Zeszyty Naukowe SGSP 2019, Nr 71/3/2019

dr inż. Tadeusz Terlikowski
Wydział Inżynierii Bezpieczeństwa Cywilnego
Szkoła Główna Służby Pożarniczej w Warszawie

Bezpieczeństwo cyberprzestrzeni wyzwaniem naszych czasów. System cyberbezpieczeństwa w Polsce (w świetle obowiązującego prawa)

Abstrakt

Nie jest pustym sloganem stwierdzenie, że funkcjonowanie współczesnych państw zależy od informacji i jej niezakłóconego przesyłu. Przesył informacji może być także wykorzystany w celach przestępczych, terrorystycznych, a nawet militarnych. Aby zapewnić bezpieczeństwo informacji przesyłanych sieciami teleinfomatycznymi, przestrzeń tego przesyłu nazywana cyberprzestrzenią, musi być odpowiednio zabezpieczona przed różnymi nieuprawnionymi dostępami. Państwa tworzą tzw. systemy cyberbezpieczeństwa. Artykuł poświęcony jest omówieniu krajowego systemu cyberbezpieczeństwa opartego o ustawę z 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa*. Artykuł jest materiałem analityczno-przeglądowym funkcjonowania cyberprzestrzeni w obecnym okresie powszechnej globalizacji.

Słowa kluczowe: Internet, cyberprzestrzeń, cyberbezpieczeństwa, incydent zakłócający funkcjonowanie sieci teleinformatycznych w cyberprzestrzeni, krajowy system cyberprzestrzeni

Cyberspace Security – a Challenge of our Times. The System of Cybersafety in Poland (according to the binding law)

Abstract

It is not an idle platitude that functioning of contemporary countries depends on information and its smooth transfer. The transfer can be also used for the criminal, terroristic and even military purposes. To ensure the information security transferred by the IT networks,

the space of the transfer called cyberspace must be properly protected against various unauthorized accesses. The countries build so called cybersecurity systems. The article discusses the state cybersecurity system based on the Law from 5 July 2018 about the state system of cybersafety. The paper is an analytical review material presenting the functioning of cyberspace in contemporary common globalization.

Keywords: Internet, cyber space, cyber security, incident disrupting functioning of IT network in cyber space, state system of cyber space

Wprowadzenie

Informacja, jej przekaz i wykorzystanie, jest nieodzownym elementem postępu technicznego, jak i rozwoju cywilizacyjnego. Rozwój gospodarczo-społeczny państwa, aby był efektywny, wymaga szybkiego i niczym niezakłóconego dostępu do informacji i jej odpowiedniego wykorzystania w zarządzaniu państwem na każdym szczeblu (rządowym i samorządowym), zarządzaniu gospodarką i usługami, transporcie towarów i osób, zapewnieniu społeczeństwu jego niezbędnych potrzeb do normalnego funkcjonowania, a więc dostępu do źródeł energii, wody, żywności itp. potrzeb, jak zapewnienie społeczeństwu podstawowych warunków bezpieczeństwa zdrowotnego, żywnościowego, ekonomicznego, bezpieczeństwa w środowisku publicznym, środowisku naturalnym, zapewnienie społeczeństwu ochrony i ratownictwa w sytuacji wystąpienia zagrożeń i ich skutków ze strony katastrof naturalnych i technicznych. Jak czytamy we wstępie do Krajowych Ram Polityki Cyberbezpieczeństwa RP na lata 2017-2022, informacje pozwalają tworzyć i kształtować w cyberprzestrzeni relacje społeczne, a Internet stał się narzędziem do wpływania na zachowania grup społecznych, a także oddziaływania na funkcjonowanie sfery politycznej[1]. Ta informacja przesyłana jest w tzw. cyberprzestrzeni, nazywanej powszechnie Internetem. To właśnie Internet stał się w obecnych czasach swoistego rodzaju medium, które zrewolucjonizowało współczesny świat. Bez Internetu powszechna globalizacja świata byłaby niemożliwa. Cyberprzestrzeń, a więc Internet, we współczesnym świecie odgrywa znaczącą rolę w kompleksowym systemie bezpieczeństwa państwa. Jak piszą M. Adamczuk i K. Liedel: bezpieczeństwo państwa zarówno w sferze militarnej, jak i pozamilitarnej, a także zewnętrznej, jak i wewnętrznej zyskało dodatkowy wymiar jakim poza lądem,

1 Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2017–2022. Ministerstwo Cyfryzacji 2017, www.gov.pl [dostęp: 30.07.2019 r.].

powietrzem, wodą i przestrzenią kosmiczną jest cyberprzestrzeń[2]. Sytuacja taka spowodowała powstanie nowych nieznanych dotychczas zagrożeń konfliktami międzynarodowymi, jak np. cyberwojna czy zagrożenia terrorystyczne określane jako tzw. cyberterroryzm. Cyberprzestrzeń, będąca elementem globalnego bezpieczeństwa w obecnej dobie, jest wyzwaniem dla całej społeczności międzynarodowej.

Jak podkreślają M. Adamczak i K. Liedel, potrzeba bezpiecznego i prawidłowego funkcjonowania cyberprzestrzeni wymaga od państwa, aby obszar funkcjonowania cyberprzestrzeni był priorytetem w krajowej polityce bezpieczeństwa, a państwo podejmowało próby efektywnego tworzenia systemów przeciwdziałania zagrożeniom na poziomach strategicznym, prawnym i instytucjonalnym[3]. W ostatnich latach w Polsce podjęto takie próby, jak chociażby opracowanie pierwszego dokumentu, jakim była Doktryna cyberbezpieczeństwa RP. Do podjęcia działań państw członków Unii Europejskiej w zakresie bezpieczeństwa w cyberprzestrzeni, zobowiązują zapisy Strategii bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń[4]. Dokument ten zobowiązuje kraje Unii Europejskiej do przyjęcia krajowych strategii w zakresie bezpieczeństwa sieci i informacji. Polska, biorąc pod uwagę fakt, że dopiero w roku ubiegłym (2018) kwestie cyberbezpieczeństwa zostały uregulowane ustawą, może być początkiem budowy zintegrowanego systemu bezpieczeństwa cyberprzestrzeni.

Dostępność do Internetu

Aby współczesne państwa mogły funkcjonować w globalnym świecie nazywanym często globalną wioską położoną w nowej przestrzeni o wirtualnym, transgranicznym, aterytorialnym i ponadnarodowym charakterze, musi być zapewniona dostępność do Internetu[5]. W tabeli nr 1 przedstawiono dostępność do Internetu w skali całego świata.

2 M. Adamczuk K. Liedel, *Doktryna cyberbezpieczeństwa*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12/7, s. 279, www.abw.gov./dokumenty i sprawozdania [dostęp: 30.07.2019].

3 Tamże, s. 1.

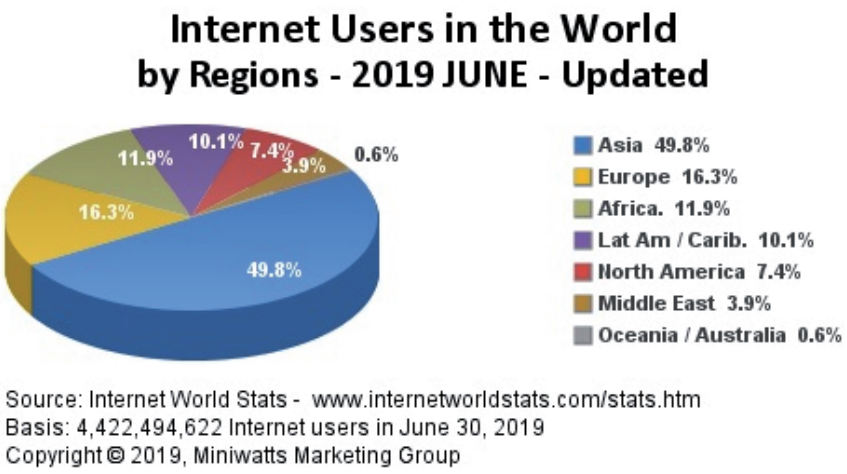
4 Wspólny Komunikat Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów; *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń* (https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52013JC0001) [dostęp: 30.07.2019].

5 J. Worona, *Cyberprzestrzeń a prawo międzynarodowe, status quo i perspektywy*, Uniwersytet w Białymstoku, rozprawa doktorska (https://repozytorium.uwb.edu.pl/jspui/handle/11320/5875) [dostęp: 27.07.2019].

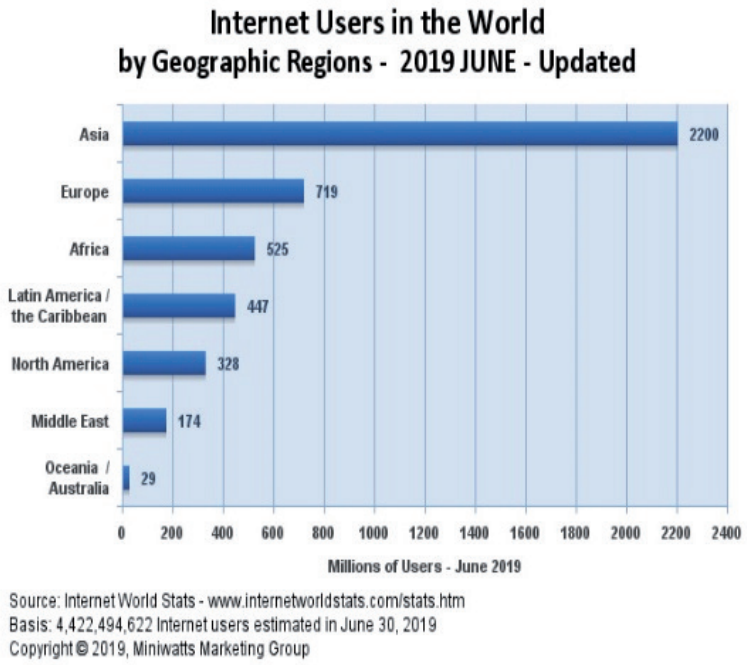
Tabela nr 1. Dostępność do Internetu w skali świata, opracowanie na podstawie www.internetworldstat.com/stats.htm [dostęp: 28.07.2019 r.]

Region świata	Populacja	Populacja (% świata)	Użytkownicy Internetu	Penetracja (% Internetu)	Wzrost w latach 2000 – 30.06.2019 %	Internet (% świata)
Afryka	1 320 038 716	17,1	525 148 631	39,8	11,53	11,9
Azja	4 241 972 790	55,0	2 200 658 148	51,9	1,82	49,8
Europa	829 173 007	10,7	719 413 014	86,8	585,6	16,3
Ameryka Łacińska	658 345 826	8,5	447 495 130	68,8	2,3	10,1
Bliski Wschód	258 356 867	3,3	173 576 793	67,2	5,1	3,9
Ameryka Północna	366 496 802	4,7	327 568 628	89,4	203,0	7,4
Australia i Oceania	41 839 201	0,5	28 634 278	68,4	276,0	0,6
Razem świat	7 716 223 209	100,0	4 422 494 622	57,3	11,0	100,0

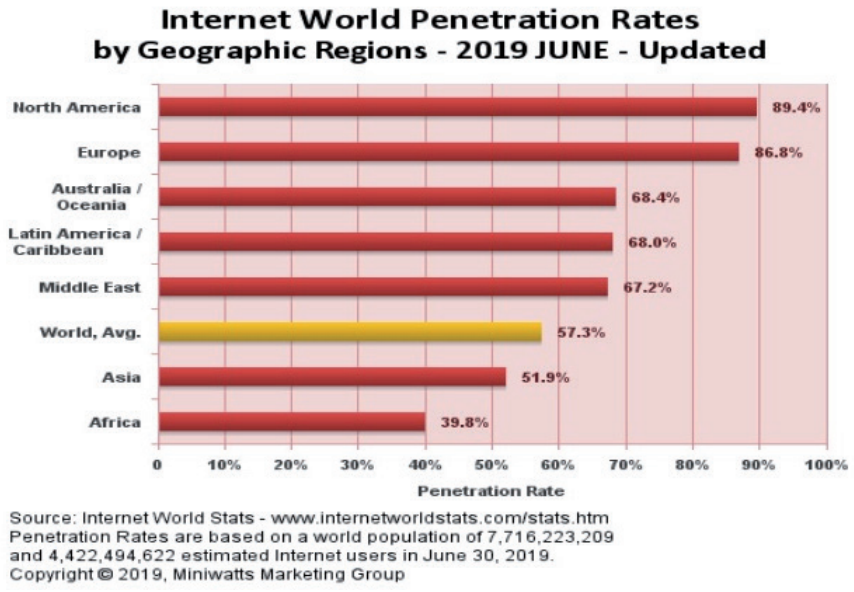
Na rys. 1 przedstawiono użytkowanie (penetracja) Internetu na świecie.



Rys. 1. Użytkowanie (penetracja) Internetu na świecie



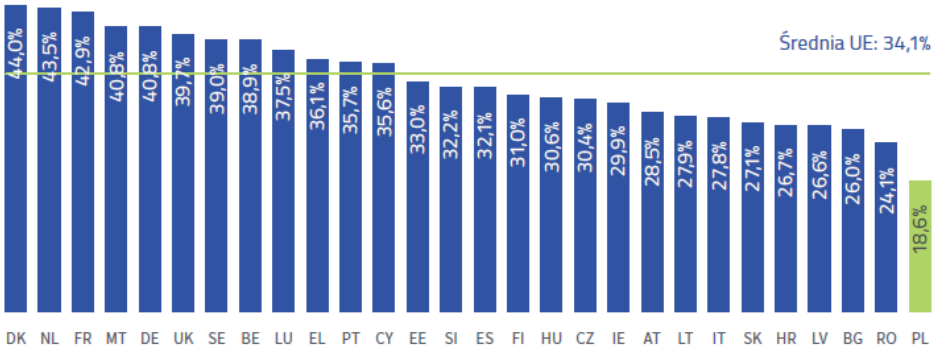
Rys. 2. Liczba użytkowników Internetu wg regionów świata



Rys. 3. Nasycenie (penetracja) Internetem poszczególnych regionów świata

Stan dostępności i nasycenia Internetu w Europie ilustrują wykresy na rysunkach 4 i 5.

WYKRES 12. **NASYCENIE USŁUGAMI INTERNETU STACJONARNEGO W UE**

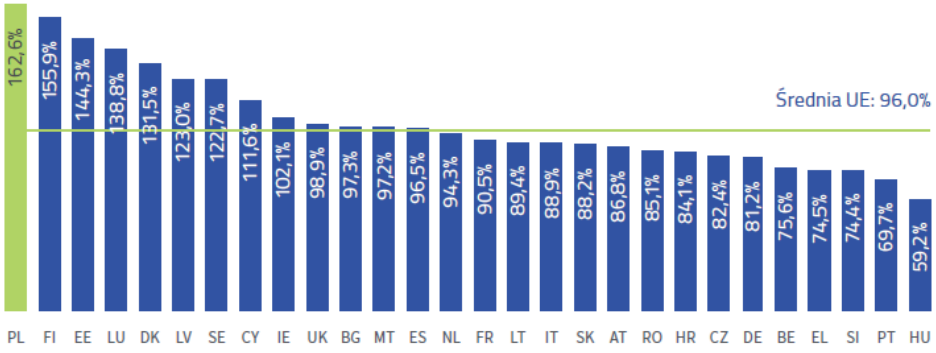


Źródło: Digital Agenda Scoreboard, czerwiec 2018 r.

Rys. 4. Nasycenie usługami Internetu stacjonarnego w Unii Europejskiej

Źródło: *Raport o stanie rynku telekomunikacyjnego w Polsce w 2018 r.*, Urząd Komunikacji Elektronicznej, Warszawa, czerwiec, 2019, s. 13, https://www.uke.gov.pl/.../raport_o_stanie_runku_telekomunikacyjnego [dostęp: 05.08.2019 r.]

WYKRES 13. **NASYCENIE USŁUGAMI INTERNETU MOBILNEGO W UE**



Źródło: Digital Agenda Scoreboard, czerwiec 2018 r.

Rys. 5. Nasycenie usługami Internetu mobilnego w Unii Europejskiej

Źródło: *Raport o stanie rynku telekomunikacyjnego w Polsce w 2018 r.*, Urząd Komunikacji Elektronicznej, Warszawa, czerwiec 2019, s. 13, https:www.uke.gov.pl/…raport_o_stanie_rynku_telekomunikacyjnego [dostęp: 05.08.2019 r.]

Jeżeli chodzi o Europę, to dostępność do Internetu na kontynencie ilustrują dane statystyczne dotyczące państw Unii Europejskiej[6]. Największą penetrację dostępu do Internetu stacjonarnego w 2018 r. zanotowano w Dani, która wyniosła 44% i była wyższa od średniej w UE o 10%. Jeżeli natomiast w przypadku dostępu do Internetu mobilnego penetracja ta wyniosła w 2018 r. 163% i była najwyższa spośród wszystkich państw Unii Europejskiej i była wyższa od średniej unijnej wynoszącej 96%, czyli polska dostępność do Internetu mobilnego była wyższa o 69% od średniej unijnej. Warto podkreślić, że dostęp do Internetu w gospodarstwach domowych wynosił 82% (z czego 68% nie odczuwało takiej potrzeby, a 54% nie odczuwało potrzeby posiadania dostępności do Internetu – co ciekawe stan taki nie zmienił się od trzech lat) przy średniej unijnej 87%, a w przedsiębiorstwach 95% przy średniej unijnej 97%[7].

Podstawowe definicje

Do podstawowych definicji charakteryzujących problematykę bezpieczeństwa informacji w cyberprzestrzeni i bezpieczeństwa zawartych w tej przestrzeni danych, systemów, zadań realizowanych przez różne systemy należą przede wszystkim:

Cyberprzestrzeń: termin „cyberprzestrzeń" pojawił się w obiegu publicznym w 1984 r. Jak podaje Tomasz R. Aleksandrowicz terminu „cyberprzestrzeń" użył po raz pierwszy William Gibson w swojej kultowej powieści cyberpunkowej „Neuromancer"[8]. Ta literacka wizja „cyberprzestrzeń" określała jako „konsensualna halucynacja, doświadczana każdego dnia przez miliardy uprawnionych użytkowników (…), jako graficzne odwzorowanie danych z banków wszystkich komputerów świata. Niewyobrażalna złożoność"[9]. W literaturze przedmiotu, jak podaje Tomasz R. Aleksandrowicz, cyberprzestrzeń określana jest także jako „całość powiązań ludzkiej działalności z udziałem ICT (ang. *Information and Communication Technology*)[10]. Niektórzy autorzy

6 *Raport o stanie rynku telekomunikacyjnego w Polsce w 2018 r.*, Urząd Komunikacji Elektronicznej, Warszawa 2019 (https://uke.gov.pl/akt/raport-o-stanie-rynku-telekomunikacyjnego-w-polsce-w-2018-r-,223.html)

7 https://antyweb.pl/gus… [dostęp: 28.07.2019].

8 T.R. Aleksandrowicz, *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, www.abw.gov.pl/download/1/2170 [dostęp: 25.07.2019].

9 Dosłowny cytat, patrz Tomasz R. Aleksandrowicz, op. cit.

10 Tamże za: A. Bógdoł-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003.

zajmujący się problematyką cyberbezpieczeństwa „cyberprzestrzeń" określają jako ogół powiązań o charakterze wirtualnym (nie przestrzennym w sensie fizycznym, niematerialnym) powstałych i istniejących dzięki ich fizycznym manifestacjom (postać występowania) takie jak komputery czy cała infrastruktura telekomunikacyjna[11]. Bardziej dokładną, precyzyjną definicję cyberprzestrzeni podają P. Tekielska i Ł. Czekaj[12], w której „mianem cyberprzestrzeni określa się sieć łączącą systemy komputerowe obejmujące jednostki centralne i ich oprogramowanie, ale także dane, sposoby i środki ich przesyłania. Cyberprzestrzeń obejmuje systemy powiązań internetowych, usługi teleinformatyczne oraz systemy zapewniające prawidłowe funkcjonowanie kraju, tj. systemy transportu, łączności, systemy infrastruktury energetycznej, wodociągowej, gazowej czy ochrony zdrowia".

Jeżeli chodzi o obowiązujące w Polsce akty normatywne (ustawy, rozporządzenia), programy, itp. dokumenty odnoszące się do cyberprzestrzeni i zapewnienia w niej bezpieczeństwa, to należy tu wymienić przede wszystkim Ustawę o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej. Ustawa przez „cyberprzestrzeń" rozumie przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne wraz z powiązanymi pomiędzy nimi relacjami z użytkownikami[13]. Identycznie „cyberprzestrzeń" definiowana jest w dokumencie rządowym, jakim są Krajowe Ramy Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022[14]. Warto w tym miejscu podkreślić, jak podaje Tomasz R. Aleksandrowicz, podobną definicję cyberprzestrzeni stosują Amerykanie[15]. Użyte w definicji „cyberprzestrzeń" określenie „sieci i systemy teleinformatyczne" oznacza:

---

11 M. Madej, *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego* [w:] M. Madej, M. Terlikowski (red.), *Bezpieczeństwo informatyczne państwa*, Warszawa 2003.

12 P. Tekielska, Ł. Czekaj, *Działania służb w Unii Europejskiej realizujących zadania na rzecz bezpieczeństwa cybernetycznego* [w:] M. Górka (red.), *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Warszawa 2014.

13 Ustawa z 29 sierpnia 2002 r. *o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej* (Dz.U. 2014 poz.1815 z późn. zm.)

14 Mc.gov. pl Krajowe ramy cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022, Ministerstwo Cyfryzacji, Warszawa 2017 [dostęp: 31.07.2019].

15 T.R. Aleksandrowicz, op. cit., s. 11.

- sieci łączności elektronicznej w rozumieniu art. 2 lit. a Dyrektywy 2002/11/WE[16],
- wszystkie urządzenia lub grupy wzajemnie połączonych lub powiązanych urządzeń, z których jedno lub większa ich liczba, wykonując program, dokonuje automatycznego przetwarzania danych cyfrowych,
- dane cyfrowe przechowywane, przetwarzane, odzyskiwane lub przekazywane przez elementy systemów teleinformatycznych, w celu ich eksploatacji, użycia, ochrony i utrzymania.

Konstatując przytoczone definicje, można zgodzić się z autorami opracowań, raportów itp. dokumentów, że „cyberprzestrzeń" jest działalnością człowieka, ale nie w sferze przestrzeni fizycznej[17]. Jest niezależna od miejsca przebywania człowieka, pozwala na daleko idącą anonimowość, itp.

Cyberprzestrzeń można charakteryzować różnymi cechami, spośród których najistotniejsze, to[18]:

- występuje niezależnie od miejsca,
- jest niezależna od odległości,
- czas nie ma żadnego znaczenia,
- nie jest określona granicami,
- zawiera znaczną swobodę anonimowości,
- istnieje możliwość ustalenia sprzętu, nigdy osoby.

W obecnym świecie cyberprzestrzeń jest swoistego rodzaju systemem nerwowym państwa, stąd tyle uwagi i podejmowanych działań państw, aby w cyberprzestrzeni można było zapewnić względne bezpieczeństwo. Tak, by cyberprzestrzeń nie stanowiła płaszczyzny, platformy, narzędzia czy też środka do występowania przeciwko powszechnym dobrom, jakie współczesne społeczeństwa wypracowały dla dalszego rozwoju i zabezpieczenia bytu przyszłym pokoleniom.

Kolejnym terminem charakteryzującym przedmiot rozważań w niniejszym artykule jest „cyberbezpieczeństwo".

---

16 Dyrektywa 2002/21/WE Parlamentu Europejskiego i Rady z marca 2002 r. *w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej* (Dyrektywa Ramowa) (Dz.U. UE. L.20011. 94.35 z póź. zm.)

17 Zob. M. Madej, *Rewolucja informatyczna*, op. cit.; T. R. Aleksandrowicz, *Bezpieczeństwo w cyberprzestrzeni*; J. Kowalewski, M. Kowalewski, *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*, „Telekomunikacja i Techniki Informatyczne" 2014, nr 1–2.

18 Zob. T.R. Aleksandrowicz, op. cit., s. 12.

Czym zatem jest cyberbezpieczeństwo, jak należy rozumieć to pojęcie i jakie zawiera w sobie informacje, cechy i inne elementy stanowiące o jego istocie tak przedmiotowej, a także i podmiotowej?

Problem bezpieczeństwa w cyberprzestrzeni wynika z faktu jej znaczenia dla funkcjonowania państwa, zarówno jako podmiotu geopolitycznego, podmiotu stosunków międzynarodowych, funkcjonowania współczesnego społeczeństwa, administracji rządowej, samorządowej, gospodarczej i wszystkich innych uczestników życia społeczno-polityczno-gospodarczego.

Cyberprzestrzeń w obecnych czasach odpowiedzialna jest za niemal wszystkie funkcje państwa tak w stosunkach międzynarodowych, jak i działaniach wewnątrz państwa, mająca na celu zapewnienie obywatelom niezbędnych dóbr w postaci usług, informacji itp. elementów warunkujących funkcjonowanie państwa. Bezpieczeństwo w cyberprzestrzeni, a inaczej cyberbezpieczeństwo, odnosi się wprost do bezpieczeństwa informacji, bez której trudno sobie wyobrazić dzisiejszą rzeczywistość.

W Krajowych Ramach Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej „cyberbezpieczeństwo" to „bezpieczeństwo sieci i systemów informatycznych" albo „bezpieczeństwo teleinformatyczne" oznacza odporność systemów teleinformatycznych przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych lub przetwarzanych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne[19]. Podobną definicję „cyberbezpieczeństwa" zawiera ustawa z 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa*[20]. Według ustawy „cyberbezpieczeństwo" jest odpornością systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Nieco inną definicję „cyberbezpieczeństwa" podają J. Kowalewski i M. Kowalewski. Odnoszą oni cyberbezpieczeństwo do ochrony cyberprzestrzeni, którą jest „zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mających na celu niezakłócone funkcjonowanie i bezpieczeństwo cyberprzestrzeni"[21]. Jak wynika z przytoczonych definicji, bezpieczeństwo cyberprzestrzeni czy też cyberbezpieczeństwo

19 Zob. Krajowe Ramy Polityki…, s. 11.

20 Ustawa z 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* (Dz.U. z 13 sierpnia 2018 r. poz. 1560)

21 J. Kowalewski, M. Kowalewski, op. cit., s. 25.

odnosi się do bezpieczeństwa informacji. To właśnie informacja traktowana jest jako przedmiot bezpieczeństwa w cyberprzestrzeni, bowiem informacja jest takim zasobem społeczeństwa który jest nieodzownym elementem postępu i cywilizacyjnego rozwoju[22]. Charakteryzując cyberbezpieczeństwo niektórzy analitycy twierdzą, że bezpieczeństwo cyberprzestrzeni można określić brakiem ryzyka utraty danych informacyjnych[23], czyli że zasobem, który chroni się w cyberprzestrzeni jest właśnie informacja. Mówi się o bezpieczeństwie w cyberprzestrzeni w kategoriach walki czy też wojny informacyjnej, co, jak podkreśla T.M. Aleksandrowicz, sytuuje bezpieczeństwo informacji w cyberprzestrzeni jako integralnej części bezpieczeństwa narodowego przed zagrożeniami informacyjnymi. Informacja zdaniem T.M. Aleksandrowicza jest zarówno celem ataku jak i bronią, tarczą ale i mieczem, zasobem, który obejmuje fizyczne niszczenie infrastruktury przeciwnika, niszczenie zasobów informacyjnych przeciwnika i zapewnienia jednocześnie własne zasoby informacyjne[24]. Bezpieczeństwo informacji w cyberprzestrzeni zapewnia ochronę podstawowych zasobów społeczeństwa informacyjnego, bez których niemożliwy byłby postęp i rozwój cywilizacyjny.

Dlatego cyberbezpieczeństwo musi być tak zbudowane i musi tak funkcjonować, aby cyberprzestrzeń była odporna na różnego rodzaju zagrożenia.

Co to są zagrożenia cyberprzestrzeni, jakie są ich rodzaje i jaki mają charakter oraz jakie mogą powodować skutki?

Według ustawy o krajowym systemie cyberbezpieczeństwa[25], zagrożeniem cyberbezpieczeństwa jest potencjalna przyczyna wystąpienia incydentu. Ustawa jako incydent uznaje zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo. Wspomniana ustawa rozróżnia pięć rodzajów incydentu, który może być zagrożeniem dla cyberbezpieczeństwa, a mianowicie:

- incydent krytyczny, którym jest zagrożenie skutkujące znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, prawa i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy Zespół Reagowania na Incydenty Komputerowe, działający na poziomie krajowym przez Szefa Agencji Bezpieczeństwa Wewnętrznego (CSIRT GOV) albo Zespół Reagowania na Incydenty

22 Tamże, s. 24.

23 B. Pacek, R. Hoffman, *Działania sił zbrojnych w cyberprzestrzeni*, Warszawa 2013.

24 T.M. Aleksandrowicz, op. cit., s. 15.

25 Ustawa z dnia 5 lipca *o krajowym systemie cyberbezpieczeństwa*, op. cit.

Bezpieczeństwa Komputerowego, działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej (CSIRT MON), albo Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy (CSIRT NASK)[26],

- incydent poważny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej[27],
- incydent istotny – incydent, który ma istotny wpływ na świadczenie usługi cyfrowej w rozumieniu art. 4 rozporządzenia wykonawczego Komisji (UE) 2018/15 z 30 stycznia 2018 r. ustanawiającego zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148, w odniesieniu do dalszego doprecyzowania elementów jakie mają być uwzględnione przez dostawców usług cyfrowych, w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych oraz parametrów służących do określenia, czy incydent ma istotny wpływ[28],
- incydent w podmiocie publicznym – incydent, który powoduje lub może powodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny[29].

Wymienione wyżej incydenty mogą mieć różną formę. Mogą być także spowodowane różnym działaniem oraz mogą również powodować różne skutki zarówno materialne jaki i niematerialne, stwarzające zagrożenia dla funkcjonowania poszczególnych obszarów działalności państwa, stwarzające zagrożenia dla zbiorowości, grup społecznych jak i jednostek.

Statystyki za 2018 r. pokazują skalę tych incydentów.

---

26 Każdy z tych zespołów ma ustawowo przypisane działy gospodarki narodowej, instytucje i inne podmioty państwowe do ochrony bezpieczeństwa w cyberprzestrzeni (szczegółowo będzie o tym w dalszej części artykułu).

27 Wykaz usług kluczowych zawiera wspomniana ustawa. Zasady zaliczania (uznawania) incydentu za poważny określa Rozporządzenie Rady Ministrów z 31 października 2018 r. *w sprawie progów uznania incydentu za poważny* (Dz.U. 2018 poz. 2180).

28 Dz.Urz. UE L. 26 z 31.01.2018 (w dalszej treści artykułu będzie określane jako „rozporządzenie wykonawcze 2018/151").

29 Ustawa z 5 lipca *o krajowym systemie cyberbezpieczeństwa*, op. cit., w art. 4 pkt. 7–15 wymienia te podmioty publiczne, które objęte są bezpieczeństwem przed zagrożeniem cyberprzestrzeni.

Według raportu o stanie bezpieczeństwa cyberprzestrzeni RP w 2018 r.[30] przygotowanego przez Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego Agencji Bezpieczeństwa Wewnętrznego w roku 2018 zanotowano 31 865 zgłoszeń incydentów z czego faktyczne naruszenie bezpieczeństwa teleinformatycznego instytucji miało miejsce w 6236 przypadkach, co stanowi wzrost w porównaniu z rokiem 2017, w którym faktycznych incydentów zanotowano 5819[31]. W latach ta statystyka zgłoszeń i faktycznych incydentów przedstawiała się następująco:

- rok 2016: zgłoszeń – 19 954, faktycznych incydentów 9288,
- rok 2017: zgłoszeń – 28 281, faktycznych incydentów 5819,
- rok 2018: zgłoszeń – 31865, faktycznych incydentów 6236.

Jak wynika z tego zestawienia, tendencja zgłoszeń o potencjalnym wystąpieniu incydentów komputerowych jest stale rosnąca. Jak podają autorzy raportu przyczyną takiego stanu rzeczy może być m.in. wzrost zainteresowania potencjalnych atakujących rządowymi sieciami w Polsce[32].

Raport za 2018 r. opracowany przez Zespół CERT Polska[33] wskazuje, że CSIRT NASK odnotował 19 439 incydentów, z czego po szczegółowej analizie uznano zaistnienie 5675 incydentów faktycznych, co w stosunku do 2017 r. stanowi wzrost o 17,5%. W zeszłym roku najczęściej występującym rodzajem incydentu był phishing[34], który stanowił 44% wszystkich incydentów. Na drugim miejscu 23% były incydenty związane z dystrybucją złośliwego oprogramowania, a na trzecim miejscu, ok. 11,2%, to incydenty o charakterze spamu. W 2018 r. odnotowano trzykrotny wzrost w stosunku

30 Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2018; www.csirt.gov.pl [dostęp: 05.08.2018].

31 Wg CSIRT GOV różnica pomiędzy incydentami zgłoszonymi a incydentami faktycznymi wynika z faktu weryfikacji zgłoszeń, podczas której porównuje się czy zgłoszona informacja nosi znamiona incydentu faktycznego czy jest to tylko tzw. *false positive*. Ponadto w wielu przypadkach ta sama złośliwa wiadomość trafia do szerokiego grona odbiorców, co generuje wiele zgłoszeń jednego incydentu.

32 Patrz: Raport CSIRT GOV, który obsługuje takie podmioty, jak wszystkie instytucje rządowe, Narodowy Bank Polski, Bank Gospodarstwa Krajowego, operatorzy infrastruktury krytycznej

33 Zespół CERT Polska podlega CSIRT NASK, któremu podlegają takie podmioty, jak administracja samorządowa, dostawcy usług cyfrowych, większość tzw. dostawców usług kluczowych (dostawców usług kluczowych wymienia ustawa z 5 lipca 2018 r. opt. cit.).

34 Phisihing jako incydent komputerowy oznacza tworzenie fałszywych stron w celu pozyskania danych uwierzytelniających (loginu i hasła) do wykorzystania w bankach i innych serwisach.

do 2017 r. incydenty związane z fałszywymi sklepami internetowymi. W porównaniu z 2017 r. incydenty o charakterze spamu w 2018 r. podwoiły swoja liczbę. Według Raportu[35] CSIRT NASK „obsłużył"[36] następującą liczbę poszczególnych incydentów (zagrożeń) cyberprzestrzeni:

Tabela 2. Incydenty obsłużone przez CSIRT NASK w 2018 r.

Nazwa incydentu	Liczba incydentów	%
Obraźliwe i nielegalne treści	431	11,53
Złośliwe oprogramowanie	862	23,05
Gromadzenie informacji	101	2,70
Próby włamań	153	4,09
Włamania	125	3,34
Dostępność zasobów	49	1,31
Atak na bezpieczeństwo informacji	46	1,23
Oszustwa komputerowe	1878	50,23
Podatne usługi	171	1,85
Inne	25	0,67

Opr. własne na podstawie Raportu za 2018 r.[37]

Natomiast zestawienie incydentów, które zaistniały w 2018 r. i zostały „obsłużone" przez Zespół CSIRT NASK w podziale na poszczególne sektory gospodarki ilustruje tabela 3.

Tabela 3. Incydenty komputerowe zaistniałe w 2018 r., obsłużone przez CSIRT NASK w podziale na poszczególne sektory gospodarki.

Sektor gospodarki	Liczba incydentów	%
Infrastruktura cyfrowa	29	0,78
Służba zdrowia	13	0,35

35 Patrz: Raport CERT POLSKA za 2018 rok.

36 Nazwa działań Zespołu CSIRT NASK

37 Raport CERT Polska, op. cit.

Bankowość	643	17,20
Finanse	62	1,66
Energetyka	20	0,53
Transport	51	1,36
Sektor publiczny	85	2,27
Wodociągi	2	0,05
Inne	2 834	75,80
Razem	3739	75,80

Raport przedstawiony przez CSIRT NASK zawiera także zestawienie incydentów komputerowych, jakie zaistniały na przestrzeni ponad 20 lat, które były przedmiotem ingerencji Zespołu CERT Polska. Zestawienie to ilustruje tabela 4.

Tabela 4. Liczba incydentów na przestrzeni lat 1996–2018, w stosunku do których Zespół CERT podjął działania

Rok	**1996**	**1997**	**1998**	**1999**	**2000**	**2001**	**2002**	**2003**	**2004**	**2005**	**2006**	**2007**
Liczba incydentów	50	75	100	105	126	741	1013	1196	1222	2516	2427	2108

Rok	**2008**	**2009**	**2010**	**2011**	**1012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**
Liczba incydentów	1796	1292	674	605	1082	1219	1282	1456	1926	3182	3739

Opracowanie na podstawie Raportu CSIRT NASK za 2018 r.

Jak wynika z przedstawionych zestawień, w podmiotach wobec których CSIRT NASK jest zobowiązany do podjęcia ingerencji systematycznie rośnie. Znaczny wzrost zanotowano zwłaszcza w ostatnich dwóch latach.

Nie można przedstawić zakresu incydentów, wobec których umocowanym ustawowo podmiotem jest CSIRT, MON, ze względu na charakter działalności podmiotów podlegających Ministrowi Obrony Narodowej. Są to dane zastrzeżone i nie są publikowane. Zadaniem CSIRT MON jest obsługa wszystkich incydentów związanych z obronnością kraju.

W podsumowaniu statystyk incydentów internetowych warto przytoczyć dane podane przez Instytut Kościuszki[38]. W 2017 r. w wyniku cyberataków gospodarka światowa straciła ponad 600 mld dolarów[39]. Analitycy podają, że w 2030 r. straty w wyniku cyberataków mogą sięgnąć 1,2 bln dolarów, czyli około 0,9% światowego PKB[40]. Cyberatak może sparaliżować niemal wszystkie sektory gospodarki, jak to miało miejsce w wyniku ataku NotPetya w 2017 r., kiedy znane firmy o światowym zasięgu poniosły straty rzędu 10 mld dolarów. Jak podaje CERT Polska w naszym kraju występuje także tendencja do ponoszenia strat przez rodzimą gospodarkę w wyniku cyberataków. W 2018 r. w stosunku do 2017 r. zanotowano o 17,5% wzrost incydentów, które spowodowały zakłócenia i przestoje w funkcjonowaniu. Według danych raportu o stanie cyberbezpieczeństwa polskie podmioty gospodarcze narażone są na straty rzędu 4 999,72 euro rocznie[41].

Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczpospolitej Polskiej

Cyberprzestrzeń, która w obecnych czasach spełnia swoistego rodzaju system nerwowy państwa, jak i stosunków międzynarodowych w skali globalnej, wymaga odpowiedniej ochrony przed różnego rodzaju zagrożeniami o różnej skali, charakterze i celu, jeżeli chodzi o osiągnięcie skutków ataku. Każde państwo stara się zapewnić „swojej" cyberprzestrzeni skuteczne warunki w zakresie jej ochrony przed incydentami zakłócającymi funkcjonalność sieci teleinformatycznej, wykorzystania usług informatycznych przez przestępców (pojawił się nowy rodzaj przestępczości jakim jest „cyberprzestępczość"), wykorzystania cyberprzestrzeni do prowadzenia swoistego rodzaju wojny cybernetycznej – wiele państw posiada w składzie swoich armii specjalne oddziały do prowadzenia takich wojen itd.

Polska także stara się budować bezpieczeństwo dla swojej cybeprzestrzeni.

Aktualnie polski system cyberbezpieczeństwa opiera się o ustawę *o krajowym systemie cyberbezpieczeństwa*[42], która uwzględnia Dyrektywę Parlamentu Europejskiego

38 *Wyzwania w cyberprzestrzeni, przykłady rozwiązań, zagrożenia , regulacje*, Instytut Kościuszki, Kraków 2019, www.ik.org.pl [dostęp: 08.08.2019].

39 *Statystyki cyberbezpieczeństwa w Wyzwania…*, , op. cit., s. 24.

40 Tamże.

41 *Wyzwania w cyberprzesrzeni…*, op. cit., s. 24.

42 Ustawa z 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* (Dz.U. RP z 13 sierpnia 2018 r. poz. 1560); należy nadmienić że ustawa w całości uwzględnia Dyrektywę Rady 2008/114/WE w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony, a także ustawę o ochronie danych osobowych RODO.

i Rady (UE)[43]. Polski system cyberbeczeństwa zbudowany w oparciu o ustawę[44] w pełni spełnia warunki określone w dokumencie rządowym, jakim są Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2020[45].

Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczpospolitej Polskiej kierują się zasadą poszanowania praw i wolności w cyberprzestrzeni, reprezentują kompleksowe podejście do bezpieczeństwa, a cyberbezpieczeństwo traktują jako istotny element polityki państwa.

Krajowe Ramy Polityki Cyberbezpieczeństwa określają kontekst strategiczny cyberbezpieczeństwa, zakres polityki państwa w zakresie cyberbezpieczeństwa, określają wizję, cel główny oraz cele strategiczne tej polityki. Krajowe Ramy Polityki Cyberbezpieczeństwa RP na lata 2017–2022 są kontynuacją działań rządu określonych w 2013 r. jako Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej. Krajowe Ramy Polityki na lata 2017–2022 określają ramowe działania mające na celu uzyskanie wysokiego poziomu odporności krajowych systemów teleinformatycznych i wszystkich podmiotów korzystających z tych systemów.

Wizja Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej jest następująca: „w roku 2022 Polska będzie krajem bardziej odpornym na ataki i zagrożenia płynące z cyberprzestrzeni. Dzięki synergii działań wewnętrznych i międzynarodowych, cyberprzestrzeń RP będzie stanowić bezpieczne środowisko umożliwiające realizowanie wszystkich funkcji państwa i pozwalać na pełne wykorzystywanie potencjału gospodarki cyfrowej, przy równoczesnym poszanowaniu praw i wolności obywateli”[46].

Celem głównym polityki państwa w cyberprzestrzeni jest „zapewnienie wysokiego poziomu bezpieczeństwa sektora publicznego, sektora prywatnego oraz obywateli w zakresie świadczenia lub korzystania z usług kluczowych oraz usług cyfrowych”[47].

Krajowe Ramy Polityki Cyberbezpieczeństwa określają cztery cele szczegółowe których realizacja warunkuje osiągnięcie celu głównego i zrealizowania wizji w zakresie cyberbezpieczeństwa, a mianowicie:

---

43 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. *w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa w sieci i systemach informatycznych na terytorium UE* (Dz.U. UE L 194 z 19.07.2016).

44 Tamże; ustawa z 5 lipca 2018 r.

45 *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2020*, Ministerstwo Cyfryzacji, Warszawa 2017, https://www.gov.pl/...cyfryzacja/krajowe-ramy-polityki-cyberbezpieczeństwa… [dostęp: 28.07.2019].

46 *Krajowe Ramy…*, op. cit., s. 8.

47 Tamże.

- osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa,
- wzmocnienie zdolności do przeciwdziałania cyberzagrożeniom,
- zwiększenie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni,
- zbudowanie silnej pozycji międzynarodowej RP w obszarze cyberbezpieczeństwa.

Każdy z tych czterech celów szczegółowych zawiera szczegółowe wytyczne ich realizacji, co stwarza warunki do osiągnięcia zamierzonych efektów.

Ponadto dokument jakim są Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej zawiera niezbędne informacje dotyczące wdrażania postanowień tego dokumentu oraz zasady raportowania Radzie Ministrów o wdrażaniu tych zasad polityki państwa.

Na podstawie postanowień, realizacji ramowych ram polityki w zakresie cyberbezpieczeństwa powołana została pierwsza w Polsce ustawa ustanawiająca krajowy system cyberbezpieczeństwa.

Krajowy system cyberbezpieczeństwa

Krajowy system cyberbezpieczeństwa powstał w oparciu o ustawę z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa*, która weszła w życie 28 sierpnia 2018 r.[48]. Ustawa zdefiniowała system poprzez określenie jego celu, jakim jest „zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienia obsługi incydentów”[49]. Użyte w ustawie określenie „usługa kluczowa” oznacza usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej[50].

48 Ustawa z 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* (Dz.U. RP z 13 sierpnia 208 r. poz. 1560).

49 Tamże, art. 3.

50 Rodzaje usług kluczowych zawiera załącznik nr 1 do ustawy poprzez przyporządkowanie usługi kluczowej do danego sektora, podsektora i rodzaju podmiotu realizującego taką usługę i jej

Natomiast „usługą cyfrową" jest usługa świadczona drogą elektroniczną, w rozumieniu ustawy o świadczeniach usług drogą elektroniczną. Wykaz usług cyfrowych zawiera załącznik nr 2 do ustawy[51], w którym wymieniono następujące rodzaje tych usług cyfrowych:

- *intensywna platforma cyfrowa:* usługa, która umożliwia konsumentom lub przedsiębiorcom zawieranie umów drogą elektroniczną z przedsiębiorcami na stronie internetowej platformy handlowej albo na stronie internetowej przedsiębiorcy, który korzysta z usług świadczonych przez internetową platformę handlową,
- *usługa przetwarzana w chmurze:* usługa umożliwiająca dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystania przez wielu użytkowników,
- *wyszukiwarka internetowa*: usługa, która umożliwia użytkownikom wyszukiwanie wszystkich stron internetowych lub stron internetowych w danym języku za pomocą zapytania przez podanie słowa kluczowego, wyrażenia lub innego elementu, przedstawiająca w wyniku odnośniki, odnoszące się do informacji związanych z zapytaniem.

Usługi kluczowe realizuje tzw. operator usługi kluczowej, którym zgodnie z art. 5 ustawy, jest podmiot posiadający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, wobec którego właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu za operatora usługi kluczowej[52].

Dostawcami usług cyfrowych są osoby prawne albo jednostki organizacyjne nieposiadające osobowości prawnej, mające siedzibę lub zarząd na terytorium Rzeczypospolitej Polskiej albo przedstawiciela mającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej[53].

---

znaczenie dla utrzymania krytycznej działalności społecznej i gospodarczej, (art. 6 ust. 1 ustawy z dnia 5 lipca 2018 r.), Rada Ministrów określiła w rozporządzeniu z 11 września 2018 r. wykaz usług kluczowych oraz progi istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz.U. RP z 11 września 2018 r., poz. 1806).

51 Ustawa z 5 lipca, op. cit.

52 Tamże; natomiast organy właściwe ds. cyberbezpieczeństwa ustawo określa w art. 41. Organami takimi są np. dla sektora energii – minister właściwy ds. energii, dla sektora transportu – minister właściwy ds. transportu, dla sektora finansowego – Komisja Nadzoru Finansowego, dla sektora ochrony zdrowia – minister właściwy ds. zdrowia, dla dostawców usług cyfrowych – minister właściwy ds. informatyzacji. Tymi operatorami usług kluczowych są najwięksi przedsiębiorcy z poszczególnych sektorów gospodarki.

53 Tamże, art. 17 ust. 1.

Ustawa określa szczegółowe zakresy działań i obowiązków zarówno dla operatorów usług kluczowych, jak i dostawców usług cyfrowych[54].

Spośród wielu obowiązków operatora usługi kluczowej można wymienić między innymi takie, jak:

- wdrożenie systemu zarządzania bezpieczeństwem w systemie informacyjnym służącym do świadczenia usługi kluczowej, wyznacza osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, w tym przede wszystkim z właściwym Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego ABW, MON lub NASK w zależności od tego w czyjej gestii jest dana usługa kluczowa. Operator usługi kluczowej opracowuje, stosuje i aktualizuje wymaganą dokumentację cyberbezpieczeństwa dla systemu informacyjnego obsługującą daną usługę kluczową, a raz na dwa lata przeprowadza audyt tego systemu. Ponadto operator usługi kluczowej zobowiązany jest do wykonywania wielu innych obowiązków w zakresie zapewnienia cyberbezpieczeństwa w sieciach informacyjnych wykorzystywanych do świadczenia przez siebie danych usług kluczowych.

Również dostawca usługi cyfrowej ma w ustawie określone zadania w zakresie cyberbezpieczeństwa, spośród których można wymienić m.in.:

- stosuje właściwe i proporcjonalne, zarówno techniczne jak i organizacyjne, środki w zakresie zarządzania ryzykiem, na jakie narażone są systemy informacyjne służące do wykonywania usługi cyfrowej[55],
- dostawca usługi cyfrowej przeprowadza czynności w zakresie wykrywania, rejestrowania, analizowania oraz klasyfikowania incydentów w sieciach teleinformatycznych stosowanych w dostawie danej usługi.

Bardzo istotnym elementem krajowego systemu cyberbezpieczeństwa są jego podmioty, którymi wg ustawy z 5 lipca 2018 r., są:

- operatorzy usług kluczowych i dostawcy usług cyfrowych,
- Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego:

54 Tamże; przepisy rozdziału 3 określają szczegółowe obowiązki dla operatora usługi kluczowej, a w rozdziale 4 dla dostawcy usługi cyfrowej.

55 Zasady zarządzania ryzykiem w systemach informacyjnych określa rozporządzenie wykonawcze Komisji (UE) 2016/1148 z 30 stycznia 2018 r. ustanawiające zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148, w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych oraz parametrów służących do określania, czy incydent ma istotny wpływ (Dz.U. L. z 19.7.2016).

a. CSIRT GOV, działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego,
b. CSIRT MON, działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej,
c. CSIRT NASK, działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy.

Zadania CSIRT GOV, CSIRT MON oraz CSIRT NASK szczegółowo określa ustawa w art. 26 ust. 5–7[56]:

- sektorowe zespoły cyberbezpieczeństwa[57],
- jednostki sektora finansów publicznych,
- instytuty badawcze,
- Narodowy Bank Polski,
- inne wymienione w art. 4 ustawy[58].

W Krajowym Systemie Cyberbezpieczeństwa funkcjonują ponadto inne podmioty i organy państwa, które wymienia ustawa i określa dla nich szczegółowe zadania[59].

Bardzo istotnym elementem Krajowego Systemu Cyberbezpieczeństwa jest pełnomocnik rządu do spraw koordynowania działań i realizowania polityki państwa w zakresie zapewnienia cyberbezpieczeństwa w Rzeczypospolitej Polskiej. Ponadto przy Radzie Ministrów działa kolegium jako organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa[60].

Należy także podkreślić, że ustawa o krajowym systemie cyberbezpieczeństwa zawiera wykaz sankcji w postaci kar pieniężnych w stosunku do podmiotów, organów i instytucji nierealizujących zadań w zakresie cyberbezpieczeństwa.

Wydaje się, że można zaryzykować stwierdzenie, iż krajowy system cyberbezpieczeństwa zbudowany w oparciu o przepisy ustawy z 5 lipca 2018 r., jest systemem optymalnym,

---

56 Ustawa z 5 lipca, op. cit.

57 Sektorowe zespoły cyberbezpieczeństwa funkcjonują w sektorach wymienionych w załączniku 1 do ustawy z dnia 5 lipca 2018 r.

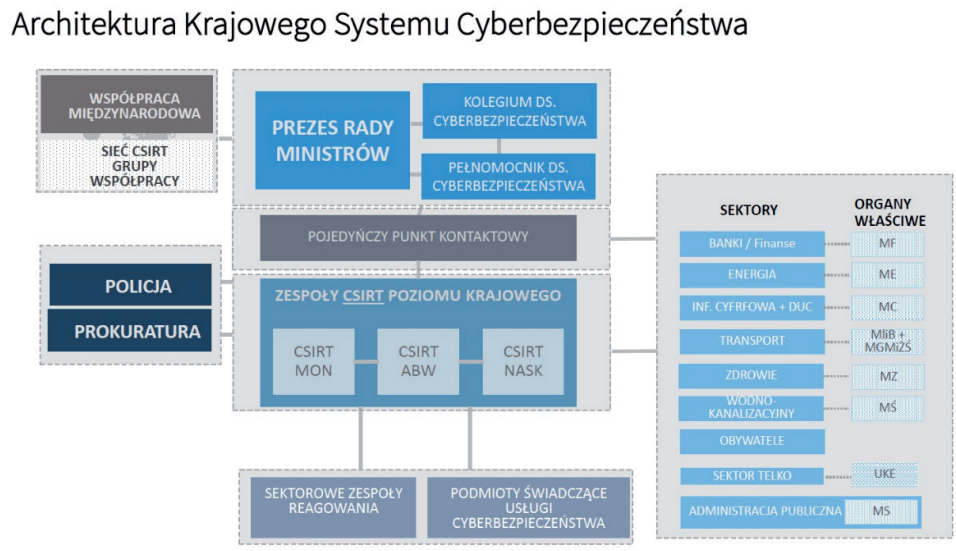
58 Ustawa z 5 lipca, op. cit.

59 Patrz: rozdział 5 „Obowiązki podmiotów publicznych"; rozdział 7 „Zasady udostępniania informacji i przetwarzania danych osobowych, organy właściwe do spraw cyberbezpieczeństwa"; rozdział 9 „Zadania dla ministra właściwego do spraw informatyzacji"; rozdział 10 „Zadania Ministra Obrony narodowej"; rozdział 11 „Zasady nadzoru i kontroli nad operatorami usług kluczowych i dostawców usług cyfrowych".

60 Zadania i zasady funkcjonowania pełnomocnika oraz skład kolegium określa ustawa w rozdziale 12.

gwarantującym w miarę pełną ochronę cyberprzestrzeni przed różnego rodzaju zagrożeniami w postaci incydentów zakłócających funkcjonowanie systemów teleinformatycznych stosowanych w zarządzaniu państwem, sterowaniu jego gospodarką, usługami zapewniającymi zaspokojenie podstawowych potrzeb funkcjonowania społeczeństwa w XXI w. Ustawa tworzy ramy krajowego systemu cyberbezpieczeństwa w Polsce.

Strukturę organizacyjno-funkcjonalną tego systemu ilustruje schemat na rys. 6.



Rys. 6. Architektura Krajowego Systemu Cyberbezpieczeństwa w Polsce.
Źródło: Narodowa Platforma Cyberbezpieczeństwa, s. 8

Podsumowanie

Cyberprzestrzeń tworzą technologie, rozwiązania oraz systemy, które stoją na pierwszej linii zagrożeń płynących z sieci. Technologie te są kluczowym ogniwem bezpieczeństwa. Cyberprzestrzeń stała się jeszcze jedną po lądzie, powietrzu, wodzie i kosmosie domeną działań militarnych[61].

Zapewnienie bezpieczeństwa informacji przesyłanych w cyberprzestrzeni jest wyzwaniem współczesnych czasów, rządów każdego państwa.

Polski Krajowy System Cyberbezpieczeństwa oparty jest o szereg podmiotów, zarówno państwowych, administracji publicznej, jak i gospodarczych.

61 Cyberprzestrzeń uznana została przez NATO jako kolejna domena działań operacyjnych na szczycie w Warszawie w 2016 r.

Powiązanie tego systemu poprzez współpracę międzynarodową w ramach takich organizacji, których Polska jest aktywnym uczestnikiem UE, NATO, ONZ, OBWE i innych, stwarza warunki do w miarę skutecznego zapewnienia cyberbezpieczeństwa i niedopuszczenia do penetracji polskiej cyberprzestrzeni przez incydenty, prowadzące zarówno do strat materialnych, jak i wizerunkowych.

Zapewnienie bezpieczeństwa w cyberprzestrzeni nabiera znaczenia wobec gwałtownie rozwijającej się sztucznej inteligencji (ang. *artifical intelligece)* AI, która jest działem informatyki zajmującym się systemami inteligentnymi wspomagającymi, bądź będącymi substytutem pracy umysłowej człowieka[62]. Jak piszą autorzy raportu[63] „Wyzwania w cyberprzestrzeni", obecnie rozpoczyna się era sztucznej inteligencji, która przekształca dotychczasowy świat cyfrowy, co z pewnością nasili liczby cyberataków i ich jakościowej zmiany.

Jak pisze Richard Baldwin: „sztuczna inteligencja i globalizacja wstrząsną rynkiem pracy ludzkiej, bowiem zastąpienie pracowników klonami ludzkiej inteligencji będzie dużo skuteczniejsze od zdalnej obsługi z *call center*"[64]. To temat na odrębne opracowanie.

Literatura

[1] Adamczuk M., Liedel K., *Doktryna cyberbezpieczeństwa,* „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12/7.

[2] Aleksandrowicz T.R., *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, www.abw.gov.pl/download/1/2170.

[3] Bógdoł-Brzezińska A., Gawrycki M.F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003.

[4] Baldwin R., *Globotyczny przewrót. Globalizacja, robotyka i przyszłość rynku pracy*, Oxford University Press 2019 za Gazetą Wyborczą z 9–10 lutego 2019, Magazyn Świąteczny „Roboty w białych kołnierzykach odbiorą nam pracę".

[5] Dul F., *Wprowadzenie do sztucznej inteligencji*, Politechnika Warszawska, Wydział Mechaniki Energetyki i Lotnictwa, Warszawa 2014.

62 F. Dul, *Wprowadzenie do sztucznej inteligencji*, Politechnika Warszawska, Wydział Mechaniki Energetyki i Lotnictwa,Warszawa 2014, s. 5, https://www.meil.edu.pl/pl/content/dowmnolad/.../AI_Wstęp_14.pdf [dostęp: 17.08.2019].

63 *Wyzwania w cyberprzestrzeni,* (praca zbiorowa), Instytut Kościuszki, Kraków 2019, s. 40, https://ik.org.plwyzwania-w-cyberprzestrzeni-przyklady – rozwiazan-zagroz… [dostęp: 17.08.2019].

64 R. Baldwin, *Globotyczny przewrót. Globalizacja, robotyka i przyszłość rynku pracy*, Oxford University Press, 2019, za Gazetą Wyborczą z 9–10 lutego 2019 r., *Magazyn Świąteczny*, „Roboty w białych kołnierzykach odbiorą nam pracę", s. 8.

[6] Dyrektywa 2002/21/WE Parlamentu Europejskiego i Rady z 7 marca 2002 r. w sprawie *wspólnych ram regulacyjnych sieci i usług łączności elektronicznej* (Dyrektywa Ramowa) (t.j. Dz.U. UE. L.20011. 94.35 z póź. zm.).
[7] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa w sieci i systemach informatycznych na terytorium UE (Dz.U. UE L 194 z 19.07.2016).
[8] Kowalewski J., Kowalewski M., *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*, „Telekomunikacja i Techniki Informatyczne" 2014, nr 1–2.
[9] Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2017–2022, Ministerstwo Cyfryzacji 2017.
[10] Madej M., *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego* [w:] *Bezpieczeństwo informatyczne państwa*, Madej M., Terlikowski M. (red.), Warszawa 2003.
[11] Pacek B., Hoffman R., *Działania sił zbrojnych w cyberprzestrzeni*, Warszawa 2013.
[12] Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2018 (www.csirt.gov.pl).
[13] Raport o stanie rynku telekomunikacyjnego w Polsce w 2018 r. Urząd Komunikacji Elektronicznej, Warszawa 2019 (https://uke.gov.pl/akt/raport-o-stanie-rynku-telekomunikacyjnego-w-polsce-w-2018-r-,223.html).
[14] Rozporządzenie Rady Ministrów z 31 października 2018 r. *w sprawie progów uznania incydentu za poważny* (Dz.U. 2018 poz.2180).
[15] Tekielska P., Czekaj Ł., *Działania służb w Unii Europejskiej realizujących zadania na rzecz bezpieczeństwa cybernetycznego* [w:] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Górka M. (red.), Warszawa 2014.
[16] Ustawa z 29 sierpnia 2002 r. *o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej* (t.j. Dz.U. 2014 poz.1815 z późn. zm.).
[17] Ustawa z 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* (Dz.U. z 13 sierpnia 2018 r. poz. 1560).
[18] Worona J., *Cyberprzestrzeń a prawo międzynarodowe, status quo i perspektywy*, Uniwersytet w Białymstoku, rozprawa doktorska (https://repozytorium.uwb.edu.pl/jspui/handle/11320/5875).
[19] Wspólny Komunikat Parlamentu Europejskiego, Rady Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń* (https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52013JC0001).
[20] *Wyzwania w cyberprzestrzeni, przykłady rozwiązań, zagrożenia, regulacje*, Instytut Kościuszki, Kraków 2019.