Teka of Political Science and International Relations – OL PAN/UMCS, 2018, 13/2, 77–96

DOI: 10.17951/teka.2018.13.2.77-96

ZAGROŻENIA BEZPIECZEŃSTWA SPOŁECZNEGO ZWIĄZANE Z FUNKCJONOWANIEM W CYBERPRZESTRZENI

Liliana Węgrzyn-Odzioba

Wydział Politologii
Uniwersytet Marii Curie-Skłodowskiej w Lublinie
ORCID ID: https://orcid.org/0000-0002-3897-8843
e-mail: liliana.wegrzyn-odzioba@poczta.umcs.lublin.pl

Streszczenie: W artykule podjęto próbę uchwycenia podstawowych elementów związanych z zagrożeniami dla bezpieczeństwa społecznego w cyberprzestrzeni. Zwrócono uwagę na różne kategorie krzyżujących się tematów obejmujących zagrożenia natury zdrowotnej, prawnej, moralnej i wychowawczej. Tematyka bezpieczeństwa społecznego w cyberprzestrzeni jest obszarem trudnym badawczo, ponieważ szybkość i pogłębiająca się penetracja przez rzeczywistość wirtualną powoduje nakładanie się różnych elementów na siebie. Zagrożenia bezpieczeństwa społecznego związane z funkcjonowaniem w cyberprzestrzeni to temat dla autorów zajmujących się tą problematyką, jak również praktyków różnych dziedzin, przed którymi stoi wyzwanie przewidzenia i prewencji potencjalnie niebezpiecznych zjawisk.

Słowa kluczowe: cyberprzestrzeń, cyberbezpieczeństwo, internet, bezpieczeństwo społeczne, zagrożenia fizyczne, zagrożenia psychiczne

WPROWADZENIE

„Cywilizacja, którą zbudujemy, zbliżając się do XXI wieku, nie będzie cywilizacją materialną, symbolizowaną przez ogromne konstrukcje, ale będzie faktycznie cywilizacją niewidoczną. Precyzyjnie powinno się ją nazwać cywilizacją informacyjną. Homo sapiens, który pod koniec ostatniej epoki lodowcowej stanął przed początkiem pierwszej – materialnej cywilizacji, stoi dziś po dziesięciu tysiącach lat na progu drugiej – cywilizacji informacyjnej" – takie słowa Yoneji Masudy – socjologa i informatyka, wizjonera świata przyszłości, pojawiły się w jego książce *The Information Society as Post-industrial Society* [Masuda 1981]. Co prawda jesteśmy jeszcze niezwykle daleko od wizji społeczeństwa według Masudy skonstruowanego wokół dóbr informacyjnych, w którym każdy znajduje

dla siebie niszę pozwalającą na realizowanie swoich potrzeb, niemniej jednak futurystyczna wizja, a zwłaszcza jej ciemna strona związana z zagrożeniami staje się powoli doświadczeniem współczesnych społeczeństw.

W niniejszym artykule, na podstawie analizy literatury, analizy dokumentów i danych statystycznych, podjęta zostanie próba uchwycenia podstawowych elementów związanych z zagrożeniami dla bezpieczeństwa społecznego w cyberprzestrzeni. Mając świadomość niezwykle złożonego charakteru badanego obszaru, autorka przyjęła jako problem badawczy stwierdzenie, że funkcjonowanie w cyberprzestrzeni może generować różnorakie zagrożenia dla bezpieczeństwa społecznego. Literatura i badania w tym temacie mają charakter rozproszony, ponieważ w ramach różnych dyscyplin są podejmowane analizy skupiające się na konkretnych, osadzonych w danej dyscyplinie problemach. Niemniej jednak można stwierdzić, że opis zagrożeń podejmowanych przez informatyków, psychologów, fizjoterapeutów, pedagogów, socjologów i innych bardzo często pozwala odnaleźć powiązania przyczynowo-skutkowe między nimi i często bywa podejmowany na przecięciu różnych dyscyplin. Tematyka zagrożeń dla bezpieczeństwa społecznego wymaga szerokich badań uwzględniających ich interdyscyplinarny i hybrydowy charakter. Wśród autorów podejmujących tę problematykę należy wymienić: Kimberly Young, Patrice Klausing, Patrice Wallace, Jamie'go Bartletta, S. Kozaka, Ł. Wojtasika, J. Grotha, J. Pyżalskiego, Mirosława Marodego, Andrzeja Augustynka, Katarzynę Kliszewską, Dominika Batorskiego, Manfreda Spitzera czy Claya Shirky'ego[1]. Świadomie w artykule nie uwzględniono ele-

[1] K. Young, P. Klausing OSF, *Uwolnić się z sieci. Uzależnienie od Internetu*, Katowice 2009; S. Kozak, *Patologie komunikowania w Internecie*, Warszawa 2011; Ł. Wojtasik, *Przemoc rówieśnicza z użyciem mediów elektronicznych – wprowadzenie do problematyki*, „Dziecko Krzywdzone" 2009, nr 1 (26); J. Groth, *Cyberstalking — perspektywa psychologiczna*, „Forum Oświatowe" 2010, nr 2 (43); J. Pyżalski, *Agresja elektroniczna wśród dzieci i młodzieży*, Gdańsk 2011; J. Pyżalski, *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży*, Kraków 2012; A. Andrzejewska, *(Nie)bezpieczny komputer: od euforii do uzależnień*, Warszawa 2008; *Cyberświat – możliwości i zagrożenia*, J. Bednarek, A. Andrzejewska (red.), Warszawa 2009; S. Juszczyk, *Człowiek w świecie elektronicznych mediów – szanse i zagrożenia (o problemach tworzącego się społeczeństwa informacyjnego)*, Katowice 2000; B. Danowski, A. Krupińska, *Dziecko w sieci*, Gliwice 2007; M. Castells, *Galaktyka Internetu: refleksje nad Internetem, biznesem i społeczeństwem*, T. Hornowski (tłum.), Poznań 2003; J. Wrycza, *Galaktyka języka Internetu*, Gdynia 2008; *Internet: między edukacją, bezpieczeństwem a zdrowiem*, M. Kowalski (red.), Tychy 2008; P. Aftab, *Internet a dzieci: uzależnienia i inne niebezpieczeństwa*, B. Nicewicz (tłum.), Warszawa 2003; *Internet a psychologia: możliwości i zagrożenia*, W.J. Paluchowski (red.), M. Ferenc-Michelson et al. (tłum.), Warszawa 2009; S. Bębas, *Patologie społeczne w sieci*, Toruń 2013; P. Wallace, *Psychologia Internetu*, T. Hornowski (tłum.), Poznań 2001; A. Augustynek, *Uzależnienia komputerowe: diagnoza, rozpowszechnienie, terapia*, Warszawa 2010; P. Majchrzak, N. Ogińska-Bulik, *Uzależnienie od internetu*, Łódź 2010; P. Chocholska, M. Osipczuk, *Uzależnienie od komputera i Internetu u dzieci i młodzieży*, Warszawa 2009; N.A. Christakis, J.H. Fowler, *W sieci*, I. Szybilska-Fiedorowicz (tłum.), Sopot 2011; K. Krzysztofek (et al.), *Wielka sieć: e-seje z socjologii Internetu*, J. Kurczewski (wstęp i red.), Warszawa 2006; E. Aboujaoude, *Wirtualna osobowość naszych czasów: mroczna strona e-osobowości*, R. Andruszko (tłum.), Kraków 2012; D. Batorski, *Uwarunkowania i konsekwencje korzystania z technologii informacyjno-komunikacyjnych*, [w:] *Diagnoza społeczna 2007:*

mentów zagrożeń społecznych związanych z cyberprzestrzenią w odniesieniu do przestępczości powiązanej z użyciem nowoczesnych technologii czy cyberterroryzmu. Podjęto próbę analizy tych zagrożeń, które mają bliższą korelację ze zdrowiem fizycznym i psychicznym użytkowników technologii informacyjnych.

POJĘCIE CYBERPRZESTRZENI I JEJ CHARAKTERYSTYKA

Termin „cyberprzestrzeń" pojawił się pierwszy raz w 1984 roku w powieści *Burning Chrome* napisanej przez Williama Gibsona i stał się kolejnym przeniesieniem literackiej formy na kształtującą się nową rzeczywistość [Konieczniak 2011]. Obecnie cyberprzestrzeń rozumiana jest jako przestrzeń otwartego komunikowania się za pośrednictwem połączonych komputerów i pamięci informatycznych pracujących na całym świecie [Levy 1997]. W dyskursie humanistycznym cyberprzestrzeń jest traktowana jako synonim internetu. Według Pierre'a Levy'ego cyberprzestrzeń ma charakter plastyczny, płynny, obliczalny z dużą dokładnością i przetwarzalny w czasie rzeczywistym, hipertekstualny, interaktywny i wreszcie wirtualny [Levy 1997]. Funkcjonowanie w tak opisanym środowisku z racji jego wielowątkowej płynności i intensywności oddziaływań na jednostki musi być powiązane z możliwością występowania różnorakich zagrożeń.

Dynamika rozwoju internetu i głębokie osadzenie współczesnych społeczeństw w cyberprzestrzeni stanowi interesujący problem badawczy, w którym istotnym wątkiem jest temat bezpieczeństwa i zagrożeń związanych z „cyfrowym zanurzeniem". Liczba użytkowników internetu według danych z 31 grudnia 2017 roku opublikowanych przez World Internet Users osiągnęła liczbę 4 156 932 140 osób [Internet usage statistics]. W Polsce według danych grupy Polskie Badania Internetu liczba internautów w marcu 2018 roku wynosiła ogółem nieco ponad 28 milionów, z czego użytkowników komputerów osobistych i laptopów 24,5 miliona, a urządzeń mobilnych (smartfony i tablety) 22,2 miliona [Polski Internet w marcu 2018]. Przełom XX i XXI wieku to dynamiczny rozwój technologii informatycznej, który poszerzył krąg odbiorców o tych uczestników, dla których sieć to nie tyle praca, co przede wszystkim rozrywka. Firma We Are

Warunki i jakość życia Polaków, J. Czapiński, T. Panek (red.), Warszawa, s. 268–288; M. Spitzer, *Cyberchoroby. Jak cyfrowe życie rujnuje nasze zdrowie*, Słupsk 2016; W. Furmanek, *Zagrożenia wynikające z rozwoju technologii informacyjnych*, „Dydaktyka Informatyki" 2014, nr 9, s. 20–48 czy publikacje popularnonaukowe: J. Bartlett, *The Dark Net*, Londyn 2015; L. Penny, *Cybersexism: Sex, gender and power on the internet*, Londyn 2013; P.J. Carnes, D.L. Demonico, E. Griffin, J.M. Moriarty, *In the Shadows of the Net: Breaking free of Compulsive Online Sexual Behaviour*, Center City, MN 2007; E. Lucas, C. Shirky, *Cyberphobia: Identity, Trust, Security and the Internet*, Nowy Jork 2015; C. Shirky, *Here Comes Everybody: The Power of Organizing Without Organizations*, Londyn 2008; N. Carr, *The Shallows: what the Internet is doing to our brains*, Nowy Jork 2010; K. S. Young, *Pathological Internet use: A case that breaks the stereotype. Psychological Reports*, 1996, s. 899–902; K. S. Young, *Caught in the Net*, Nowy Jork 1998.

Social opublikowała raport z danymi na koniec marca 2018 roku, wskazując w swoich infografikach na udział w rynku mediów społecznościowych 3 297 000 użytkowników i 5 061 000 użytkowników telefonów komórkowych [2018 Q2 Global Digital Statshot].

Tabela 1. Użytkownicy internetu na świecie. Statystyka populacji, 31 grudnia 2017 r.

Regiony	Ludność (2018 Est.)	Procentowy udział ludności	Użytkownicy internetu 31.12.2017	Wzrost 2000–2018	Użytkownicy internetu %
Afryka	1 287 914 329	16,9%	453 329 534	9,941%	0,9%
Azja	4 207 588 157	55,1%	2 023 630 194	1,670%	48,7%
Europa	827 650 849	10,8%	704 833 752	570%	17,0%
Ameryka Środkowa i Karaiby	652 047 996	8,5%	437 001 277	2,318%	10,5%
Bliski Wschód	254 438 981	3,3%	164 037 259	4,893%	3,9%
Ameryka Północna	363 844 662	4,8%	345 660 847	219%	8,3%
Oceania/Australia	41 273 454	0,6%	28 439 277	273%	0,7%
Świat	7 634 758 428	100,0%	4 156 932 140	1,052%	100,0%

Źródło: World Internet Usage and Populations Statistic, https://www.internetworldstats.com/stats.htm [dostęp: 26.04.2018].

Z punktu widzenia bezpieczeństwa społecznego interesujące są dane dotyczące wieku użytkowników internetu, ponieważ wskazują one jednoznacznie na osoby młode jako te, które są narażone na różnego typu zagrożenia. Natomiast brakuje na tyle długiej perspektywy, pozwalającej przeanalizować, co dalej z osobami, które są obecnie poddawane oddziaływaniu niekorzystnych zjawisk, czy osoby należące do pokolenia Z i Y[2] i które stanowią prawie 2/3 wszystkich użytkowników serwisu Facebook w Polsce, z upływem czasu nadal będą najaktywniejszymi użytkownikami mediów społecznościowych i czy w przyszłości ich aktywność będzie się zmniejszała [Raport Newspoint].

Tabela 2. Użytkownicy Facebooka i Instagrama

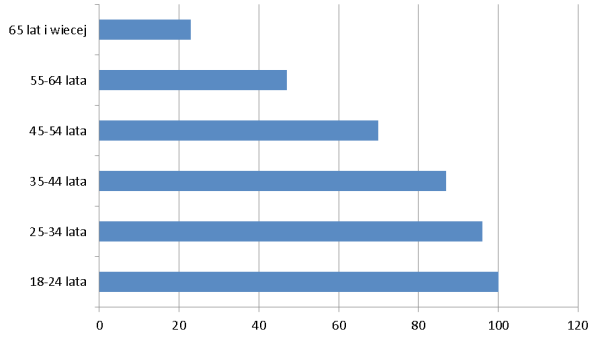
Państwo	Facebook	Państwo	Instagram
	Liczba użytkowników		Liczba użytkowników
1. Indie	270 000 000	1. Stany Zjednoczone	120 000 000
2. Stany Zjednoczone	240 000 000	2. Brazylia	61 000 000
3. Indonezja	140 000 000	4. Indie	59 000 000
5. Brazylia	130 000 000	3. Indonezja	56 000 000
6. Meksyk	85 000 000	4. Turcja	34 000 000
7. Filipiny	69 000 000	5. Rosja	31 000 000
8. Wietnam	58 000 000	6. Iran	24 000 000

[2] Pokolenie (generacja) Y, czyli millenialsi, za których uważa się osoby urodzone pomiędzy 1984 a 1996 rokiem oraz pokolenie (generacja) Z – osoby urodzone po 1997 roku.

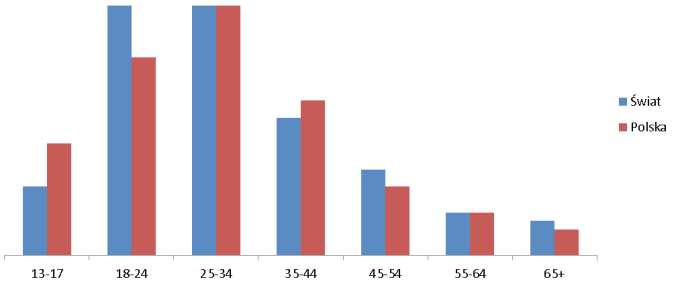
Państwo	Facebook	Państwo	Instagram
	Liczba użytkowników		Liczba użytkowników
9. Tajlandia	52 000 000	7. Japonia	23 000 000
10. Turcja	52 000 000	8. Wielka Brytania	23 000 000
11. Wielka Brytania	46 000 000	9. Meksyk	21 000 000

Źródło: 2018 Q2 Global Digital Statshot, We are Social, Hootsuite, https://wearesocial.com [dostęp: 26.04.2018].

Dane dla Polski według raportu *We Are Social* przedstawiają się następująco: spośród ponad 38 milionów obywateli niemal 30 milionów jest użytkownikami internetu, z czego 17 milionów jest aktywnymi użytkownikami mediów społecznościowych [*We Are Social*]. Raport Newspoint z kolei uwzględnia dane dotyczące wieku użytkowników Facebooka, który wciąż jest najpopularniejszym medium społecznościowym, chociaż wśród młodych ludzi, zwłaszcza poniżej 20. roku życia, zwiększa się odsetek użytkowników Instagrama, Twittera, Snapchata [*We Are Social*].



Rycina 1. Odsetek osób korzystających z internetu w grupach wiekowych.
Źródło: *Korzystanie z internetu*, Komunikat z badań nr 49/2017 CBOS, Warszawa 2017, s. 2.



Rycina 2. Użytkownicy Fecebooka – przedziały wiekowe Polska i świat.
Źródło: Raport Newspoint: *Pokolenia w Polsce i potrzeba monitorowania ich rosnącej aktywności*, https://blog.newspoint.pl/index.php/2018/03/21/raport-newspoint-pokolenia-w-polsce-i-potrzeba-monitorowania-ich-rosnacej-aktywnosci/ [dostęp: 26.04.2018].

Raport wskazuje, że w najaktywniejszych na Facebooku grupach wiekowych dane z Polski i ze świata są porównywalne i wynoszą w grupie wiekowej 25–34 lata po 29%, interesująca jest natomiast różnica w dwóch pierwszych grupach wiekowych, w których osiągnięto odpowiednio wyniki dla grupy 13–17 lat: Polska 13%, świat 8% i dla grupy 18–24 lata: świat 29%, Polska 23%. W Polsce w świetle badań przeprowadzonych w 2013 roku zanotowano również, że aż 83% dziesięciolatków posiada telefony komórkowe[3] [Yapp 2012].

BEZPIECZEŃSTWO A BEZPIECZEŃSTWO SPOŁECZNE

W badaniach nad zjawiskiem bezpieczeństwa w drugiej połowie XX wieku nastąpiła wyraźna ewolucja rozumienia tego pojęcia oraz poszerzenie pola badawczego związanego z wyodrębnieniem kategorii, takich jak bezpieczeństwo kulturowe, społeczne czy ideologiczne. Tym samym zwrócono uwagę na płaszczyzny, które wcześniej dla wielu naukowców i praktyków zajmujących się bezpieczeństwem były zbyt „miękkie" i niemierzalne [Buzan 1983; Pietraś 1996]. Na przełomie XX i XXI wieku kategorie te zyskały szczególne zainteresowanie badaczy wielu dziedzin nauki[4], zwracając uwagę na interdyscyplinarny charakter

[3] Średnia międzynarodowa w tym badaniu wynosiła 45%. Wyniki w pozostałych państwach: Wielka Brytania – 73%, Brazylia – 73%, Niemcy – 69%, Meksyk – 68%, Chiny – 49%, Hiszpania – 37%, USA – 31%, Australia – 31%, Japonia – 20%, Kanada – 17%, Francja – 10% [Yapp 2012].

[4] Literatura dotycząca problematyki bezpieczeństwa i bezpieczeństwa społecznego jest niezwykle obszerna i obejmuje między innymi następujące pozycje: K. Kiciński, *Socjologiczne problemy bezpieczeństwa narodowego – prognozy, przewidywania*, [w:] *Wybrane problemy socjologii wojska*, cz. 1, J. Kunikowski (red.), Warszawa 1998; *Kondycja moralna społeczeństwa polskiego*, J. Mariański (red.), Kraków 2002; A. Nowak, E. Wysocka, *Problemy i zagrożenia społeczne we współczesnym świecie*, Katowice 2001; *Wymiary życia społecznego. Polska na przełomie XX i XXI wieku*, M. Marody (red.), Warszawa 2002; W. Kitler, *Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania. System*, Warszawa 2011; K. Loranty, *Idea bezpieczeństwa społecznego państwa*, [w:] *Współczesne bezpieczeństwo. Perspektywa teoretyczno-metodologiczna*, S. Jaczyński, M. Kubiak, M. Minkina (red.), Warszawa–Siedlce 2011; R. Jakubczak, R. Kalinowski, K. Loranty, *Bezpieczeństwo społeczne w erze globalizacji*, Siedlce 2008; A. Korcz, *Bezpieczeństwo społeczne Rzeczypospolitej Polskiej*, www.adamkorcz. w.interia.pl/spol.pdf [dostęp: 3.01.2012]; M. Leszczyński, *Bezpieczeństwo społeczne a bezpieczeństwo państwa*, Kielce 2009; M. Leszczyński, *Bezpieczeństwo społeczne a współczesne państwo*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2011; M. Leszczyński, *Bezpieczeństwo socjalne a bezpieczeństwo państwa*, „Securitologia" 2008, nr 2; M. Pietraś, *Bezpieczeństwo ekologiczne w Europie. Studium politologiczne*, Lublin 2000; A. Skrabacz, *Bezpieczeństwo społeczne*, „Zeszyty Naukowe AON" 2002, nr 3–4; A. Skrabacz, *Współczesne zagrożenia społeczne*, [w:] *Patologie społeczne jako zagrożenia państwa i jego obywateli*, „Biuletyn Informacyjny Towarzystwa Wiedzy Obronnej i Wyższej Szkoły Humanistycznej", Warszawa 2004; A. Skrabacz, K. Loranty, *Bezpieczeństwo społeczne*, [w:] *Bezpieczeństwo narodowe Polski w XXI wieku. Wyzwania i strategie*, R. Jakubczak, J. Marczak (red.), Warszawa 2011; *Bezpieczeństwo społeczne. Pojęcia. Uwarunkowania. System*, A. Skrabacz, S. Sulowski (red.), Warszawa 2012; R. Szarfenberg, „Bezpieczeństwo socjalne a wykluczenie społeczne". Referat wygłoszony na konferencji „Bezpieczeństwo socjalne"

tego zjawiska oraz na znaczenie elementów, które mają charakter pozapaństwowy, społeczny i opierają się na subiektywnych wskaźnikach wyrażanych często w badaniach opinii publicznej[5]. W ramach tych koncepcji wyodrębniła się nowa dyscyplina naukowa – securitologia, w której polu zainteresowań znajdują się problemy związane z zagrożeniami odnoszącymi się do istnienia, rozwoju i funkcjonowania człowieka i organizacji społecznych [Majer]. W kontekście zagrożeń bezpieczeństwa społecznego tym bardziej widać interdyscyplinarny charakter omawianych zjawisk, które są w obszarze zainteresowań nauk powiązanych z informatyką, medycyną, psychologią, socjologią, prawem czy komunikowaniem. Jednocześnie zagrożenia związane z cyberprzestrzenią powinno się traktować jako hybrydowe, o wielu krzyżujących się poziomach analizy. Należy dodatkowo zdać sobie sprawę, że elementy państwowe, których mechanizmy powinny stabilizować i regulować to, co generuje zagrożenia dla bezpieczeństwa społecznego, w przypadku cyberprzestrzeni mają zadanie niezwykle utrudnione, a często zbyt późno wychwytują i reagują na zaistniałe niekorzystne zjawiska bądź podejmują działania nieskuteczne w zdecentralizowanym obszarze wirtualnej rzeczywistości.

W literaturze przedmiotu wyraźnie widać dwa podstawowe nurty w badaniu tej problematyki. Skupiono się na analizie bezpieczeństwa społecznego z punktu widzenia polityki społecznej oraz podejściu związanym z rozwojem nauk o securitologii, niejako rozszerzającym tę dziedzinę w stosunku do pierwszego tropu, łączącym tematykę polityki społecznej z polityką bezpieczeństwa w ogóle[6]. Do rozwoju badań

w Ustroniu 2003, Biała Księga Bezpieczeństwa Narodowego RP, 2013; *Współczesny wymiar bezpieczeństwa. Między teorią a praktyką*, J. Pawłowski (red.), Warszawa 2011; *Metodologia badań bezpieczeństwa narodowego*, t. 3, P. Sienkiewicz, M. Marszałek, H. Świeboda (red.), Warszawa 2012; *Bezpieczeństwo narodowe Polski w XXI wieku. Wyzwania i strategie*, R. Jakubczak, J. Marczak (red.), Warszawa 2012; R. Zięba, *Pojęcie i istota bezpieczeństwa państwa w stosunkach międzynarodowych*, „Sprawy Międzynarodowe" 1989, nr 10; J. Kukułka (red.), *Bezpieczeństwo międzynarodowe w Europie Środkowej po zimnej wojnie*, Warszawa 1994; B. Buzan, *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*, Harvester Wheatsheaf, London 1991; O. Waever, B. Buzan, M. Kelstmp, P. Lemataire, *Identity, Migration and the New Security Agenda in Europe, Centre for Peace and Conflict Research*, London 1993; B. Buzan, *Rethinking Security after the old War*, „Cooperation and Conflict" 1997, vol. 32, nr 1; B. Barry, O. Wæver, J. de Wilde Jaap, *Security: a new framework for analysis*, Lynne Rienner 1998; B. McSweeney, *Security, Identity and Interests: A Sociology of International Relations*, 1996.

[5] Zwłaszcza problematyka zagrożeń bezpieczeństwa społecznego jest analizowana jako zjawisko subiektywne. Zobacz szerzej: [Buzan, Wæver, de Wilde 1998: 27]; [Zięba 2012, 1: 9–11].

[6] Sam termin „bezpieczeństwo społeczne" po raz pierwszy pojawił się w roku 1935 w ustawie Stanów Zjednoczonych Ameryki odnoszącej się do stosowania programów w przypadku starości, inwalidztwa, śmierci czy bezrobocia, a następnie w Nowej Zelandii w 1938 roku w ustawie wprowadzającej świadczenia socjalne. W latach 1952–1982 Międzynarodowa Organizacja Pracy podjęła próbę uporządkowania tego terminu, łącząc w nim takie elementy, jak m.in.: ubezpieczenia społeczne, świadczenia rodzinne, pomoc społeczną. Najbardziej znaną definicją *social security* jest definicja Międzynarodowej Organizacji Pracy z 1984: „jest to ochrona, którą dostarcza społeczeństwo swoim członkom poprzez zapobieganie ekonomicznej i społecznej nędzy, która może być powodowana redukcją zarobków, chorobą, macierzyństwem, dyskryminacją w sektorze zatrudnienia, bezrobociem,

nad bezpieczeństwem społecznym przyczyniło się również wprowadzenie pojęcia *human security*, zwracając tym samym uwagę na jednostkowy wymiar bezpieczeństwa. W Raporcie ONZ wydanym w ramach Programu ds. Rozwoju z 1994 roku wskazano na cztery główne cechy *human security*. Uznano, że bezpieczeństwo jest pojęciem uniwersalnym, związanym z ludzkością, a wszystkie wymiary wchodzące w jego zakres są powiązane i zorientowane na człowieka. Wskazano również na znaczenie działań prewencyjnych [Development Report 1994][7]. *Societal security* to z kolei koncepcja separująca problematykę bezpieczeństwa od państwa, związana z taką możliwością zachowania homeostazy społecznej, która nie powoduje zaangażowania państwa, a zwraca uwagę na tożsamościowy wątek połączeń w ramach społeczeństwa. Być może właśnie ta perspektywa, chociaż zapewne w odległej przyszłości, będzie podstawowym modelem analizy bezpieczeństwa społecznego w zdecentralizowanej cyberprzestrzeni i słowa Yoneji Masudy dotyczące integracji grup społecznych wokół pewnych wartości i wymiany informacji rozbiją dotychczasowy model analizy bezpieczeństwa [Masuda 1981]. Wydaje się, że słuszne byłoby uznać uzupełniający charakter obu pojęć, uwzględniając przynależność tego pierwszego do szerszej kategorii drugiego przy zastrzeżeniu, że oba mogą oczywiście podlegać odrębnej analizie i oba podlegają podobnym zagrożeniom, pierwsze w wymiarze jednostkowym, drugie społecznym.

Pod pojęciem bezpieczeństwa społecznego najogólniej możemy rozumieć: ochronę egzystencjalnych podstaw życia ludzi, zapewnienie możliwości zaspokajania indywidualnych potrzeb (materialnych i duchowych), realizację aspiracji życiowych przez tworzenie warunków do pracy i nauki, ochronę zdrowia, jak również utrzymywanie w zadowalających warunkach rozwoju tradycyjnych wzorców języka, kultury i tożsamości religijnej i narodowej oraz dotychczasowych zwyczajów [Buzan, Wæver, de Wilde 1998].

W pracy Aleksandry Skarbacz *Bezpieczeństwo społeczne. Podstawy teoretyczne i praktyczne* autorka scharakteryzowała dwa podsystemy konstytuujące bezpieczeństwo społeczne. Podsystem bezpieczeństwa socjalnego, który według niej wiąże się z obowiązkiem zapewnienia przez „państwo wszystkim obywatelom (szczególnie bezrobotnym, samotnym matkom czy bezdomnym) minimalnego standardu życia przez wprowadzenie odpowiednich ułatwień lub możliwości bezpłatnego korzystania z lecznictwa, oświaty i kultury" (poziom *hard*). Drugi z nich to podsystem bezpieczeństwa psychospołecznego, który odnosi się do stanu psychicznego i społecznego jednostek i grup społecznych gwarantującego stabilny rozwój i realizację podstawowych celów i zadań życiowych oraz zawodowych w warunkach akceptacji i tolerancji społecznej" (poziom *soft*) [Skarbacz 2012]. Wprowadzenie powyższego

niepełnosprawnością, podeszłym wiekiem i śmiercią. Dostarcza opiekę zdrowotną i ochronę dla rodzin z dziećmi". Zob. [Buzan, Wæver, de Wilde 1998: 119–120]; [Skrabacz 2012: 31–33].

[7] Wątek ten rozwijały kolejne raporty ONZ: United Development Program, Human Development Raport 1999. Globalization with a Human Face. Więcej na temat rozwoju koncepcji *human security:* [Marczuk 2007: 56–95]; [Tajbakhsh, Chenoy 2006]; [Alkire 2002].

rozróżnienia, po pierwsze, potwierdza uznanie łączności między *human security* a *societal security*, po drugie zaś wskazuje jak poziom *soft* jest konstytuowany przez subiektywny format odniesienia jednostki w społeczeństwie.

RODZAJE ZAGROŻEŃ BEZPIECZEŃSTWA W CYBERPRZESTRZENI

Omawiając pojęcie „bezpieczeństwo społeczne", należy zwrócić szczególną uwagę na zagrożenia, które są nierozerwalnie związane z tą kategorią. Termin „zagrożenia" należy odnieść do sfery świadomościowej danego podmiotu (człowieka, grupy społecznej, narodu) i powiązać ze stanem psychiki lub świadomości wywołanym postrzeganiem zjawisk, które mogą być oceniane jako niekorzystne lub niebezpieczne [Dworecki 2002]. W związku z tym należy je analizować w kategoriach poczucia bezpieczeństwa oraz odzwierciedlenia w świadomości realnego lub potencjalnego zagrożenia. Oznacza to tym samym, że może być niezgodna ze stanem faktycznym, ponieważ uwzględnia nie tylko obiektywne, ale przede wszystkim subiektywne aspekty zagrożeń i bezpieczeństwa [Zięba 1999][8]. Szwajcarski politolog Daniel Frei przedstawił cztery sytuacje na podstawie obu komponentów bezpieczeństwa:

- stan braku bezpieczeństwa (rzeczywiste zagrożenie, adekwatnie postrzegane),
- stan obsesji (nieznaczne zagrożenie, ale postrzegane nieadekwatnie jako duże),
- stan fałszywego bezpieczeństwa (zagrożenie poważne, ale nieadekwatnie postrzegane jako niewielkie),
- stan bezpieczeństwa (zagrożenie nieznaczne, adekwatnie postrzegane) [Frei 1977].

W związku z tym zagrożenia w cyberprzestrzeni w odniesieniu do społeczeństwa i jednostek mogą być analizowane jako:

- zagrożenia zdrowia psychicznego i fizycznego,
- zagrożenia społeczno-wychowawcze,
- zagrożenia związane z uzależnieniami,
- zagrożenia związane z treściami szkodliwymi i nielegalnymi,
- zagrożenia związane z ochroną prywatności.

Inny katalog zagrożeń przedstawił Waldemar Furmanek [Furmanek 2014] i według niego to:

I. Zagrożenia o charakterze psychologicznym:

- wewnętrzny przymus bycia w sieci,
- ucieczka od świata realnego do sztucznego świata wirtualnego,
- dostęp do patologicznych grup kulturowych,
- alienacja (np. alienuje telepraca);

[8] Por. [Witaszek 2013: 194–195], na temat badania zagrożeń: [Loranty 2012: 10–18].

II. Zagrożenia o charakterze technicznym:
- zagrożenie utraty danych w wyniku kradzieży lub ich zniszczenie przez człowieka,
- wirusy komputerowe;

III. Zagrożenia o charakterze medycznym:
- zagrożenia zdrowia człowieka powodowane m.in. pracą przy komputerze czy szkodliwością promieniowania monitora komputera;

IV. Zagrożenia o charakterze prawnym:
- zagrożenie praw autorskich;

V. Zagrożenia o charakterze społecznym:
- niebezpieczeństwo nowych podziałów społecznych spowodowane nierównomiernym dostępem do informacji – problem wykluczenia,
- atomizacja społeczeństwa,
- zanik poczucia służby publicznej,
- problemy ochrony prywatności,
- napływ informacji niezamawianej, nieprawdziwej, niekompletnej;

VI. Zagrożenia informacyjne wynikające z rozwoju współczesności:
- nadmiar informacji,
- pomijanie informacji,
- niezależność informacji,
- rozbieżność informacji,
- problematyczna wartość informacji,
- szum informacyjny,
- stres informacyjny,
- niskie kompetencje informacyjne odbiorców informacji (ang. *information illiteracy*),
- dylematy etyczne.

Widać zatem, że bezpieczeństwo społeczne w cyberprzestrzeni, a zwłaszcza zagrożenia bezpieczeństwa mogą być rozpatrywane z punku widzenia wielu dyscyplin naukowych, wiele z tych zagrożeń ma niejako charakter krzyżowy i jest ze sobą powiązanych, co stanowi dodatkowy element komplikujący zarówno badanie tematu, jak i prewencję wobec zagrożeń.

Walka z zagrożeniami hybrydowymi w ramach bezpieczeństwa społecznego wymaga zmiany sposobu patrzenia na bezpieczeństwo. Po pierwsze obok działań państw – w pierwszej kolejności prawnych i edukacyjnych – powinna zaistnieć świadomość ludzi dotycząca myślenia o bezpieczeństwie w kategoriach jednostkowych.

Zagrożenia zdrowia psychicznego i fizycznego stanowią jeden z najbardziej czytelnych zagrożeń związanych z cyberprzestrzenią. Zarówno w odniesieniu do jednostki, jak i społeczeństwa zwraca uwagę fakt silnego skorelowania wielu patologii społecznych z ich osadzeniem w internecie. Warto w związku z tym w kontekście zagrożeń dla bezpieczeństwa społecznego zwrócić uwagę na cechy społeczności wirtualnej wyróżnione przez Marka Smitha [za: Szpunar 2004], które również wpływają na rozpowszechnianie się różnych negatywnych tendencji:

- aprzestrzenność – uczestnicy z całego świata mogą się ze sobą kontaktować za pośrednictwem internetu,
- asynchroniczność – komunikacja nie zawsze ma miejsce w czasie rzeczywistym,
- acielesność – jedynym nośnikiem informacji jest język,
- astygmatyczność – nie są istotne cechy wyglądu danej osoby, ale wspólne poglądy,
- anonimowość – użytkowników znają się po „nickach".

Jednym z zagrożeń związanych z funkcjonowaniem w cyberprzestrzeni jest tzw. zespół uzależnienia od internetu – ZUI. Wyraźnie widać, że w jego ramach mieści się większość wymienionych wcześniej zagrożeń. Badanie i analiza tych krzyżowych zagrożeń stanowi podstawę do całościowego zrozumienia problemu. Uzależnienie od komputera, gier komputerowych, a zwłaszcza internetu od początku 2018 roku zostało wpisane do klasyfikacji ICD-10 jako jednostka chorobowa. Pod pojęciem zespół uzależnienia od internetu możemy rozumieć „zespół zależności polegających na wielogodzinnym korzystaniu z sieci Internet, które są dla pacjenta źródłem stresu oraz negatywnie wpływają na jego funkcjonowanie w sferze fizycznej, psychicznej, interpersonalnej, społecznej, rodzinnej i ekonomicznej" [Wallis 1997]. W literaturze można spotkać się z takimi terminami, jak: patologiczne używanie internetu, nadużywanie internetu, kompulsywne używanie internetu (w piśmiennictwie anglojęzycznym są używane następujące terminy: *Internet addiction disorder*, *Internet addiction syndrome*, *Internet abuse*, *compulsive Internet use*, *pathological Internet use*). Według WHO o uzależnieniu można mówić, gdy spełnione zostaną trzy warunki. Po pierwsze, gdy osoba utraci zdolność kontrolowania czasu, jaki spędza na graniu. Po drugie, gdy gry staną się najważniejszą wykonywaną czynnością, a pozostałe zejdą na dalszy plan. I po trzecie, gdy osoba będzie kontynuowała grę mimo wystąpienia negatywnych konsekwencji [Public Health Implications of Excessive Use of the Internet].

Dla Kimberly Young [1998] patologiczne używanie internetu to „zaburzenie kontroli nawyków niepowodujące intoksykacji, natomiast istotnie i wyraźnie pogarszające funkcjonowanie człowieka we wszystkich sferach jego życia". Autorka zaproponowała następującą metodę diagnostyczną przy spełnieniu 5 z 8 symptomów w ciągu ostatniego roku: 1) silne zaabsorbowanie internetem, przejawiające się ciągłym myśleniem o byciu online; 2) wzmagająca się potrzeba coraz dłuższego przebywania online, aby być tym faktem usatysfakcjonowanym; 3) powtarzające się, lecz nieudane próby kontroli własnego korzystania z internetu polegające na redukcji lub zaprzestaniu; 4) pojawianie się silnych negatywnych afektów w sytuacji ograniczania używania internetu, jak np. przygnębienie, irytacja itp.; 5) problemy z organizowaniem czasu przebywania online; 6) stres, problemy osobiste i społeczne wynikające z używania internetu; 7) manipulacja w relacjach z otoczeniem, której celem jest ukrywanie informacji na temat własnego zaabsorbowania internetem; 8) regulacja emocjonalna przy pomocy aktywności internetowej, która przybiera formę ucieczki od problemów i uśmierzania negatywnych emocji.

Wśród podtypów zespołu uzależnienia od internetu Kimberly Young wymieniła m.in. erotomanię internetową (ang. *cybersexual addiction*), która polega na oglądaniu filmów i zdjęć z materiałami pornograficznymi oraz rozmowach na chatach czy forach internetowych o tematyce seksualnej. Należy zwrócić uwagę, że kontakt z takimi materiałami szczególnie osób małoletnich może spowodować różne zaburzenia w sferze emocjonalnej. Badania wśród polskich nastolatków z września 2013 roku [*Prezentacja treści seksualnych*…] wskazały na to, że o zjawisku wykorzystania rozmów wideo do prezentacji treści seksualnych słyszała około połowa badanych nastolatków, zaś około 16% badanych zetknęło się z tym zjawiskiem bezpośrednio podczas wideorozmów [*Prezentacja treści seksualnych*…]. Do tego można jeszcze dołączyć badania dotyczące ryzykownych zachowań seksualnych związanych z internetem, które wskazują na fakt, że nawet zakładanie profili na portalach randkowych wiąże się z możliwością seksualnego napastowania, cyberprzemocy bądź w przypadku spotkania się z takim partnerem poza siecią naraża na przemoc lub zarażenie chorobą[9]. Drugą formą zaburzeń jest socjomania internetowa (ang. *cyber-relationship addiction*) związana z potrzebą nawiązywania i utrzymywania kontaktów społecznych tylko przez sieć – powoduje ograniczenie, a nawet zanik kontaktów osobistych przy jednoczesnym upośledzeniu odbierania sygnałów komunikacji niewerbalnej, zubożeniu języka, aż do postępującego zamykania się we własnym świecie. Inną formą jest uzależnienie od sieci (ang. *net compulsions*) i uzależnienie od komputera. Uzależnienia te łączą w sobie wszystkie formy ZUI. Spektrum tych form należy poszerzyć o konsekwencje wynikające z tych zaburzeń. I tak, A. Hoall i J. Parsons wprowadzili termin *internet behavior dependece* (IBD), czyli uzależnienie behawioralne. Autorzy stwierdzili, że patologiczne wykorzystywanie internetu może uszkodzić funkcje poznawcze, zaburzyć zachowanie i różne sfery zdrowia jednostki [Hoall, Parsons 2001], może nastąpić reorganizacja struktury potrzeb, doprowadzając jednostkę do chorób psychicznych, agresywnych zachowań skierowanych zarówno na siebie, jak i innych, bezdomności i atrofii struktur rodzinnych. W tym duchu Małgorzata Styśko-Kunkowska i Grażyna Wąsowicz, autorki raportu *Uzależnienia od e-czynności wśród młodzieży: diagnoza i determinanty*, wprowadzając pojęcie „e-czynności" jako jednostkę aktywności powiązanej z nowymi technologiami, zwróciły uwagę na różnorodne zagrożenia. W ich badaniach pojawiły się następujące niebezpieczeństwa:

[9] Przegląd wybranych zagrożeń zdrowotnych związanych z internetem: Ł. Wojtasik, *Sekstingwśród dzieci i młodzieży*, „Dziecko Krzywdzone. Teoria, Badania, Praktyka" 2014, vol. 13, nr 2; E.R. Buhi, N. Klinkenberger, M. McFarlane, R. Kachur, E.M. Daley, J. Baldwin, H.D. Blunt, S. Hughes, C.W. Wheldon, C.A. Rietmeijer, *Evaluating the Internet asa sexually transmitted disease risk environment for teens: findings from the communication, health and teens study*, „Sex. Trans. Dis." 2013, nr 40, 7, s. 528–533; H. Klein, *Anonymous sex and HIV risk practices among men using the Internet specifically to find male partners for unprotected sex*, „Public Health" 2012, nr 126, 6, s. 471–481; A.A. Al-Tayyib, M. McFarlane, R. Kachur, C.A. Rietmeijer, *Finding sex partners on the internet: what is the risk for sexually transmitted infection?*, „Sex. Trans. Infect." 2009, nr 85, 3, s. 216–220.

- wyobcowanie, które może być powiązane z wykluczeniem społecznym,
- uzależnienie od gier, które może powodować brak lub utratę umiejętności nawiązywania relacji i współżycia w grupie,
- zachowania agresywne słowne (wulgaryzmy) i fizyczne (niekontrolowane wybuchy agresji, pobicia), a nawet brak zdolności założenia własnej rodziny lub trudności z utrzymaniem relacji rodzinnych,
- problemy szkolne i zawodowe związane z zaburzeniem uwagi, problemami z koncentracją oraz skupienie myśli tylko na tematyce związanej z daną e-czynnością.

W kontekście problemów zawodowych związanych z e-uzależnieniami (od e-gier, e-hazardu i e-zakupów) autorki wymieniły między innymi problemy z pozyskaniem lub utrzymaniem pracy, co jest związane z brakiem motywacji, umiejętności i wiedzy oraz z brakiem szacunku do pracy jako sposobu pozyskiwania pieniędzy lub z zaniedbywaniem jej (np. przez spóźnienia). W przypadku e-gier i e-hazardu efektem mogą być także ograniczenia intelektualne i problemy neurologiczne związane z ograniczeniem zainteresowań wyłącznie do tej jednej e-czynności i brakiem stymulacji zmysłów dotyku, zapachu, motoryki stymulacją jednej sfery motoryki, czyli ręki. Takie zjawiska mogą utrudniać zarówno funkcjonowanie szkolne, jak i zawodowe. Zaburzenia osobowościowe (niskie poczucie własnej wartości, mała wiara w siebie, mniejsze lub większe zaburzenia tożsamości, niewłaściwe wzorce zachowań) i zaburzenia emocjonalne (depresja lub nastroje depresyjne, nerwowość, drażliwość, agresja, pobudliwość, spadek odporności psychicznej) [Styśko-Kunkowska, Wąsowicz: 26–27].

Z kolei dla Macieja Tanasia młodzież korzystająca z nowych technologii informacyjnych może być narażona na zagrożenia dydaktyczne oraz psychiczne. Autor wyróżnił między innymi:

- zaburzenia funkcji poznawczych prowadzące do niemożności kontynuowania nauki (zaburzenia percepcji, płynności uwagi, ograniczenie lub utrata zdolności logicznego myślenia, poczucie zagubienia, natrętne myśli, zachowania kompulsywne, zaburzenia pamięci, niemożność kontynuowania nauki jako konsekwencja wyżej wymienionych zaburzeń i objawów towarzyszących, związana np. z dyskomfortem psychicznym, pojawiającym się w wyniku drastycznych interwencji, tj. syndrom odstawienia, niekiedy o drastycznym przebiegu [Tanaś 1993],
- ucieczkę od świata realnego do sztucznego, wirtualnego: złudne poczucie siły i przynależności, często patologizującej rywalizację (rekordy w grach), bez respektowania zasad etycznych; złudne poczucie wolności, bycia niezastąpionym, przymus bycia online, potrzeba autoprezentacji i poczucia obecności (własna strona WWW),
- specyficzne postacie patologii społecznej: nieuzasadniona indywidualna lub zbiorowa agresja i autoagresja oraz frustracje; powielanie wzorców patologicznych i destrukcyjnych – agresja na ekranie ujawnia się w normach akceptowanych przez grupy rówieśnicze i społeczności lokalne (subkultury,

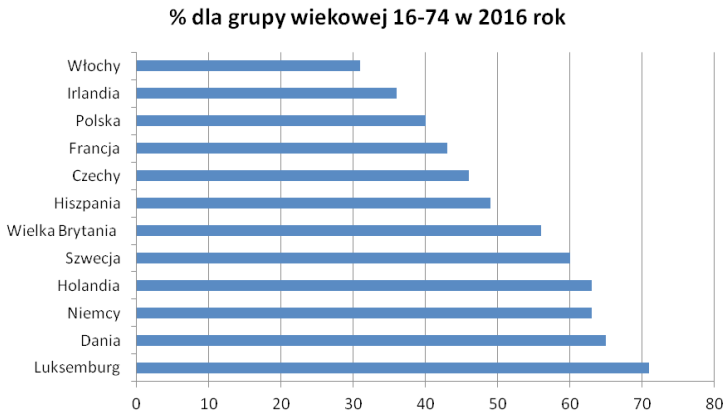
lokalne nacjonalizmy, rejony podwyższonego ryzyka); dostęp do patologicznych grup o celach niejasnych, funkcjonujących na pograniczu lub poza prawem. Przystąpienie do nich jest równoznaczne z zaangażowaniem się lub byciem ofiarą (prostytucja, pornografia dziecięca, pedofilia, handel żywym towarem, organami itd.); dostęp do toksycznych grup kulturowych, parareligijnych, pseudoterapeutycznych, krypto lub jawnie satanistycznych, szerzących ideologię destrukcji, zła, agresji i nihilizmu,

- uzależnienia: syndrom *internet addiction disorder* – niejednorodne zjawisko uzależnienia od internetu, tj. wewnętrzny przymus bycia w sieci. Ulega mu 18% użytkowników spędzających w internecie ponad 70 godzin tygodniowo; syndrom technohipnozy – popadanie w trans przez dzieci w trakcie emisji reklam lub gier komputerowych; syndrom ASC – intensywne korzystanie z komputera może prowadzić do zmienionych stanów świadomości, podobnych fizjologicznie i psychologicznie do stanów intoksykacji farmakologicznej, alkoholowej czy narkotycznej. Syndrom ten ułatwia akceptowanie różnych nakazów i zakazów, także groźnych społecznie ideologii; uzależnienie od programów zawierających elementy psychomanipulacji, technik perswazyjnych, technik kontroli umysłu, technik bioneuromanipulacyjnych, działających na centralny układ nerwowy,
- dysfunkcje neurologiczne: syndrom padaczki ekranowej, któremu w Japonii w roku 1997 uległo prawie 1000 osób; nerwice [Tanaś 1993].

Z kolei w pracy *iMózg. Jak przetrwać technologiczną przemianę współczesnej umysłowości* autorstwa G. Smalla i G. Vorgan zwrócono uwagę na zmiany strukturalne i funkcjonalne w neuronalnej budowie mózgu związane z długotrwałym korzystaniem z internetu [Small, Vorgan 2011]. Zmiany te powodują określone konsekwencje i wpływają na procesy poznawcze człowieka.

Obok problemów o charakterze psychicznym należy zwrócić uwagę na wiele konsekwencji dla zdrowia fizycznego. Niezdrowy tryb życia, brak aktywności, siedząca pozycja, stosowanie używek czy zaniedbywanie potrzeb fizjologicznych wpływają na ogólną kondycję człowieka. Na pogorszenie stanu zdrowia mogą się składać dolegliwości związane z funkcjonowaniem organu wzroku, wystąpienie bólów kręgosłupa, barków, karku, nadgarstków i mięśni, przykurczy ścięgien, zmian w postawie ciała oraz pojawienie się trudności z oddychaniem (związanych z niedoborem tlenu). Dla części z tych dolegliwości opracowano termin RSI (ang. *repetitive strain injury*) – urazy na skutek chronicznego przeciążenia mięśni i ścięgien. Powstają na skutek długotrwałego powtarzania czynności. Jest to powszechna dolegliwość wśród pracowników linii montażowych, piszących na klawiaturze, graczy używających myszy komputerowych, sekretarek i pracowników IT itd. Choroba ta jest związana z długotrwałym utrzymywaniem tej samej pozycji ciała – siedzenie bez możliwości przerwy przez długi czas, bądź wykonywaniem powtarzających się czynności – obsługa komputera za pomocą myszy i klawiatury, praca narzędziami ręcznymi. W odpowiedzi na nią w ramach systemów operacyjnych Windows i Linux opracowano program Workrave, który

ma za zadanie przypominanie o aktywności i proponowanie określonych zestawów ćwiczeń. Wycinkowe badania Marii Bartosińskiej, Jana Ejsmonta i Marii Tukalskiej-Parszuto przeprowadzone na grupie 477 osób pracujących na stanowiskach komputerowych skłoniły badaczy do stwierdzenia, że taka praca może stanowić obciążenie nie tylko dla narządu wzroku, układu mięśniowo-kostnego, ale również jest obciążeniem psychicznym. Na skutek długotrwałej i intensywnej pracy przy komputerze, nieprawidłowego usytuowania stanowiska pracy, niewłaściwego oświetlenia może dochodzić nie tylko do zmęczenia wzroku, lecz także do pogłębiania się lub ujawnienia jego wad. Wysiłek statyczny czy nieprawidłowa pozycja ciała podczas pracy mogą doprowadzić do przewlekłych zespołów przeciążenia układu mięśniowo-kostnego i trwałych zmian zwyrodnieniowych. Autorzy badania zwrócili również uwagę na różnego rodzaju promieniowania, w tym promieniowanie jonizujące (rentgenowskie), ultrafioletowe, podczerwone, radiowe oraz ultradźwięki, nie zauważając jednak ich niebezpiecznego oddziaływania [Bartosińska, Ejsmont, Tukalska-Parszuto 2001]. Najnowsze badania prowadzone przez A.M. Laverdurea, G. Ermakova, V. Bondarovskaja, I. Petrovskaja i innych, które dotyczyły szkodliwości promieniowania elektromagnetycznego o niskich częstotliwościach (do 50 Hz) emitowanego przez ekrany monitorów komputerowych oraz telewizorów, jak również telefonów komórkowych, wskazują na powiązania z występowaniem chorób cywilizacyjnych. Autorzy stwierdzili, że pole elektromagnetyczne powoduje obniżenie wydolności immunologicznej, co sprzyja rozwojowi chorób nowotworowych, a także powstawaniu alergii. Według badaczy pole elektromagnetyczne powoduje również częste infekcje, obniżenie płodności, zespół przewlekłego zmęczenia, problemy z zapamiętywaniem oraz wzrost agresywności [Szymański].



Rycina 3. Użytkownicy internetu a „Doktor Google" – 2016 rok.
Źródło: Eurostat – marzec 2017[10].

[10] Zob. także: [*eHealth literacy and Web 2.0*… 2015].

Na drugim biegunie problemów społecznych związanych z cyberprzestrzenią w obszarze zdrowia jest powiększająca się liczba użytkowników, dla których internet jest źródłem wiedzy medycznej. „Doktor Google" oraz różne strony i portale określające się jako medyczne stały się dla wielu osób „lekarzem pierwszego kontaktu". Oczywiście niesie to ze sobą liczne zagrożenia związane z błędnymi diagnozami, brakiem wdrożenia właściwego leczenia, diagnostyki itd.

Dane wskazują, że w wielu państwach występuje w związku z tym poważny problem. Uzupełnieniem tego zjawiska jest cyberchondria, czyli często nieuzasadnione, wzmożone zamartwianie się swoim stanem zdrowia, spowodowane poszukiwaniem w internecie informacji medycznych na temat objawów różnych chorób i dolegliwości. Jest to zaburzenie neurotyczne uważane za odmianę hipochondrii [*Cyberchondria and Intolerance of Uncertainty*]. Innym niezwykle złożonym problemem jest ruch pro-ana (*professional-ana*) – związany z promocją w sieci anoreksji. Jednym z haseł tego ruchu jest zdanie *quod me nutrit me destruit* – „to, co mnie żywi, niszczy mnie". Ruch powstał po 2001 roku i nawiązuje do wielu stron internetowych i forów poświęconych wspieraniu osób, które obsesyjnie się odchudzają. Są to jednak strony związane z promocją takiego stylu życia (osoby w tym ruchu używają sformułowania „thinspiracje"), np.: ANAMADIM, Pro-Anorexia, Pro-ED, Pro-Eating, Disorder, Anorexic Nation, 2b-Thin, Thinspiration, ED's Friends, Totally in Control, Starving for Perfection i Dying to be Thin. Aby zostać przyjętym do grupy, trzeba przejść system weryfikacji po to, by udowodnić, że jest się „motylkiem" – jak nazywają same siebie osoby należące do tego ruchu. W środowisku pro-ana anoreksja jest spersonalizowana i nazywana „Aną" [Środek 2011]. Zgromadzenie Narodowe we Francji w 2008 roku przy olbrzymim sprzeciwie branży mody przyjęło ustawę nakładającą karę 35 tysięcy euro i dwóch lat więzienia za zachęcanie kobiet do ekstremalnej diety oraz 45 tysięcy euro i trzech lat więzienia, jeśli skutkiem anoreksji byłaby śmierć [*Nie dla promowania anoreksji*]. Inne państwa również planują takie działania. Podobnym ruchem jest ruch pro-mia (pro bulimia).

Kolejną dużą grupą zagrożeń bezpieczeństwa społecznego związanego z cyberprzestrzenią są zagrożenia finansowe i prawne. Uzależnienie od e-czynności (e-gier, e-hazardu i e-zakupów) może prowadzić do problemów finansowych, będących bezpośrednim (nadmierne wydawanie, przegrane) lub pośrednim efektem wykonywania danej e-czynności (długi, spirala zadłużenia). Tymi samymi konsekwencjami uzależnienia mogą być problemy z prawem, działanie na pograniczu prawa lub łamanie zasad współżycia społecznego. Zdarzają się osoby, które w celu pozyskania pieniędzy wchodzą w konflikt z prawem albo podejmują decyzje i zajęcia ryzykowne (prostytucja, kradzieże, przemyt, udostępnianie swoich danych osobowych do czynności niezgodnych z prawem) [Styśko-Kunkowska, Wąsowicz 2014: 29–39, 42–45].

Małgorzata Styśko-Kunkowska i Grażyna Wąsowicz [2014: 9], powołując się na prace Ogińskiej-Bulik [2010], Woronowicza [2009] i Guerreschiego [2010] wskazały, że pojawiły się badania wskazujące na wspólne cechy zwiększające

prawdopodobieństwo uzależnienia nie tylko od samego surfowania w sieci, ale także od e-hazardu i e-zakupów:

- coraz bardziej powszechny dostęp, a także dostęp w każdej chwili i bez wychodzenia z domu (również przez urządzenia przenośne),
- anonimowość dająca poczucie bezpieczeństwa oraz pozwalająca na prezentowanie tożsamości i podejmowanie zachowań niemożliwych w rzeczywistości,
- swoboda ekspresji,
- równość pod względem statusu społecznego,
- możliwość zamaskowania rzeczywistego wyglądu fizycznego.

Agresja i przemoc rówieśnicza w Internecie to kolejne typy zagrożeń, takie jak *cyberbulling*, *cyberstalking*, *happyslaping*, *flaming* czy *trolling*. *Cyberbulling* to „wykorzystanie technik informacyjnych i komunikacyjnych do świadomego, wielokrotnego i wrogiego zachowania się osoby lub grupy osób, mającego na celu krzywdzenie innych" [Wojtasik 2009]. Z kolei *cyberstalking* to uporczywe i niesprowokowane przez ofiarę działanie, groźby i nękanie [Goth 2010]. *Happy slapping* polega na prowokowaniu lub atakowaniu innej osoby wraz z dokumentowaniem zdarzenia za pomocą filmu lub zdjęć, które są udostępniane w sieci [Pyżalski 2011]. Kolejne zagrożenie to *flaming*, czyli zamieszczanie serii wiadomości o celowo wrogim lub obraźliwym charakterze na forum, liście czy też grupie dyskusyjnej w internecie. I w końcu *trolling*, czyli świadome prowokowanie użytkowników do konfliktu przez publikowanie komunikatów mających spowodować wyzwolenie u nich negatywnych emocji. Z tymi zjawiskami można również powiązać dwa kolejne, które mogą, ale nie muszą mieć swoje źródła w dotychczas wymienionych zjawiskach. To cybersamobójstwa (ang. *net suicides*, *cybersuicide*) i cała subkultura związana z licznymi stronami internetowymi i forami, na których młodzi ludzie zachęcają się nawzajem do popełniania samobójstw, zawiązują pakty, w których zobowiązują się do wspólnego popełnienia samobójstwa i opisują metody, jakimi można je popełnić – 480 stron internetowych dotyczących samobójstw, z czego 45 stron zachęcało do samobójstwa (*pro-suicide*) i 43 strony opisywały metody samobójstw [Drzewiecki 2011]. Najgłośniejsze i najliczniejsze wypadki tego typu zanotowano w Japonii, gdzie rocznie dochodzi do około 60 takich przypadków [*Cybersuicide and the adolescent population* 2009].

KONKLUZJE

Przedstawione zagrożenia oczywiście nie wyczerpują katalogu możliwych konsekwencji funkcjonowania społeczeństw w cyberprzestrzeni, tym bardziej że rozwój technologii informatycznych znacznie przyspiesza, nie dając czasu na utrwalenie i refleksję nad istotą zmian. Bezpieczeństwo społeczne będzie w tym kontekście rozszerzającą się i niedomkniętą kategorią, w której będą się stykały problemy z pogranicza medycyny, psychologii, polityki społecznej, edukacji,

socjologii, prawa, informatyki i wielu innych. Tym bardziej na tak szeroko zakreślonej perspektywie należy skupić badania, które pozwolą sformułować diagnozę dotyczącą specyfiki przemian społecznych i w tym kontekście transgresji rozumienia bezpieczeństwa. Zagrożenia bezpieczeństwa społecznego związane z funkcjonowaniem w cyberprzestrzeni to wyzwanie dla autorów zajmujących się tą problematyką oraz praktyków różnych dziedzin, przed którymi stoi wyzwanie przewidzenia i prewencji potencjalnie niebezpiecznych zjawisk. Rozwój technologii informacyjnych jest procesem dynamicznym, wymagającym stałego monitorowania zmian i analizy zachodzących w związku z tym procesów. Ważnym elementem powinno być przemodelowanie systemu edukacji na każdym szczeblu, aby od najmłodszych lat kształcić użytkowników, którzy będą świadomi zarówno korzyści, jak i zagrożeń płynących z nowoczesnych technologii informacyjnych. Ważne jest także, aby wcześnie reagować na zmiany, które będą wymagały nieustannego podnoszenia kwalifikacji w tej dziedzinie.

Title: Threats to Social Security Related to Functioning in Cyberspace

Summary: The article attempts to capture basic elements related to threats to social security in cyberspace. Attention was paid to various categories of intersecting themes covering both health, legal, moral and educational risks. The subject of social security in cyberspace is a difficult research area because the speed and deepening penetration through virtual reality causes overlapping of various elements. Cyberspace and cybersecurity area are the challenge for authors dealing with this issue as well as practitioners of various fields facing the challenge of predicting and preventing potentially dangerous phenomena.

Keywords: cybersecurity, cyberspace, Internet, social security

BIBLIOGRAFIA

1. 2018 Q2 Global Digital Statshot (2015), *We are Social*, Hootsuite, https://wearesocial.com, [dostęp: 2.05.2018].
2. Bartosińska M., Ejsmont J., Tukalska-Parszuto M. (2001), *Chorobowość pracowników zatrudnionych na stanowiskach pracy wyposażonych w komputery*, „Medycyna Pracy", vol. 52, nr 3, s. 185–195.
3. *Bezpieczeństwo prawne. Nowy poziom bezpieczeństwa narodowego*, (2009), [w:] *Bezpieczeństwo wewnętrzne Rzeczpospolitej Polskiej na tle innych państw Unii Europejskiej. Stan obecny oraz perspektywy zmian*, Józefów, Wyższa Szkoła Gospodarki Euroregionalnej, s. 363–378.
4. Birba R.l., Birba R.l., lapperton M., Jarvis J., Ragoonath A., Uppalapati K., Maharajh H.D. (2009), *Cybersuicide and the adolescent population: Challenges of the future?,* https://www.researchgate.net/publication/26762475_Cybersuicide_and_the_adolescent_population_Challenges_of_the_future, "International Journal of Adolescent Medicine and Health" 21(2):151-9 • April 2009, p. 1–8 [dostęp: 20.05.2018].
5. Buzan B., Wæver O., de Wilde J. (1998), *Security a New Framework for Analysis*, Boulder, s. 27.

6. Cudo A., Stróżak P., Kopiś N. (2016), Raport z projektu badawczego „*Specyfika funkcjonowania poznawczego osób uzależnionych od Internetu oraz osób uzależnionych od gier komputerowych*", Lublin.
7. Drzewiecki P. (2011), *Samobójstwa nastolatków w Internecie w perspektywie pedagogiki mediów*, „Kultura, Media, Teologia", nr 5, s. 61–73.
8. Dworecki S. (2002), *Zagrożenia bezpieczeństwa państwa*, Warszawa 2002, s. 61.
9. Fergus T.A. (2013), *Cyberchondria and Intolerance of Uncertainty: Examining When Individuals Experience Health Anxiety in Response to Internet Searches for Medical Information*, „Cyberpsychology, Behavior, and Social Networking", vol. 16, no. 10, https://www.liebertpub.com/doi/10.1089/cyber.2012.0671 [dostęp: 20.05.2018]. DOI: https://doi.org/10.1089/cyber.2012.0671.
10. Frei D. (1977), *Sicherheit Grundfragen der Welpolitik*, Stuttgart, s. 17–21.
11. Furmanek W. (2014), *Zagrożenia wynikające z rozwoju technologii informacyjnych*, „Dydaktyka Informatyki", nr 9, s. 20–48.
12. Groth J. (2010), *Cyberstalking — perspektywa psychologiczna*, „Forum Oświatowe", nr 2, vol. 43, s. 85–98.
13. Hoall A., Parsons J. (2001), *Internet Addiction: Collage Student Case Study Using Best Practices in Cognitive, Therapy*, „Journal of Mental Health Counseling", nr 23, s. 312–327.
14. *Internet usage statistics. The Internet Big Picture, World Internet Users and 2018 Population Stats*, (2018), https://www.internetworldstats.com/stats.htm, [dostęp: 26.04.2018].
15. Konieczniak M. (2011), *Poszukiwanie tożsamości w cyberprzestrzeni. Implikacje pedagogiczne*, „Edukacja i Dialog", nr 5/6, s. 8–19.
16. Leszczyński M. (2011), *Bezpieczeństwo społeczne Polaków wobec wyzwań XXI wieku*, Warszawa, s. 14.
17. Lévy P. (2018), *Drugi potop*, http://www.tezeusz.pl/cms/tz/index.php?id=287 [dostęp: 6.05.2018].
18. Majer P. (2012), *W poszukiwaniu uniwersalnej definicji bezpieczeństwa wewnętrznego*, „Przegląd Bezpieczeństwa Wewnętrznego", nr 7, vol. 12, s. 11.
19. Masuda Y. (1981), *The Information Society as Post-industrial Society. Institut for the Information Society*, Tokyo.
20. *Nie dla promowania anoreksji,* (2008), http://wiadomosci.gazeta.pl/wiadomosci/1,114881,5123540.html [dostęp: 20.05.2018].
21. Nowina-Konopko M. (2006), *Istota i rozwój społeczeństwa informacyjnego*, [w:] *Społeczeństwo informacyjne. Istota, rozwój, wyzwania*, Warszawa, s. 14.
22. Pietraś M. (1996), *Bezpieczeństwo ekologiczne w Europie*, Lublin, s. 21–27.
23. Polski Internet w marcu 2018, (2018), Badanie Gemius PBI z 10 marca 2018, http://pbi.org.pl/badanie-gemius-pbi/polski-internet-marcu-2018/ [dostęp: 20.05.2018].
24. *Prezentacja treści seksualnych przez młodzież poprzez wideoczaty. Badania*, dyżur.net, NASK, (2013) Research.nk [dostęp: 13.06.18].
25. *Public Health Implications of Excessive Use of the Internet, Computers, Smartphones and Similar Electronic Devices*, (2014), Meeting report Main Meeting Hall, Foundation for Promotion of Cancer Research, https://apps.who.int/iris/handle/10665/184264 [dostęp: 23.05.2018].
26. National Cancer Research Centre, Tokyo, Japan 27–29 August 2014, s. 13–14, http://apps.who.int/iris/bitstream/handle/10665/184264/9789241509367_eng.pdf;jsessionid=BCA387AB1E-3B406E91F8046F9FBCEEF9?sequence=1 [dostęp: 21.05.2018].

27. Pyżalski J. (2011), *Agresja elektroniczna wśród dzieci i młodzieży*, Gdańsk, s. 97–98.
28. Raport Newspoint: *Pokolenia w Polsce i potrzeba monitorowania ich rosnącej aktywności*, (2018), https://blog.newspoint.pl/index.php/2018/03/21/raport-newspoint-pokolenia-w-polsce-i-potrzeba-monitorowania-ich-rosnacej-aktywnosci/, [dostęp: 12.06.2018].
29. Rutkowski C. (2010), *Bezpieczeństwo wewnętrzne. Tożsamość – kierowanie – zarządzanie*, Warszawa, s. 7.
30. Skrabacz A. (2012), *Bezpieczeństwo społeczne. Podstawy teoretyczne i praktyczne*, Warszawa, s. 38.
31. Small G., Vorgan G. (2011), *iMózg. Jak przetrwać technologiczną przemianę współczesnej umysłowości*, Poznań.
32. Szpunar M. (2004). *Społeczności wirtualne jako nowy typ społeczności – eksplikacja socjologiczna*, „Studia Socjologiczne", nr 2 (173), s. 95–130.
33. Środek I. (2011), *Motyle w sieci. Krótka charakterystyka ruchu pro-ana*, „Current Problems of Psychiatry" nr 12 (3), s. 322–329, http://www.psychologia.net.pl/artykul.php?level=461 [dostęp: 20.05.2018].
34. Tanaś M. (1993), *Medyczne skutki uboczne kształcenia wspomaganego komputerowo*, „Toruńskie Studia Dydaktyczne", s. 107–109.
35. *United Nations Development Program Human Development Report 1994*, (1994), New York, s. 22.
36. *Uzależnienia od e-czynności wśród młodzieży: diagnoza i determinanty. Raport*, (2014), M. Styśko-Kunkowska, G. Wąsowicz (oprac.), s. 9–10, www.kbpn.gov.pl/portal?id=15&res_id=5064290 [dostęp: 20.05.2018].
37. Wallis D. (1997), Just Click No. January 1997 „The New Yorker", s. 28. https://www.newyorker.com/magazine/1997/01/13/just-click-no [dostęp: 21.05.2018].
38. Wojtasik Ł. (2009), *Przemoc rówieśnicza z użyciem mediów elektronicznych — wprowadzenie do problematyki*, „Dziecko Krzywdzone. Teoria, badania, praktyka", vol. 26, nr 1, s. 8.
39. Wojtasik Ł. (2014), *Seksting wśród dzieci i młodzieży*, „Dziecko Krzywdzone. Teoria, badania, praktyka", vol. 13, nr 2, s. 78.
40. Yapp R. (2012), *Three-quarters of British children aged 10 own a mobile phone – twice as many as overseas*, http://www.dailymail.co.uk/news/ article-2198450/Three-quarters-British-children-aged-10-mobile-phone--twice-overseas.html#ixzz358DpOqIL [dostęp: 20.05.2018].
41. Young K.S. (1998), *Internet addiction: the emergence of a new clinical disorder*, „Cyber Psychology and Behavior", nr 1, s. 237–244. DOI: https://doi.org/10.1089/cpb.1998.1.237.
42. Zięba R. (1999), *Instytucjonalizacja bezpieczeństwa europejskiego*, Warszawa, s. 28.
43. Zięba R. (2012), *O tożsamości nauk o bezpieczeństwie*, „Zeszyty Naukowe AON", nr 1 (86), s. 9–11.