Współczesne Problemy Zarządzania • Volume 8 • Number 1 (16) • 2020 • 67–81
DOI: https://doi.org/10.52934/wpz.85

Mariusz Rabka
Państwowa Wyższa Szkoła Techniczno-Ekonomiczna
im. ks. B. Markiewicza w Jarosławiu
mariusz.rabka@pwste.edu.pl https://orcid.org/0000-0001-6336-4870

Internet XXI wieku – pułapka zagrożeń dla dzieci, młodzieży i osób starszych w dobie pandemii Covid-19

Boję się dnia, w którym technologia przewyższy nasze ludzkie interakcje. Świat będzie miał wówczas generację idiotów.

Albert Einstein

Wstęp

Albert Einstein – wielki umysł, naukowiec i wizjoner żyjący na przełomie XIX i XX wieku – nie dożył czasów przełomu technologicznego w dziedzinie komputerów. Miał jednak świadomość zagrożeń, jakie niosą za sobą postęp techniczny i rozwój nowych technologii.

Maszyna ENIAC (Electronic Numerical Integrator And Computer, co można przetłumaczyć jako Elektroniczny, Numeryczny Integrator i Komputer) skonstruowana w latach 1943–1945 przez naukowców – J.P. Eckerta i J.W. Mauchly´ego – dała początek rozwoju nowej dziedzinie technologii, której przełom w powszechności i dostępności datuje się od 1982 roku debiutem komputera Commodore 64[1].

Dla pokolenia urodzonego po milenijnym 2000 roku trudne jest do zrozumienia, iż świat może istnieć bez Internetu. Laptop, smartfon i ciągła „obecność" w sieci potęguje tę świadomość, że Internet był zawsze. Jednak co niektórzy pamiętają ten charakterystyczny dźwięk połączenia za pośrednictwem modemu telefonicznego, prędkość, której w dzisiejszej dobie nikt z użytkowników nie zaakceptowałby, nie mówiąc już o portalach społecznościowych, których w owym czasie (połowa lat 90. XX wieku) po prostu nie było. Tak małymi krokami wkroczyliśmy w XXI wiek,

[1] https://www.benchmark.pl/aktualnosci/historia-rozwoju-komputerow-i-laptopow.html

w którym pojęcie społeczeństwa informacyjnego ze swoistymi cechami[2] zaczęło wypierać cechy społeczeństwa tradycyjnego. Takie wartości jak anonimowość, bezpieczeństwo, prawo do prywatności coraz częściej zaczęły ustępować takim pojęciom jak *social media, fallowers*, *trollowanie* czy też *lajk*. To co początkowo było fantazją i fabułą filmową w takich filmach jak Matrix czy Avatar, powoli stawało się naszą otaczającą rzeczywistością ze wszystkimi korzyściami, jak i niemałym bagażem zagrożeń. Przestrzeń definiowana jako nieskończony, nieokreślony obszar trójwymiarowy czy też określony, mający pewne wymiary obszar trójwymiarowy[3] traciła swoje znaczenie w zetknięciu z nową technologią informacyjno-komunikacyjną. Coraz częściej w to miejsce zaczęło pojawiać się pojęcie *cyberprzestrzeni*.

W tym kontekście istotnym jest umiejscowienie młodego pokolenia oraz osób w grupie wiekowej 65+ w cyfrowym świecie, jako istotnego elementu tego świata zwłaszcza w dobie pandemii Covid-19. Człowiek z natury rzeczy w zetknięciu z technologiami jest z jednej strony najbardziej wrażliwym elementem na wszelkiego rodzaju zagrożenia, będąc jednocześnie źródłem tych zagrożeń. Analiza regularności korzystania z Internetu w latach 2003–2020 w różnych grupach wiekowych w zestawieniu z danymi statystycznymi dotyczącymi zagrożeń związanych z cyberprzemocą i cyberprzestępczością pozwoli na wskazanie trendów i tendencji w tym obszarze oraz grup wiekowych najbardziej zagrożonych.

Cyberprzestrzeń – pojęcie i funkcje w społeczeństwie na przełomie XX i XXI wieku

Przedstawione przez Norberta Wienera jeszcze w 1948 r. pojęcie *cybernetyki* (ang. cybernetics) jako kontroli oraz komunikacji pomiędzy światem zwierząt oraz maszyn, z uwagi na rosnące znaczenie systemów teleinformatycznych wykorzystywanych obecnie przez społeczeństwa na całym świecie[4], ewoluowało przez dekady ubiegłego i obecnego wieku, wypracowując w tym obszarze różnorodność definicyjną.

Najczęściej w literaturze dotyczącej Internetu możemy spotkać się z pojęciem cyberprzestrzeni definiowanej jako: *przestrzeń wizualna, utworzona przez zgromadzone w Internecie zasoby lub jako iluzja wygenerowana przez specjalne oprogramowanie i sprzęt, takie jak: okulary, hełmy i okulary*[5]. Część specjalistów uważa, że cyberprzestrzeń narodziła się w momencie powstania politycznej koncepcji „autostrad informacyjnych", w czasie kampanii prezydenckiej Billa Clintona w 1992 roku[6].

W Polsce pojęcie cyberprzestrzeni pierwszy raz zostało zdefiniowane w założeniach do Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2009–2011, rozwinięte w kolejnym Rządowym Programie Ochrony Cyberprzestrzeni

[2] S. Wojciechowska-Filipek, Z. Ciekanowski, *Bezpieczeństwo funkcjonowania w cyberprzestrzeni, jednostki-organizacji-państwa*, Warszawa 2019, s. 14–15.

[3] B. Dunaj (red.), *Popularny słownik języka polskiego*, Warszawa 2001, s. 553.

[4] J. Wasilewski, *Przegląd Bezpieczeństwa Wewnętrznego*, 2013, nr 9, s. 227. https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa/987,Przeglad%20Bezpieczenstwa-Wewnetrznego-nr-9-5-2013.html

[5] A. Andrzejewska, J. Bednarek, *Zagrożenia cyberprzestrzeni i świata wirtualnego*, Warszawa 2014, s. 19.

[6] J. Kosiński, *Paradygmaty cyberprzestępczości*, Warszawa 2015, s. 32.

Rzeczypospolitej Polskiej na lata 2011–2016, opracowanym przez Ministerstwo Spraw Wewnętrznych i Administracji w czerwcu 2010 roku. Przedstawiona tam definicja uległa rozbudowaniu i za cyberprzestrzeń uznano „cyfrową przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami”[7].

Dynamiczny rozwój gospodarczy uzależniony od szybkiego i nieskrępowanego dostępu do informacji oraz jej wykorzystania w zarządzaniu, produkcji, sektorze usług oraz sektorze publicznym spowodował modyfikację podejścia do ochrony cyberprzestrzeni RP. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022 ustąpiła Uchwale nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024[8], w której ochrona systemów informacyjnych oraz przetwarzanych w nich informacji jest wyzwaniem dla wszystkich podmiotów tworzących krajowy system cyberbezpieczeństwa, a więc podmiotów gospodarczych świadczących usługi przy wykorzystaniu systemów informacyjnych, organów władzy publicznej, organów odpowiedzialnych za bezpieczeństwo narodowe, a także wyspecjalizowanych podmiotów zajmujących się cyberbezpieczeństwem w sferze operacyjnej.

Cyberprzestrzeń ze względu na zmienność swoich cech oraz dominującą rolę interaktywnych technologii, w której jest wykorzystana, kształtuje nowe oblicza współczesnej kultury i swoje miejsce w edukacji, wyróżniając się następującymi funkcjami:

- informacyjną – oznaczającą niemalże błyskawiczne dostarczenie różnorodnych informacji;
- ludyczną – dostarczającą rozrywki, której wartość jest uzależniona od jakości programów i sposobu ich odbioru;
- stymulującą – wyrażającą się w inspiracji odbiorców do aktywnego odbioru nadawanych treści;
- wzorcotwórczą – polegającą na programowaniu określonych stylów życia, ideałów, wzorców postępowania i zachowania;
- interpersonalną – wynikającą z wszechobecnej telewizji i komputerów łączących się z całym światem przez Internet[9].

Eksploatacja Internetu w Polsce w różnych grupach wiekowych przed i w czasie pandemii Covid-19

Dostrzegając pozytywy, jakie niosą za sobą nowe technologie na przestrzeni tych kilku dekad, możemy zaobserwować zmiany zachowań społecznych z różnych grup wiekowych. Trudno nie dostrzec, że pokolenie milenijne (urodzeni po 2000 roku – przyp. autora) nie ma problemu z akceptacją i intuicyjnym przyswajaniem nowinek technicznych, gdzie pokolenie 45+ w tym zakresie wykazuje swoiste cechy wykluczenia społecznego.

Chcąc opisać zjawisko wykluczenia społecznego, możemy stwierdzić, iż jest to:

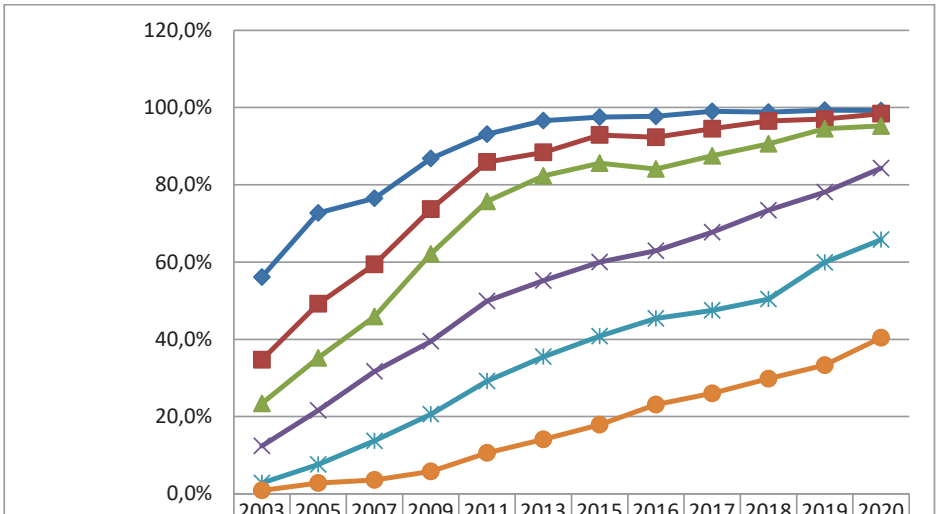
- niezdolność do uczestnictwa w uznawanych za ważne aspektach życia społecznego – gospodarczych, politycznych i kulturowych;

[7] Ibidem, s. 33.
[8] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf (dostęp: 11.01.2021).
[9] A. Andrzejewska, J. Bednarek, *Zagrożenia cyberprzestrzeni i świata wirtualnego*, Warszawa 2014, s. 20.

- odmowa podstawowych praw socjalnych, zapewniających obywatelom pozytywną wolność od uczestnictwa w życiu społecznym i ekonomicznym i przez to nadających znaczenie ich podstawowym wolnościom negatywnym;
- proces erozji uznania i szacunku dla praw obywatelskich, od których zależą środki do życia i jego poziom[10].

Jednak w dzisiejszej dobie informatyzacji nieuniknionym jest korzystanie z Internetu przez wszystkie grupy wiekowe społeczeństwa, chociażby w tak prozaicznych sytuacjach jak wykorzystanie darmowych komunikatorów internetowych lub aplikacji do wideokonferencji czy też przeglądanie portali z wiadomościami.

Proces ten zobrazuje poniższe zestawienie zmian korzystania z Internetu w grupach społeczno-demograficznych w latach 2003–2020.



	2003 r.	2005 r.	2007 r.	2009 r.	2011 r.	2013 r.	2015 r.	2016 r.	2017 r.	2018 r.	2019 r.	2020 r.
16 - 24 lat	56,1%	72,7%	76,5%	86,8%	93,1%	96,6%	97,5%	97,7%	99,0%	98,8%	99,3%	99,2%
25 - 34 lat	34,7%	49,2%	59,4%	73,7%	85,9%	88,4%	92,9%	92,3%	94,5%	96,5%	97,0%	98,4%
35 - 44 lat	23,4%	35,2%	45,9%	62,1%	75,7%	82,3%	85,6%	84,1%	87,5%	90,6%	94,5%	95,2%
45 - 59 lat	12,4%	21,6%	31,7%	39,5%	49,9%	55,2%	60,0%	62,9%	67,7%	73,4%	78,1%	84,3%
60 - 64 lat	2,8%	7,6%	13,7%	20,6%	29,2%	35,5%	40,8%	45,4%	47,5%	50,4%	59,9%	65,8%
65 i więcej lat	0,9%	2,8%	3,6%	5,8%	10,6%	14,1%	17,9%	23,1%	26,0%	29,8%	33,3%	40,4%

Wykres 1. Procentowe zestawienie liczby osób regularnie korzystających z Internetu w poszczególnych grupach wiekowych w latach 2003–2020

Źródło: Diagnoza Społeczna 2015[11] i Dane GUS[12]; opracowanie własne.

[10] Ibidem, s. 39.

[11] J. Czapiński, T. Panek (red.), *Diagnoza Społeczna*, 2015. www.diagnoza.com (dostęp:18.01.2021).

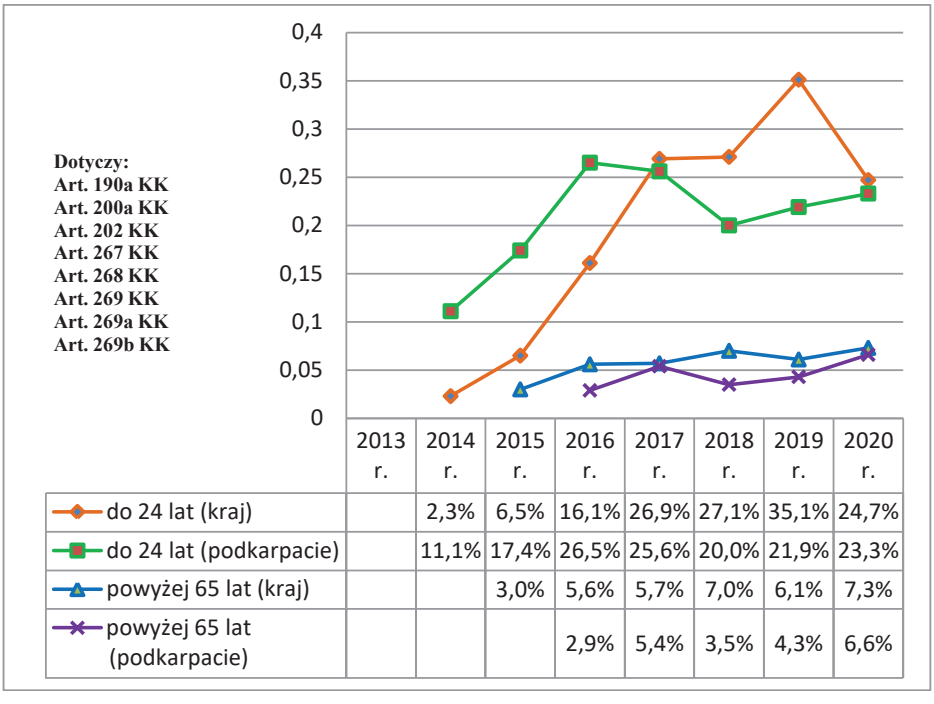
[12] E. Kacperczyk, B. Rzymek (red.), *Społeczeństwo informacyjne w Polsce. Wyniki badań z lat 2013–2017*, Warszawa–Szczecin 2017. https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/ (dostęp: 23.03.2021) oraz E. Kacperczyk, B. Rzymek (red.), *Społeczeństwo*

Gdyby przyjąć, kto w poszczególnych grupach wiekowych w latach 2003 do 2020 zanotował największy progres w korzystaniu z Internetu, to niewątpliwie seniorzy w wieku 65+ należą do tych, którzy odnotowali ponad czterdziestokrotny przyrost; z 0,9 procent korzystających osób w wieku 65+ w 2003 roku do 40,4 procent korzystających z Internetu w 2020 roku. Znamienne jest, że im młodsze pokolenie, tym przyrost procentowy korzystających z Internetu w analogicznym okresie nie był już tak dynamiczny. Wpływ na to miało niewątpliwie większe „*obycie*" młodego pokolenia z tą technologią. Przy grupie wiekowej 16–24 lat w latach 2003 do 2015 ilość użytkowników Internetu prawie podwoiła się, osiągając wysoki wynik 97,5 procenta, który to wynik do 2020 roku zmieniał się nieznacznie, ale i tak osiągając bardzo wysoki pułap 99,2 procent młodych ludzi, w tej grupie wiekowej, systematycznie korzystających z Internetu. Zestawienie to pokazuje, jak dostępność i korzystanie z Internetu rok rocznie wzrasta i w związku z tym, jak w różnym stopniu i o różnym charakterze niesie zagrożenia dla poszczególnych grup wiekowych. Niezależnie od wnikliwości i przyjętych zakresów analiz, dostępność i wykorzystanie technologii informacyjno-komunikacyjnej w drugiej dekadzie XXI wieku systematycznie rośnie w całej populacji Polski, a tym samym rosną też potencjalne zagrożenia z tym związane.

Zagrożenia te mogą przybierać postać cyberprzemocy, której niektóre formy niekiedy trudno kwalifikować z karno-prawnego punktu, a ich skalę możemy obserwować jedynie przez pryzmat badań naukowych. Inaczej sprawa wygląda przy cyberprzestępczości. Przez pryzmat statystyk policyjnych jest łatwiejsza do zdefiniowania, a pomijając „ciemną liczbę" przestępczości popełnianej w cyberprzestrzeni, możliwa jest pełniejsza analiza w wybranym zakresie.

Przedstawienie zgromadzonych danych statystycznych dotyczących osób pokrzywdzonych wybranych grup wiekowych w ogólnej liczbie pokrzywdzonych w wybranych kategoriach przestępstw w Polsce w latach 2013–2020 pozwoli, w zestawieniu z procentową liczbą regularnych użytkowników Internetu, na ocenę skali oraz tendencji w tym obszarze.

informacyjne w Polsce w 2020 r., Warszawa–Szczecin 2020. https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/ (dostęp: 23.03.2021).



	2013 r.	2014 r.	2015 r.	2016 r.	2017 r.	2018 r.	2019 r.	2020 r.
do 24 lat (kraj)		2,3%	6,5%	16,1%	26,9%	27,1%	35,1%	24,7%
do 24 lat (podkarpacie)		11,1%	17,4%	26,5%	25,6%	20,0%	21,9%	23,3%
powyżej 65 lat (kraj)			3,0%	5,6%	5,7%	7,0%	6,1%	7,3%
powyżej 65 lat (podkarpacie)				2,9%	5,4%	3,5%	4,3%	6,6%

Wykres 2. Procentowy udział osób pokrzywdzonych wybranych grup wiekowych w ogólnej liczbie pokrzywdzonych w wybranych kategoriach przestępstw w Polsce w latach 2013–2020

Źródło: Dane KSIP; opracowanie własne.

Trendy wzrostowe ilości osób pokrzywdzonych w poszczególnych grupach wiekowych, pokrywające się ze wzrostem ilości użytkowników regularnie korzystających z Internetu w kolejnych latach, osiągnęły w dobie pandemii Covid-19 najwyższe wartości. Zauważalny w kraju w grupie wiekowej do 24 lat spadek ilości osób pokrzywdzonych o ponad 10 procent w stosunku do wcześniejszych lat, może nasuwać konkluzję, że umiejętności wynikające z częstego korzystania i obycie się z Internetem wpływają na unikanie zagrożeń czyhających w sieci.

Pandemia Covid-19 – determinant zmian w korzystaniu z sieci i zagrożeń w XXI wieku

Internet sam w sobie, jak każde narzędzie, z natury nie stwarza żadnych zagrożeń. Możemy przytoczyć wiele przedmiotów, których cechy użytkowe nie przywołują na myśl żadnych niebezpieczeństw, a dopiero w rękach nieodpowiedzialnego człowieka stają się niebezpiecznym narzędziem, mogącym spowodować znaczny uszczerbek na zdrowiu czy nawet spowodować śmierć. Komu przyszłoby na myśl, że takie rzeczy codziennego użytku jak but czy szalik, w niektórych okolicznościach mogą stać się niebezpiecznymi przedmiotami.

Zauważone zostało to w orzecznictwie sądowym. Między innymi w uzasadnieniu prawnym wyroku Sądu Apelacyjnego w Poznaniu z 2005 roku, w oparciu o orzecznictwo Sądu Najwyższego (por. wyrok SN z dnia 30 grudnia 1971 r. I KR 181/71, OSNPG 1972, z. 5, poz. 90; wyrok SN z dnia 21 stycznia 1987 r. V KRN 460/86, OSNPG 1987, z. 8, poz. 104; wyrok SN z dnia 13 września 1971 r., III KR 102/71, LEX nr 21421; wyrok SN z dnia 22 sierpnia 1986 r., III KR 242/86, LEX nr 22036) przywołano, że ów potencjał niebezpieczeństwa narzędzia wynika nie tylko z jego właściwości, lecz także ze sposobu jego użycia. W konsekwencji takiego stanowiska, opartego na dwóch kryteriach niebezpieczeństwa narzędzia, w orzecznictwie za niebezpieczne uznawane były nie tylko takie przedmioty, jak siekiera, nóż czy żelazny łom, lecz także drewniana pałka, garnek metalowy, ciężki but żołnierski, szalik czy wreszcie butelka[13].

Ten fenomen dotyka również Internetu; w rękach nieodpowiedzialnych ludzi staje się niebezpiecznym narzędziem, wyrządzającym szkodę w mieniu czy w sferze relacji międzyludzkich, a niejednokrotnie doprowadzając do tragedii ludzkich.

Internet złych rzeczy istnieje wszędzie; ani Tor, ani VPN, ani anonimowość nie są potrzebne, aby robić złe rzeczy w sieci. Portale społecznościowe, chmury, serwisy i fora – wszystko to, do czego mamy dostęp z domu, z własnego komputera jest wystarczającym narzędziem do zrobienia lub doznania krzywdy[14].

Jedną z pułapek Internetu jest jego uzależniające działanie. Ile razy w swoim otoczeniu widzieliśmy sytuacje, gdzie grupy młodych ludzi, rodziny przy obiedzie w restauracji czy czekający na przystanku autobusowym pasażerowie „zatopieni" byli w ekrany swoich smartfonów? Na pewno wiele razy. Czy ze względu na ich charakterystyczne sylwetki, pochylone nad smartfonami, nie przychodzi na myśl skojarzenie, aby nazwać ich „pokoleniem zgiętych karków"? Na pewno tak.

W kontekście społecznym nie są to jednak odosobnione sytuacje, a wręcz nabierają w dzisiejszej dobie charakteru dysfunkcji związanych z nadmiarem korzystania z technologii informacyjnych przybierających formę uzależnień jako:

- syndrom IDA (Internet Addiction Disorder) – nabycie wewnętrznego przymusu bycia w sieci, co w efekcie powoduje, że Internet staje się czymś koniecznym do życia oraz funkcjonowania – infoholizm;
- syndrom ASC (Alcohol Stupor Condition) powodowany intensywnym korzystaniem z komputera, prowadzący do stanów świadomości podobnych fizjologicznie i psychologicznie do upojenia alkoholowego lub narkotycznego[15].

Niewątpliwie sytuacja pandemii, która dotknęła w 2020 roku świat i nasz kraj, pogłębiła to negatywne zjawisko.

Przez blisko sto lat, od pandemii wywołanej wirusem grypy nazywanej *grypą hiszpanką,* ludzie nie przypuszczali, że podobna i równie tragiczna sytuacja może się

[13] Wyrok Sądu Apelacyjnego w Poznaniu z dnia 6 września 2005 roku II AKa 170/05; https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/ii-aka-170-05-ocena-niebezpiecznosci-przedmiotu-uzytego-520265635 (dostęp: 20.01.2021).

[14] J. Chmielecka, *Internet złych rzeczy*, Bielsko-Biała 2017, s. 307.

[15] A. Andrzejewska, J. Bednarek, *Zagrożenia cyberprzestrzeni i świata wirtualnego*, Warszawa 2014, s. 41.

powtórzyć. Rozwój medycyny, postęp w dziedzinie różnych technologii, skok cywilizacyjny XXI wieku dawał złudne poczucie, że jako ludzie jesteśmy w stanie kontrolować otaczający świat i zapewniać sobie bezpieczeństwo. Jeszcze przełom 2019/2020 roku nie zapowiadał tak tragicznego rozwoju sytuacji, której początek dały pierwsze sygnały z listopada 2019 roku z Chin, z prowincji Wuhan, o zakażeniach nieznanym jeszcze wówczas szczepem wirusa grypy SARS-CoV-2 i zachorowaniami oraz zgonami na chorobę COVID-19.

Kolejne stwierdzane przypadki zachorowań na COVID-19 w Europie i na świecie spowodowały, że Światowa Organizacja Zdrowia (WHO, *przyp. autora)* 30 stycznia 2020 roku ogłosiła stan zagrożenia dla zdrowia publicznego o zasięgu międzynarodowym w wyniku rozprzestrzeniającej się epidemii COVID-19, a 11 marca 2020 roku uznając serię zachorowań na COVID-19 za pandemię.

W Polsce od 3 marca 2020 roku zaczęła obowiązywać Ustawa o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych[16], a dzień później minister zdrowia ogłosił zdiagnozowany pierwszy przypadek zachorowania na COVID-19, 66-latka z Cybinic w woj. lubuskim.

Nikt wówczas nie przypuszczał, jakie nastąpią ograniczenia oraz zmiany w życiu społecznym i w relacjach międzyludzkich w związku z sytuacją pandemiczną. O ograniczeniach, jakie zaszły i nadal trwają niech świadczą 43 (czterdzieści trzy) Rozporządzenia[17] wydane w tym zakresie przez Radę Ministrów do 4 stycznia 2021 roku. Relacje międzyludzkie w znacznej mierze zostały ograniczone; ograniczona została możliwość spotykania się. Działalność gospodarcza w kraju (i na świecie) praktycznie zahamowała, a w oświacie i szkolnictwie wyższym nastąpiło przejście do nauczania na odległość w formie on-line.

Pojawiło się pojęcie pracy zdalnej[18], która mogła przybierać formy pracy hybrydowej, polegającej na realizacji swoich obowiązków pracowniczych częściowo w siedzibie firmy (uczelni, szkoły itp.), a częściowo w formie zdalnej, czyli on-line. Zauważalnym stało się powszechniejsze niż wcześniej dokonywanie zakupów „w sieci". Wizyty, spotkania czy spędzanie wspólnie rodzinnych świąt przeniosły się do cyberprzestrzeni. Świat wirtualny zaczął żyć nowym życiem, w którym mocniej niż kiedykolwiek zaczął „żyć" człowiek.

W tym świecie, dzieci i młodzież urodzona po 1980 roku, zaliczane do: e-generacji, Generacji Y, Millenium Kids, Millenium Generation, Net Generation,

[16] Ustawa z dnia 2 marca 2020 r. *o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych* (Dz. U. 2020, poz. 374 ze zm.).

[17] Liczba rozporządzeń na podstawie udostępnienia na stronie Śląskiego Urzędu Wojewódzkiego w Katowicach – https://www.katowice.uw.gov.pl/aktualnosci/akty-prawne-i-dokumenty-dotyczace-zapobiegania-przeciwdzialania-i-zwalczania-covid-19 (dostęp: 21.01.2021).

[18] Art. 3. 1. W okresie obowiązywania stanu zagrożenia epidemicznego albo stanu epidemii, ogłoszonego z powodu COVID-19, oraz w okresie 3 miesięcy po ich odwołaniu, w celu przeciwdziałania COVID-19 pracodawca może polecić pracownikowi wykonywanie, przez czas oznaczony, pracy określonej w umowie o pracę, poza miejscem jej stałego wykonywania (praca zdalna).

Gen Netters czy też Generacja Digital Natives (Cyfrowych tubylców), niewątpliwie dystansując w możliwościach i częstotliwości korzystania z cyberprzestrzeni generację Cyfrowych imigrantów (Generacja Digital Immigrants)[19], stała się dla nich przewodnikiem „życiowym". To wnuczek stawał się nauczycielem i wprowadzającym w nowy świat swoich dziadków, zakładając Facebook, WhatsApp czy inny komunikator, bądź pomagając przy założeniu konta e-Pacjent lub zakupach w sklepie internetowym.

Po 3 marca 2020 roku w Polsce relacje międzyludzkie zostały sprowadzone do komunikacji w świecie wirtualnym. Komunikacja, która ma postać werbalny i niewerbalny, w wymiarze cyberprzestrzeni została pozbawiona ważnego – niewerbalnego – elementu. To co mogliśmy wyczytać z mowy ciała, zostało „ukryte" za monitorem komputera, laptopa czy smartfona. Anonimowość, a co za tym idzie możliwość ukrywania tożsamości, z jednej strony dodała niektórym użytkownikom pewności w relacjach interpersonalnych, a z drugiej stały się dla niektórych doskonałą „okazją", jak dla kieszonkowca pozostawiony na ladzie sklepowej portfel, do czynienia zła lub wejścia na drogę przestępstwa.

Internet stał się swoistą pułapką, która w zawoalowany sposób nęci korzyściami i pięknem bycia w tym świecie, a tak faktycznie będąc tonią najeżoną rafami koralowymi i wirami, czyhającymi na nieostrożnych podróżników, aby wciągnąć w głębię, sponiewierać, wyrzucić na brzeg z bagażem traumy, a w najgorszym razie doprowadzić do tragedii.

Cyberbezpieczeństwo, rozumiane jako *odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy*[20] stało się więc priorytetem i wyzwaniem dla władz krajowych i międzynarodowych. Zwiększenie zdolności do zwalczania cyberprzestępczości zostało ujęte w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 jako jeden z celów szczegółowych[21].

Cyberprzestępczość nie jest jedynym zagrożeniem w sieci. Biorąc pod uwagę interdyscyplinarny charakter zagrożeń bezpieczeństwa, możemy przyjąć podział na[22]:

1. zagrożenia ogólne:
   a. niewłaściwe wykorzystanie zasobów,
   b. kradzież zasobów,
   c. ujawnienie informacji osobom nieupoważnionym,
   d. podsłuchiwanie,
   e. projektowanie wadliwej infrastruktury informacyjnej;
2. zagrożenia wynikające z aspektów psychologicznych:
   a. błędy i pomyłki ludzkie,
   b. nieuczciwi pracownicy,

[19] M. Górka, *Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa*, Warszawa 2017, s. 134–136.

[20] Art. 2 pkt 4 ustawy z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* (Dz. U. 2018, poz. 1560).

[21] Monitor Polski z 30.10.2019 r. poz. 1037.

[22] K. Wojtaszek, A. Materska-Sosnowska, *Bezpieczeństwo państwa*, Warszawa 2009, s. 196–197.

c. celowe działania nieuczciwych pracowników,
d. działania intruzów komputerowych;
3. zagrożenia środowiskowe i kryminalne:
a. przestępczość – włamania, wymuszenia, napady itp.,
b. kataklizmy – woda, ogień,
c. terroryzm;
4. zagrożenia wynikające z nieuczciwej konkurencji:
a. opinie branży,
b. wywiadownie gospodarcze,
c. weryfikacja dokumentów.

Człowiek z tymi wszystkimi zagrożeniami staje się częścią e-świata; przestrzeni, w której wirtualny wymiar miesza się z rzeczywistością, którego jednak skutki oddziaływania jak najbardziej stają się realne. Staje się tak, gdyż instytucje publiczne, podmioty gospodarcze i wszelkie organizacje coraz częściej wykorzystują nowe możliwości technologii informacyjno-komunikacyjnych, oferując produkty i usługi dla obywateli on-line.

Terminologia w tym zakresie wytworzyła swoistą typologię, adekwatną do dziedzin działalności, usług itp., posługując się pojęciem:

- e - administracja,
- e - biznes,
- e - handel,
- e - bankowość,
- e - zdrowie,
- e - edukacja[23].

Człowiek „wchodząc" w tym e-świecie w interakcję, nie zawsze uświadamia sobie, że właśnie stał się ofiarą. Niezmiennie od kilku lat na liście zagrożeń w tym zakresie jest phishing.

Phishing (z ang. *password harvesting fishing,* czyli „łowienie haseł") jest rodzajem oszukańczego pozyskiwania poufnych informacji osobistych, takich jak: loginy, hasła, szczegóły karty kredytowej czy konta bankowego, poprzez podszywanie się pod osobę (instytucję) godną zaufania, której te informacje są pilnie potrzebne lub niezbędne do normalnego funkcjonowania[24]. Pandemia pokazała, że izolacja i częstsze korzystanie z Internetu spowodowało znaczny wzrost tego typu zachowań. Alarmujące są dane uzyskane przez ekspertów NASK[25] wskazujące, że w pierwszym kwartale 2020 roku odnotowano 1 752 przypadki ataków typu phishing, co stanowiło niemal połowę wszystkich ataków phishingowych zarejestrowanym w całym 2019 roku[26].

[23] S. Wojciechowska-Filipek, Z. Ciekanowski, *Bezpieczeństwo funkcjonowania w cyberprzestrzeni, jednostki-organizacji-państwa*, Warszawa 2019, s. 102–137.

[24] J. Kosiński, *Paradygmaty cyberprzestępczości*, Warszawa 2015, s. 126.

[25] Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy z siedzibą w Warszawie, ul. Kolska 12, nadzorowany przez Kancelarię Prezesa Rady Ministrów, z Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego działającym na poziomie krajowym.

[26] https://www.nask.pl/pl/aktualnosci/3835,Dane-CERT-Polska-za-pierwszy-kwartal-2020roku-pokazuja-ze-w-okresie-pandemii-li.html (dostęp: 22.01.2021).

Wprowadzenie w pierwszym kwartale 2020 roku nauki i studiowania do wirtualnej przestrzeni w formie on-line, przy jednoczesnym wprowadzeniu ograniczeń w poruszaniu się, spotęgowało wśród dzieci i młodzieży poczucie izolacji i frustracji. Czas ten pokazał, że szkoła (studia) niejednokrotnie do tej pory krytykowana i często niedoceniana przez uczniów (studentów), zaczęła być miejscem, do którego chętnie każdy chciał wrócić. Izolacja i frustracja stały się czynnikami, które w znacznej mierze negatywnie odbiły się na zachowaniach w sieci. Nieodosobnione były przypadki zakłócania prowadzonej lekcji, prezentowania niestosownych treści lub innych zachowań cyberprzemocy, jako formy agresji i przemocy rówieśniczej, wyrażanej w formie ubliżania, grożenia, straszenia czy nękania.

Wiele negatywnych zachowań, które w „realnym" świecie byłyby zauważalne, w cyberprzestrzeni przestają być tak wyraźne, a przynajmniej dla najbliższych; rodziców, rodzeństwa, przyjaciół.

Pojęcie „galerianki" – młodej dziewczyny, która szuka sponsora najczęściej w galeriach handlowych – używane jeszcze do niedawna, powoli odchodzi do lamusa. „Galerianki" były jednak widoczne i to dosłownie. Ten sam typ zachowań przeniesionych do Internetu jako nowe zjawisko, jakim jest sponsoring, z natury rzeczy nie jest już tak zauważalny, przynajmniej w początkowej fazie.

Można przyjąć, że sponsoring jest pewną płaszczyzną interakcji seksualnych pomiędzy prostytucją a akceptowanym w dzisiejszych czasach posiadaniem stałego, dobrze sytuowanego kochanka, oparta na bliskości, a nawet zażyłości, trwająca nawet wiele lat, gdzie korzyści są obustronne. Istotnym faktem jest, że z punktu widzenia moralności oceniane jest to bardzo często jako pewna forma pracy, a nie coś złego[27]. Stąd też aspekt oceny i opinii otoczenia, jak również innych czynników, nie bez znaczenia ma wpływ na zachowanie osoby, niejednokrotnie w bardzo młodym wieku, wchodzącej na drogę sponsoringu. Czynnikami wpływającymi na podjęcie decyzji o zaoferowaniu usług w formie sponsoringu będzie między innymi chęć poprawy statusu materialnego i dorównanie w tym zakresie grupie rówieśniczej, ciekawość nowych przeżyć, rodzinne patologie (alkoholizm, narkomania itp.) czy zaimponowanie innym. Młody wiek, a tym samym słaba zdolność przewidywania i małe doświadczenie życiowe, powodują, że skutki takiego zachowania mogą doprowadzić do nieszczęścia. Nie wiedząc, kim jest osoba po drugiej stronie komputera, wchodzący na drogę sponsoringu może spotkać kogoś z zaburzeniami psychicznymi lub dewiacyjnymi, a spotkanie w „realu" może mieć tragiczne skutki.

Internet jest także wykorzystywany do wyszukiwania małoletnich ofiar oraz propagowania i pochwalania zachowań pedofilskich. Można tutaj wyróżnić dwa sposoby działania przestępców: bezpośredni i ostrożny[28]. Sprawcy chilg-groomingu, czyli uwodzenia i nagabywania dzieci z wykorzystaniem systemów teleinformatycznych lub technologii informacyjnych, zachęcają dziecko do udziału w czynnościach seksualnych, dyskutując na temat intymnych zachowań, prezentując treści

[27] A. Andrzejewska, *Dzieci i młodzież w sieci zagrożeń realnych i wirtualnych. Aspekty teoretyczne i empiryczne*, Warszawa 2014, s. 170.

[28] J. Kosiński, *Paradygmaty cyberprzestępczości*…, op. cit., s. 168.

o charakterze pornograficznym w celu doprowadzenia do fizycznego spotkania i seksualnego wykorzystania dziecka.

Podsumowanie

Niewątpliwie zagadnienie wielości zagrożeń w sieci, przez obszerność i stały rozwój technologii komunikacyjno-informacyjnych, będzie sukcesywnie dostarczało nowych pojęć i będziemy obserwować nowe zjawiska.

Pandemia, która dotknęła cały świat w 2020 roku pokazała, jak ważnym elementem są bezpośrednie relacje międzyludzkie, które dostarczają doznań werbalnych i niewerbalnych, a które kształtują właściwe oceny i relacje.

Czas pandemii obnażył zagrożenia w cyberprzestrzeni, wśród których wymienia się:

- dostęp do nieodpowiednich treści;
- niebezpieczeństwo chorób układu wzrokowego, mięśniowo-szkieletowego;
- niebezpieczeństwo chorób psychicznych;
- uzależnienia;
- specyficzne zachowania związane z realizowaniem różnych form przemocy i agresji w świecie wirtualnym;
- zmiany o charakterze społecznym;
- seksting;
- zanik samodzielnego myślenia i pogłębionej refleksji;
- i inne[29], których zwalczanie jest powinnością państwa, za pośrednictwem właściwych służb i instytucji.

Rok 2020 wyraźnie zaznaczył się we wzroście ilości użytkowników Internetu, poczynając od 16-latków, a kończąc na seniorach 65+. Ten swoisty popyt nie bez odzewu pozostał w sferze cyberprzemocy oraz działalności cyberprzestępców. Płynące stąd zagrożenia, w różnym stopniu dla seniorów oraz młodego pokolenia, są wynikiem systematycznie rosnącego trendu wykorzystywania cyberprzestrzeni przez tych, dla których wartości moralne i prawne nic nie znaczą. W tej walce przegrywają ci, którzy są mniej „obyci" z nowinkami technologii informatyczno-komunikacyjnych. Sukcesywny wzrost liczby seniorów stających się ofiarami cyberprzestępców, plasuje osoby 65+ w grupie ryzyka zagrożeniami płynącymi z Internetu.

Jednak społeczeństwo obywatelskie nie powinno pozostawać w tym zakresie bierne. Od społecznej aktywności, zaangażowania, a przede wszystkim dostrzeżenia pułapek, jakie zastawia Internet na jego użytkowników, zależy sukces w walce z cyberprzemocą i zagrożeniami w sieci. Ponadto zwiększenie kampanii medialnych oraz zaangażowanie służb i instytucji winno być priorytetem, aby uchronić osoby starsze z jednej strony przed wykluczeniem społecznym, a z drugiej przed zagrożeniami w cyberprzestrzeni.

Bardzo wymowna wypowiedź Billa Gates´a, że „internet jest jak przypływ. Zaleje przemysł komputerowy i wiele innych, zatapiając tych, którzy nie nauczą się

[29] A. Andrzejewska, J. Bednarek, *Zagrożenia cyberprzestrzeni*…, op. cit., s. 87.

w nim pływać", winna być ostrzeżeniem, ale też refleksją, aby nie dać się „zatopić". Jedyna droga, aby tego uniknąć to nauka, mądre korzystanie z Internetu i pomoc seniorom w zrozumieniu tej technologii.

Abstrakt

Internet XXI wieku – pułapka zagrożeń dla dzieci, młodzieży i osób starszych w dobie pandemii Covid-19

Technologie informacyjno-komunikacyjne na przełomie XX i XXI wieku przechodziły ewolucję, której zastosowanie w warunkach ekstremalnej eksploracji, jako podstawowe medium komunikacji międzyludzkiej, można było obserwować po wybuchu pandemii Covid-19 w 2020 roku. Wymuszona izolacja, jako element walki z pandemią, przeniosła życie społeczno-gospodarcze w cyberprzestrzeń. Korzystanie z Internetu w wielu aspektach stało się koniecznością, a funkcje cyberprzestrzeni nabrały nowego wymiaru i znaczenia w relacjach interpersonalnych. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej stała się kluczowym instrumentem dla wyspecjalizowanych podmiotów zajmujących się cyberbezpieczeństwem w identyfikowaniu i zwalczaniu zagrożeń w sieci. Zmieniające się na przestrzeni lat regularne korzystanie z Internetu w różnych grupach wiekowych osiągnęło najwyższy poziom w 2020 roku. Korzystający tak chętnie z technologii komunikacyjno-informacyjnych małoletni, ale też, z bardzo dużym progresem eksplorowania Internetu, seniorzy 65+, stali się grupami najbardziej narażonymi na pułapki i zagrożenia płynące z Internetu. Przez pryzmat zmian w korzystaniu z sieci w dobie pandemii Covid-19, wynikających z prawodawczej działalności polskiego rządu, ukazano w opracowaniu spektrum wybranych zagrożeń, na które narażone były w różnym stopniu zarówno osoby młode, jak i seniorzy. Procentowa analiza liczby osób regularnie korzystających z Internetu w poszczególnych grupach wiekowych w latach 2003 do 2020 w zestawieniu z zagrożeniami w cyberprzestrzeni, pozwoliło na wyciągnięcie wniosków co do skali i trendów zagrożeń w cyberprzestrzeni, będących wynikiem pandemii Covid-19.

Słowa kluczowe: cyberprzestrzeń, cyberbezpieczeństwo, cyberprzestępstwo, chilg-groomingu, cyfrowy imigrant, cyfrowy tubylca, pandemia, phishing, sponsoring, uzależnienie od technologii informacyjnych, wykluczenie społeczne

Abstract

Internet of the 21st century – a trap of threats for children, youth and the elderly in the time of the Covid-19 pandemic

Information and communication technologies at the turn of the 20th and 21st centuries underwent an evolution, the use of which in the conditions of extreme exploration, as the basic medium of interpersonal communication, could be observed after the outbreak of the Covid-19 pandemic in 2020. Forced isolation, as part of the fight

against the pandemic, moved socio-economic life into cyberspace. Using the Internet in many aspects has become a necessity, and the functions of cyberspace have acquired a new dimension and importance in interpersonal relations. The Cybersecurity Strategy of the Republic of Poland has become a key instrument for specialized entities dealing with cybersecurity in identifying and combating online threats. Regular use of the Internet in different age groups, which has changed over the years, reached its highest level in 2020. Minors who are so eager to use communication and information technologies, but also with a very large progress in exploring the Internet, seniors 65+ have become the groups most exposed to the traps and threats of the Internet. Through the prism of changes in the use of the Internet during the Covid-19 pandemic, resulting from the legislative activity of the Polish government, the study presents a spectrum of selected threats to which both young people and seniors were exposed to a varying degree. Percentage analysis of the number of people regularly using the Internet in individual age groups in the years 2003–2020 in comparison with treats in cyberspace, allowed to draw conclusions about the scale and trends of threats in cyberspace resulting from the Covid-19 pandemic.

Keywords: cyberspace, cybersecurity, cybercrime, chilg-grooming, digital immigrant, digital native, pandemic, phishing, sponsorship, information technology addiction, social exclusion

References

1. Adamski A., *Cyberprzestępczość – aspekty prawne i kryminologiczne*, Studia Prawnicze, 2005, nr 4.
2. Andrzejewska A., Bednarek J., *Zagrożenia cyberprzestrzeni i świata wirtualnego*, Warszawa 2014.
3. Andrzejewska A., *Dzieci i młodzież w sieci zagrożeń realnych i wirtualnych. Aspekty teoretyczne i empiryczne*, Warszawa 2014.
4. Chmielecka J., *Internet złych rzeczy*, Bielsko-Biała 2017.
5. Dąbrówka A., Geller E., Turczyn R., *Słownik synonimów*, Warszawa 1995.
6. Dunaj B. (red.), *Popularny słownik języka polskiego*, Warszawa 2001.
7. Górka M., *Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa*, Warszawa 2017.
8. https://isap.sejm.gov.pl
9. https://www.katowice.uw.gov.pl/aktualnosci/akty-prawne-i-dokumenty-dotyczace-zapobiegania-przeciwdzialania-i-zwalczania-covid-19
10. https://www.nask.pl
11. Kosiński J., *Cyberprzestępczość – przegląd wybranych szkoleń*, Przegląd Policyjny, 2004, nr 3.
12. Kosiński J., *Paradygmaty cyberprzestępczości*, Warszawa 2015.

13. Ratajczak M., *Czynności pedofilskie – ujęcie prawne i kryminologiczne*, Prokuratura i Prawo, 2014, nr 2.
14. Snopkiewicz K., *Cyberbezpieczeństwo w polskich realiach*, [w:] *Cyberbezpieczeństwo w polskich realiach*, G. Skrobotowicz (red.), Wydawnictwo Naukowe TYGIEL, Lublin 2019.
15. Wasilewski J., *Przegląd Bezpieczeństwa Wewnętrznego*, 2013, nr 9. https://www.abw.gov.pl/pl/pbw/publikacje/przeglad%20bezpieczenstwa/987,Przeglad-Bezpieczenstwa-Wewnetrznego-nr-9-5-2013.html
16. Wojciechowska-Filipek S., Ciekanowski Z., *Bezpieczeństwo funkcjonowania w cyberprzestrzeni, jednostki-organizacji-państwa*, Warszawa 2019.
17. Wojtaszek K., Materska-Sosnowska A., *Bezpieczeństwo państwa*, Warszawa 2009.