości czy niezgodne z prawem wykorzystywanie serwisów społecznościowych[19].

Pośród zagrożeń istniejących w cyberprzestrzeni należy wyjaśnić kilka z nich[20]:

1) cyberprzemoc, czyli wykorzystanie cyberprzestrzeni do wymuszenia przyjęcia niepożądanych wiadomości o zawartości informacyjnej niezgodnej z wartościami jej odbiorcy;
2) cyberprzestępstwo, czyli użycie cyberprzestrzeni z zamysłem dokonania nielegalnej agresji;
3) cyberinwigilacja, czyli kontrolowanie i zdobywanie informacji na temat różnych podmiotów;
4) cyberterroryzm, czyli przestępstwo zmierzające do osiągnięcia zamierzonego celu poprzez działania terrorystyczne;
5) cyberwojna, czyli realizacja działań politycznych z wykorzystaniem sił zbrojnych, których celem są zasoby, informacje, systemy czy infrastruktura krytyczna przeciwnika.

Warto również opisać kilka rodzajów cyberataków, które mogą nieść za sobą duże konsekwencje w działaniach państwa i jego obywateli[21]:

Ataki przez Internet rzeczy (*Internet of Things,* IoT)

Większość ludzi korzysta z różnych dobrodziejstw, jakie dają nam inteligentne urządzenia. Dzięki IoT możemy łączyć ze sobą wszystkie nasze urządzenia. Na przykład za pomocą telefonu komórkowego można obsługiwać i kontrolować wszystkie swoje urządzenia domowe z dowolnego miejsca. Dzięki temu człowiek pozostaje w stałej łączności z siecią. Przestępca, hakując jedno z takich urządzeń,

[19] Ibidem.
[20] K. Gawkowski, *Cyberkolonializm…*, op. cit., s. 51-75.
[21] Ibidem.

uzyskuje dostęp do pozostałych, a następnie do wszystkich informacji z życia osobistego czy zawodowego.

Ataki na kryptowaluty i systemy blockchain

Światowe firmy stosujące technologię kryptowalut nie posiadają odpowiednich kontroli bezpieczeństwa. Podczas pracy z kryptowalutami i systemami blockchain może dojść do ataków, w których napastnik przejmie pełną kontrolę nad wszystkimi połączeniami ofiary. Ten rodzaj ataku może być wykorzystywany do ukrywania informacji o użyciu kryptowalut w sieci (tzw. *Eclipse Attack*). Inny rodzaj ataku charakteryzuje się uzyskaniem przez jeden węzeł w sieci kilku tożsamości (tzw. *Sybil Attack*). Przestępcy włamują się do całego systemu i w ten sposób uzyskują dostęp do każdej pojedynczej informacji zawartej w sieci, tym samym otrzymując informacje o osobach, firmach czy organizacjach. Fałszowanie i kradzież tożsamości rosną na większą skalę. Za pomocą *cryptojackingu*, czyli inaczej złośliwego wydobywania kryptowalut, przestępcy zdobywają je dla swojego wirtualnego portfela. Istnieją jednak legalne strony internetowe, na których złodzieje mogą wydobywać kryptowaluty.

Problemy z bezpieczeństwem w chmurze

Platformy chmurowe przechowują duże ilości wrażliwych i cennych danych. Istnieją problemy, które wymagają szczególnej uwagi, to m.in.: niwelowanie nieprawidłowości w konfiguracji chmur. Firmy nie są jeszcze do końca świadome złożoności związanej z zabezpieczaniem danych w chmurze, więc jeszcze więcej naruszeń spowodowanych błędami i projektowaniem czeka w najbliższej przyszłości. Utrata danych to jedno z zagrożeń, których nie należy ignorować. Klęska żywiołowa lub zwykły błąd ludzki może doprowadzić do utraty danych. Jedynym sposobem na ograniczenie ryzyka ich utraty jest tworzenie wielu kopii zapasowych w różnych lokalizacjach.

Ataki oparte na uczeniu maszynowym i sztucznej inteligencji

Oprogramowanie sztucznej inteligencji (z ang. *Artificial Intelligence*, AI) oraz uczenie maszynowe (z ang. *Machine Learning*, ML) mogą „uczyć się" na podstawie konsekwencji przeszłych wydarzeń, aby osiągnąć wyznaczony cel. Podczas gdy wielu specjalistów do spraw cyberbezpieczeństwa używa narzędzi AI i ML do przeprowadzania cyberataków, istnieje szansa, że hakerzy zechcą również ich użyć. Mogą być one wykorzystywane do przeprowadzania różnego rodzaju ataków: od wysyłania dużej ilości spamu, oszustw, phishingu poprzez boty do odgadywania haseł opartych na sztucznej inteligencji czy przeprowadzania ataków kryptograficznych.

Phishing

Zjawisko oznacza wyszukiwanie użytkowników mobilnych usług przez cyberprzestępców – poprzez podstawianie fałszywych stron internetowych banku, w celu wyłudzenia poufnych informacji, takich jak hasło, login, numer karty płatniczej oraz zawirusowania urządzenia sieciowego, a następnie dokonania transakcji finansowych bez wiedzy użytkownika[22]. Poprzez ataki phishingowe w 2017 r, swoje dane utraciło 12 mln osób. Z kolei z analizy Google wynika, iż ponad 80% ataków było przeprowadzonych w celu pozyskania adresu identyfikacyjnego[23].

Wyróżnia się również inne rodzaje ataków bądź problemów, na które może być narażony zwykły użytkownik, są to m.in.: dolegliwości zdrowotne w związku z długim wykorzystywaniem Internetu, stalking poprzez cyberprzestrzeń, pedofilia w Internecie, uzależnienia od gier komputerowych, portali społecznościowych, pornografii, seksting, oszustwa związane z zakupami typu online, ataki na bankowość elektroniczną, kradzieże tożsamości, pieniędzy, danych wrażliwych, fałszywe strony i aukcje internetowe narażające na utratę mienia, złośliwe oprogramowania, SPAM-y, wirusy internetowe, fałszowanie tożsamości, powstawanie niebezpiecznych sekt na forach internetowych, hakowanie samochodów za pomocą nowoczesnych systemów elektronicznych[24].

4. Przykłady cyberataków na świecie

Pierwszym najbardziej znanym atakiem w cyberprzestrzeni był Slammer, który zaatakował systemy komputerowe w 2003 r. Wirus ten wykorzystał lukę w oprogramowaniu, doprowadzając do zainfekowania ponad 75 tysięcy komputerów na świecie. Kolejny atak miał miejsce w najbardziej zcyfryzowanym państwie Europy – Estonii w 2007 r. Rok później doszło do cyberataków w Azerbejdżanie i Gruzji. Wirus Stuxnet zainfekował 100 tysięcy komputerów w 155 państwach. Ataki miały miejsce również w Arabii Saudyjskiej, kiedy to w 2012 r. zainfekowano 30 tysięcy komputerów[25].

[22] https://pl.malwarebytes.com/phishing/ [ostęp: 25.08.2020].
[23] K. Gawkowski, *Cyberkolonializm*…, op. cit., s. 82.
[24] K. Snopkiewicz, *Zagrożenia w cyberprzestrzeni w opinii użytkowników*, Warszawa 2020, s. 32-38 [praca magisterska pod kierunkiem dr J. Stochaj].
[25] T. Hoffmann, *Wybrane aspekty cyberbezpieczeństwa w Polsce*, Poznań 2018, s. 71.

W 2014 r. pojawił się botnet Zeus Gameover, którego unieszkodliwiało aż 11 państw globu[26]. W tym samym roku wykryto również szpiegowskie operacje BlackEnergy i Sandworm. Można uznać, że są to kolejne dowody, które potwierdzają, że walka na wschodzie Europy odbywa się również w cyberprzestrzeni. Warto również wspomnieć o kampanii APT28, za którą stała grupa rosyjskich przestępców, a ich działania miały być skierowane na organizacje w Europie Wschodniej, szczególnie Gruzji oraz członków OBWE i NATO, w tym Polski[27]. Według Fundacji *Bezpieczna Cyberprzestrzeń* najwięcej popełnianych przestępstw w 2015 r. jest za pomocą phishingu z wykorzystaniem poczty elektronicznej. Z raportów NIK wynika, że cyberataki miały również miejsce w Polsce[28].

Przykładem hackerskiego ataku w naszym kraju może być zdarzenie z 2012 r., kiedy to uderzono w systemy teleinformatyczne instytucji państwowych. Polegał on na tym, że wysłano zmasowane pytania, które spowodowały zablokowanie usług informacyjnych na przeciążonych serwerach. Był to protest przeciwko podpisaniu umowy ACTA przez władze polskie. Trudności głównie wystąpiły w dostępach do stron m.in. Ministerstwa Obrony Narodowej, Sztabu Generalnego Wojska Polskiego, Żandarmerii Wojskowej, Kancelarii Sejmu i Senatu RP, Kancelarii Prezydenta RP, Kancelarii Prezesa Rady Ministrów, Komendy Głównej Policji, Centralnego Biura Antykorupcyjnego. Ich celem było przeciążenie serwerów udostępniających strony internetowe tych instytucji[29]. Podobne ataki dotknęły również strony internetowe Ministerstwa Gospodarki, a dotyczyły wykradania danych osobowych (paszportowych, mailowych, hasłowych). W lipcu 2014 r. wydarzyły się cyberataki o charakterze terrorystycznym. Anonimowi nadawcy rozpowszechnili informację o podłożeniu ładunków wybuchowych w ważnych instytucjach państwowych. W tym samym roku, w październiku nastąpiła kradzież danych z systemów informatycznych Giełdy Papierów Wartościowych. W listopadzie wykradziono dane pracowników Państwowej Komisji Wyborczej. Miało to miejsce w okresie, w którym PKW borykała się z problemem do obliczenia wyników przeprowadzonych wyborów samorządowych. Oprócz tych incydentów wydarzyły się również inne, jak udostępnianie danych osobowych w Internecie ponad 400 tys. abonentów firmy telefonicznej ORANGE oraz HYPERION[30] (opisy ataków – Tabela 1.).

[26] Największe zagrożenie dla bezpieczeństwa w Internecie w 2015 r. Głos polskich ekspertów, *Raport Fundacji Bezpieczna Cyberprzestrzeń*, 2015, s. 6.
[27] T. Hoffmann, *Wybrane*…, op. cit., s. 72.
[28] Największe zagrożenie dla bezpieczeństwa w Internecie w 2015 r. Głos polskich ekspertów, *Raport Fundacji Bezpieczna Cyberprzestrzeń*, 2015, s. 7.
[29] Wyniki Najwyższej Izby Kontroli. *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP*, Warszawa 2015, s. 20.
[30] T. Hoffmann, *Wybrane*…, op. cit., s. 78.

Tabela 1. Wybrane cyberataki na świecie

Przykłady cyberataków	Rok	Opis
Slammer	**2003**	Pierwszy wirus zaatakował systemy komputerowe. Wykorzystał on lukę w oprogramowaniu doprowadzając do zainfekowania ponad 75 tys. komputerów na świecie
Przestępstwa cybernetyczne Estonia	**2007**	Ataki cybernetyczne na masową skalę będące pokłosiem zwrócenia uwagi na bezpieczeństwo cybernetyczne
Stuxnet	**2012**	Zainfekował 100 tys. komputerów w 155 państwach. Najbardziej dotknięta została Arabia Saudyjska, gdzie zainfekowano 30 tys. komputerów
Zeus Gameover	**2014**	Botnet Zeus Gameover, którego unieszkodliwiało aż 11 państw globu
Ataki typu DDoS Polska	**2012-14**	Grupa Anonymous podjęła działania ofensywne, które unieruchamiały na pewien okres rządowe witryny w domenie .gov.pl w Polsce. Do zdarzenia doszło w ramach protestu przeciwko podpisaniu ACTA
Kradzież danych Korea Płd.	**2014**	Dane ze 100 milionów kart kredytowych zostały skradzione w ciągu kilku lat. Ponadto włamano się do 20 mln kont bankowych
Kradzież danych Rosja	**2014**	Rosyjscy hakerzy ukradli 1,2 miliarda loginów i haseł na 420 000 witrynach internetowych na całym świecie
Złośliwy program Turcja, Ukraina	**2015**	Przestępcy złamali zabezpieczenia wyrzutni rakiet w Turcji oraz unieruchomiono elektrownię na Ukrainie
Kradzież tożsamości USA	**2015**	Przy pomocy złośliwego oprogramowania zaatakowano ok. 22 mln użytkowników w USA, kradnąc dane 1,1 mln osób
Cyberatak USA	**2017**	Udaremniony przez amerykańskie służby cyberatak na sieć elektrowni atomowych w USA
Kradzież pieniędzy Korea Płd.	**2019-2020**	Zostało skradzionych ok. 2,3 miliarda dolarów amerykańskich przy wsparciu kryptowalut
Pandemia SARS-CoV-2 Świat	**2020**	W wyniku trwającej pandemii, w związku z wykorzystaniem trybu zdalnego w codziennym życiu dochodziło do wielu cyberataków każdego dnia

Źródło: opracowanie własne.

Polska jako kraj, który nie jest tak wysoko zinformatyzowany jak chociażby Estonia oraz inne państwa zachodnie, może być również celem ataków cyberterrorystycznych. Przyczyny takiego stanu rzeczy są następujące[31]:

- infrastruktura krytyczna jest w znacznym stopniu zinformatyzowana;
- wzrastający odsetek użytkowników Internetu (Polska znajduje się w pierwszej dziesiątce);
- większa część Polaków korzysta z możliwości obsługi kont bankowych przez Internet;

[31] M. Łapczyński, *Zagrożenia cyberterroryzmem a polska strategia obrony przed tym zjawiskiem* [online], http://www.psz.pl/tekst-19752/Marcin-Lapczynski-Polska-strategia-obronyprzed-cyberterroryzmem [dostęp: 25.08.2020].

- zagrożenie cyberszpiegostwem służb specjalnych innych państw;
- Polska jest uczestnikiem działań stabilizacyjnych w Afganistanie czy też Iraku przez co narażona jest na cyberatak ze strony terrorystów z tychże państw.

Przypuszcza się, że ataki cyberterrorystyczne w Polsce są nieuniknione i to tylko kwestia czasu, kiedy nastanie ich wzrost. Prawdopodobnie obiektami najbardziej zagrożonymi staną się lotniska, elektrownie jak również duże firmy przemysłowe[32]. Obecnie kraj jest celem dość licznych cyberataków – według Polskiego Instytutu Cyberbezpieczeństwa dziennie dochodzi do ponad 100 tysięcy różnego rodzaju ataków[33].

Podsumowanie

Upowszechnienie Internetu doprowadziło do swoistego przeniesienia życia w sferę cybernetyczną. Cyberprzestrzeń nie jest elementem w pełni poznanym przez człowieka. W wielu przypadkach, to w jaki sposób funkcjonujemy i działamy w sieci może narazić nas na cyberatak. Bierze się to najczęściej z niewiedzy w zakresie rozróżnienia sfery realnej od wirtualnej. Człowieka kuszą przede wszystkim pozory anonimowości w świecie cyberprzestrzeni. Cyberprzestępczość jest działaniem na wielką skalę w obecnych czasach. Na każdym kroku należy zachować czujność i poszerzać świadomość swojego działania w sieci. Walka z cyberprzestępczością wymaga holistycznego i spójnego systemu, wprowadzenia odpowiednich przepisów prawnych przy zatrudnieniu wysokiej klasy specjalistów. Każdy obywatel może zrobić wiele sam dla siebie, dbając o poufność swoich danych i rozwagę w korzystaniu z udogodnień w sieci[34].

Bibliografia

1. Białoskórski R., *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku Zarys Problematyki*, Warszawa 2011.
2. *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej*, 2015.
3. Gawkowski K., *Cyberkolonializm*, Gliwice 2018.
4. Gibson W., *Neuromancer*, Warszawa 2001, [za:] K. Gawkowski, *Cyberkolonializm*, Gliwice 2018.

[32] *Cyberataki terrorystyczne w Polsce to tylko kwestia czasu. Które branże narażone są najbardziej?* [online], https://www.polskieradio.pl/42/273/Artykul/1768361,Cyberataki-terrorystyczne-w-Polsce-to-tylko-kwestia-czasu-Ktore-branze-narazone-sa-najbardziej [dostęp: 25.08.2020].

[33] *Raport o stanie bezpieczeństwa informacji*, Polski Instytut Cyberbezpieczeństwa, Warszawa 2018.

[34] K. Snopkiewicz, *Zagrożenia w cyberprzestrzeni w opinii użytkowników*, op. cit., s. 93-95.

5. Hoffmann T., *Wybrane aspekty cyberbezpieczeństwa w Polsce*, Poznań 2018.
6. Lisiak-Felicka D., *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, Kraków 2016.
7. Największe zagrożenie dla bezpieczeństwa w Internecie w 2015 r. Głos polskich ekspertów, *Raport Fundacji Bezpieczna Cyberprzestrzeń*, 2015.
8. Penkowska G., *Człowiek i komputer. Zbiór esejów*, Gdańsk 2005.
9. *Raport o stanie bezpieczeństwa informacji*, Polski Instytut Cyberbezpieczeństwa, Warszawa 2018.
10. Siemieniecki B., *Rzeczywistość wirtualna a edukacja*, [w:] *Cyberprzestrzeń i edukacja*, red. T. Lewowicki, B. Siemieniecki, Toruń 2012.
11. Snopkiewicz K., *Cyberbezpieczeństwo w polskich realiach*, [w:] G. Skrobotowicz, *Cyberbezpieczeństwo w polskich realiach*, Lublin 2019.
12. Snopkiewicz K., *Zagrożenia w cyberprzestrzeni w opinii użytkowników*, Warszawa 2020 [praca magisterska pod kierunkiem dr J. Stochaj].
13. Wyniki Najwyższej Izby Kontroli. Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP, Warszawa 2015.
14. Zięba R., *Bezpieczeństwo międzynarodowe w XXI wieku*, Warszawa 2018.
15. *Cyberataki terrorystyczne w Polsce to tylko kwestia czasu. Które branże narażone są najbardziej?* [online], https://www.polskieradio.pl/42/273/Artykul/1768361,Cyberataki-terrorystyczne-w-Polsce-to-tylko-kwestia-czasu-Ktore-branze-narazone-sa-najbardziej.
16. http://winntbg.bg.agh.edu.pl/skrypty2/0095/373378.
17. https://pl.malwarebytes.com/phishing/.
18. https://sjp.pwn.pl/sjp/cyberprzestrze%C5%84;2553915.
19. Internet Live Stats, 2018 r., https://www.internetlivestats.com/.
20. Łapczyński M., *Zagrożenia cyberterroryzmem a polska strategia obrony przed tym zjawiskiem*" [online], http://www.psz.pl/tekst-19752/Marcin-Lapczynski-Polska-strategia-obronyprzed-cyberterroryzmem.
21. Sienkiewicz P., http://winntbg.bg.agh.edu.pl/skrypty2/0095/373378.
22. WeAreSocial UK – Digital in 2018: *World's internet users pass the 4 billion mark* [online], https://wearesocial.com/uk/blog/2018/01/global-digital-report-2018.

Threats in cyberspace in the opinion of users

Abstract

Cyberspace has gained universal importance at an extremely dynamic pace. Nowadays it is difficult to imagine functioning without logging into the network. Surfing the Internet has become commonplace, it can be said that it is one of the key human needs. The once new and now familiar Internet environment has created a new serious threat, which is cybercrime. Cyber-attacks are one of the greatest threats of the 21st century. It is much easier to commit crimes using the mask of anonymity of action. Cybercrime affects the stability of state institutions as well as the political and economic system. This study presents an overview of threats in cyberspace, from the most common to the most dangerous, affecting the functioning of the state and people.

Keywords: cyberspace, threats, security