dr Julia Nowicka
Akademia Sztuki Wojennej
Wydział Wojskowy
ORCID: 0000-0002-0778-0519

prof. dr hab. inż. Yury Pauliuchuk
Wydział Nauk Społecznych
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
ORCID: 0000-0002-2077-5124

WYBRANE ELEMENTY BEZPIECZEŃSTWA SPOŁECZNEGO W CYBERPRZESTRZENI

SELECTED ELEMENTS OF SOCIAL SECURITY IN CYBERSPACE

Streszczenie
Zakres pojęciowy cyberprzestrzeni jest bardzo szeroki stąd stanowi wyzwanie zarówno dla analizy badawczej, jak i interpretacji. Główne cechy cyberprzestrzeni to m.in. globalny zasięg, wydajność, uniwersalność a w szczególności taniość w dostępie. Czynniki te powodują, że kolejne dziedziny życia społecznego są przenoszone do świata wirtualnego. Możliwości cyberprzestrzeni ulegają ciągłemu rozwojowi i pojawia się coraz więcej bardziej doskonałych i innowacyjnych rozwiązań teleinformatycznych. Obok ogromnych korzyści, jakie niesie za sobą informatyzacja, w tym dostęp do informacji i wiedzy wyrównujący w pewnym stopniu szanse edukacyjne, pojawiają się istotne nieznane wcześniej zagrożenia, które dotykają wszystkich grup społecznych. Zarówno korzyści wynikające z wykorzystywania zasobów cyberprzestrzeni, jak i zagrożenia w jej funkcjonowaniu sprawiają, że problematyka cyberprzestrzeni i bezpieczeństwa stały się przedmiotem badań, a także regulacji prawnych, tworzących podstawy pod kształtowanie się nowej dyscypliny naukowej. W rozdziale podjęto próbę identyfikacji, analizy i oceny zagrożeń wynikających z korzystania z cyberprzestrzeni.

Słowa kluczowe: atak, cechy, cyberprzestrzeń, strategia, zasięg

Abstract
The conceptual scope of cyberspace is very widely understood. It also appears that the term can be the most challenging for both research analysis and interpretation. The main features

of cyberspace include global reach, efficiency, universality and especially cheapness of access. These factors cause more areas of social life to be transferred to the virtual world. The possibilities of cyberspace are constantly developing and more and more perfect and innovative ICT solutions appear. In addition to the enormous benefits of computerization, including access to information and knowledge that equalizes educational opportunities to some extent, there are significant previously unknown risks that affect all social groups. Both benefits of cyberspace and threats to its functioning make the issues of cyberspace and security in it have become the subject of research, as well as legal regulations, creating the basis for the formation of a new scientific discipline. The chapter attempts to identify, analyze and assess the threats resulting from the use of cyberspace.

Keywords: attack, features, cyberspace, strategy, range

Wstęp

Współczesne funkcjonowanie człowieka trudno jest oddzielić od wirtualnej rzeczywistości. Stała się ona płaszczyzną komunikacji, ale też umożliwiła wymianę usług, co nadaje jej walor powszechności i uniwersalności. Specyfika ta nie dotyczy tylko krajów rozwiniętych, ale pośrednio – całej cywilizacji. Początek rozważań o cyberprzestrzeni naznaczył ją jako (...) *konsensualną halucynację, doświadczaną każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach, przez dzieci nauczane pojęć matematycznych* (...). *Graficzne odwzorowanie danych z banków wszystkich komputerów świata. Niewyobrażalna złożoność* (...)[1]. Mimo iż przytoczona definicja pochodzi z dzieła literackiego, nie tylko dała początek wielkiej debacie nad istotą cyberprzestrzeni, lecz także wskazała podstawowe elementy, które dotyczą tego osobliwego środowiska: rozległość (zasięg światowy), spajanie wszelkich zasobów w jedną, olbrzymią bazę danych, złożoność oraz bezprzestrzenność rozumianą jako brak możliwości odniesienia cyberprzestrzeni do fizycznych (w tym geograficznych) wymiarów realnego świata. W literaturze przedmiotu cyberprzestrzeń określa się jako ogół powiązań o charakterze wirtualnym, nie dającym się zawrzeć w fizycznie obserwowalną, ograniczoną wymiarami przestrzeń, istniejącą jednak dzięki fizycznym atrybutom takim jak komputery, infrastruktura telekomunikacyjna itp.[2] Cyberprzestrzeń to rzeczywistość ludzkiego funkcjonowania z udziałem technologii informacyjnych i komunikacyjnych. Jest płaszczyzną działania m.in. systemów transportu, łączności, infrastruktury energetycznej, wodociągowej i gazowej oraz tej związanej z ochroną zdrowia. Odnosi się to do systemów komputerowych, możliwości i specyfiki przesyłu różnego rodzaju danych, zapewniając funkcjonowanie jednostek, ale i instytucji, co ma zasadnicze znaczenie dla zachowania bezpieczeństwa państwa.

Odnosząc się nomenklatury narodowej o cyberprzestrzeni jest mowa w ustawie nowelizującej regulacje prawne stanów nadzwyczajnych z 2011 r. *Przez cyberprzestrzeń, o której mowa w ust. 1, rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących*

[1] W. Gibson, *Neuromancer*, Ace Books, New York 1984, s. 58.

[2] M. Madej, *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, [w:] M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Polski Instytut Spraw Międzynarodowych, Warszawa 2009, s. 28.

zadania publiczne, wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami[3]*.* Cechą wspólną rozumienia cyberprzestrzeni jest tu zatem jedna płaszczyzna, w której wytwarza się, wprowadza, modyfikuje i monitoruje dane oraz informacje.

Przestrzeń wirtualną (cyber) traktuje się jako równoległy wymiar ludzkich działań we współczesnym życiu społecznym. Jej dominującym elementem jest sieć Internet, z uwagi na powszechność użycia i szereg innych zalet. Nie są one w pełni tożsame z czynnościami podejmowanymi w realnej rzeczywistości, co stanowi o ich specyfice i jest czynnikiem różnicującym oba wymiary funkcjonowania człowieka. Niezależnie od lokalizacji, w jednym momencie elementy systemu mają dostęp do tych samych zasobów w ramach określonych uprawnień, statusów. Kolejnymi cechami świadczącymi o uniwersalności są możliwe anonimowość i względnie niskie koszty dostępu do strefy cyber, co jest specyfiką zarówno w wymiarze psychospołecznym jak i tym obejmującym całość fizycznych i technicznych odniesień, reprezentowanych przez odpowiednie programy, sieci, systemy, które stanowią składową cyberprzestrzeni.

Według National Strategy to Secure Cyberspace cyberprzestrzeń stała się *systemem nerwowym państwa: (...) nasza gospodarka i bezpieczeństwo narodowe stały się w pełni zależne od technologii i infrastruktury informatyczne*j[4]. Podsumowując można stwierdzić, że cyberprzestrzeń charakteryzuje się następującymi cechami:

- niezależnością od miejsca;
- niezależnością od odległości;
- niezależnością od czasu;
- niezależnością od granic;
- względną anonimowością;
- możliwością ustalenia sprzętu, nie osoby[5].

Badając cyberprzestrzeń na początku XXI wieku w zakresie edukacji dominowało stanowisko wskazujące konieczność przeciwdziałania zagrożeniom. Pojawiające się dane o kryzysach i potencjalnie negatywnych skutkach, wymuszały dyskusję o konieczności ochrony użytkowników sieci. Wydawać by się mogło, że małoletni użytkownicy sieci w sposób zupełnie naturalny przyjęli cyberśrodowisko za własne, ale przeczą temu badania. W ramach projektu EU Kiks Online wykazano, że tylko kilkanaście procent dzieci (do 17 roku życia) specyfikę świata wirtualnego przedkłada nad wymiar realny. *Mniej niż 16% czuło (często lub zawsze), że w Internecie jest im łatwiej być sobą. Nieco mniej niż 17% rozmawiało*

[3] *Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw* (Dz.U. Nr 222, poz. 1323).

[4] T. R. Aleksandrowicz, *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, „Przegląd Bezpieczeństwa Wewnętrznego", nr 8/2016, s. 12.

[5] Ibidem, s. 13.

w Internecie o innych rzeczach, niż spotykając się w „realu" twarzą w twarz, a 7% o sprawach osobistych, których nie poruszali offline[6].

Współczesna literatura przedmiotu coraz częściej obfituje w obszar wzmacniania kompetencji użytkowania, które prowadzą do rozwoju i udogodnień funkcjonowania współczesnego człowieka, obywatela. Wydaje się, że pozytywny trend edukacji wzmacnia świadomość wielowymiarowości świata wirtualnych możliwości i zagrożeń.

Zagrożenia w cyberprzestrzeni

Korzystanie z wirtualnych możliwości funkcjonowania w środowisku społecznym stworzyło nowe szanse porozumiewania się, dzięki czemu powstały np. nowe profesje, branże biznesu itp. Jednak masowość działań uruchomiła potrzebę kierowania niektórymi aktywnościami, a to w swej negatywnej odsłonie rodzi możliwość cyberinwigilacji. Może być ona dokonywana zarówno na poziomie państwowym (działalność określonych służb względem obywateli), jak i może dotyczyć określonych potentatów w sferze np. ekonomii. Ponieważ sieć jest przestrzenią globalną o charakterze inkluzywnym, z jej zasobów i możliwości korzystają grupy przestępcze czy terrorystyczne. Potencjalni przestępcy z racji tego, iż są w większości anonimowi w sieci czują się praktycznie bezkarni a osoby poszkodowane bezradne. Ofiarami zjawisk groźnych, generowanych przez Internet mogą być zarówno młodzi odbiorcy jak i dorosłe osoby[7].

Zjawiska niekorzystne dla rozwoju i funkcjonowania człowieka, związane z jego uczestnictwem w cyberspołeczności niekoniecznie muszą być związane z przestępczością i przemocą zewnętrzną. Podkreślanym przez ekspertów obszarem problemowym, który dotyka najwięcej osób jest uzależnienie od Internetu. W latach 90. XX wieku nowojorski psychiatra – dr Ivan Goldberg określił cechy sieciozależności, choć jeszcze na nadał definicji temu zjawisku. Przedkładanie codziennego, regularnego, kiklugodzinnego korzystania z Internetu, nad aktywność realną związaną z budowaniem relacji międzyludzkich, życia zawodowego, społecznego, rodzinnego i kosztem zdrowia fizycznego i psychicznego, stało się istotą zjawiska uzależnienia od Internetu. Wskazana działalność z jednej strony przynosi chwilowe zadowolenie i przyjemność, które w początkowej fazie pozostają pod pełną kontrolą użytkownika, jednak z czasem zakres tej kontroli na poziomie emocjonalnym przestaje mieć siłę oddziaływania. Świat zewnętrzny przestaje dostarczać bodźców w dostatecznym stopniu, zaś potrzeba bycia „online" staje się dominująca. W zaawansowanych przypadkach uzależnieni wolą ograniczać czas

[6] J. Pyżalski, A. Zdrodowska, K. Abramczuk, Ł. Tomczyk, Polskie badanie EU KIDS, Wydawnicto Naukowe UAM 2018, https://fundacja.orange.pl/files/user_files/EU_Kids_Online_2019_v2.pdf, s. 26. [dostęp: 23.11.2020].

[7] P. Sienkiewicz, *Terroryzm w cybernetycznej przestrzeni*, [w:] T. Jemioło, J. Kisielniecki, K. Rajchel. (red.), *Cyberterroryzm – nowe wyzwania XXI wieku*, Wyższa Szkoła Informatyki, Zarządzania i Administracji, Warszawa 2009, s. 46.

snu, konsumpcji, higieny, by tylko móc kontynuować aktywność za pomocą narzędzi cyber. Mówi się wtedy o fazie destrukcyjnej *uzależnienia od Internetu i może się ona niekorzystnie odbijać na stanie zdrowia osoby uzależnionej*[8].

Zagrożeniem, które dotyka ogromną grupę użytkowników Internetu są różnego rodzaju wirusy. Można zarazić komputer lub smartfon zupełnie nieświadomie, klikając w nieznany link lub otwierając zainfekowaną wiadomość pocztową czy post. Wirusy, czyli złośliwe oprogramowanie atakujące komputery i telefony, dostają się do urządzeń najczęściej właśnie przez Internet. Ich szkodliwe działanie umożliwia m.in.:

- wykradnie poufnych informacji;
- zniszczenie danych, znajdujących się na dysku;
- za pomocą adresu e-mail wysyłanie spamu do posiadanych kontaktów, bez zgody i świadomości właściciela danego konta;
- zaszyfrowanie danych i wymuszanie okupu za ich odszyfrowanie,
- sprawdzanie historii przeglądania i wymuszania okupu, jeśli np. w historii widnieją serwisy kompromitujące właściciela;
- wysyłanie płatnych smsów typu premium z przejętego telefonu;
- przekazywanie informacji o położeniu użytkownika telefonu lub komputera osobom trzecim itp.

Innym zagrożeniem dla osób korzystających z Internetu jest publikowanie w nim danych wrażliwych określonych osób np. daty urodzenia, miejsca zamieszkania, statusu rodzinnego, statusu społecznego, miejsca pracy czy numeru telefonu. Pozyskane dane wrażliwe mogą służyć do różnego rodzaju operacji niezgodnych z prawem, co wiąże się z np. z zaciąganiem nielegalnych kredytów oraz innymi oszustwami czy sprzedażą danych osobom zamieszanym w proceder przestępczy. Z kradzieżą tożsamości użytkownik Internetu ma do czynienia, wówczas, gdy ktoś bezprawnie wejdzie w posiadanie danych osobowych i wykorzysta je wbrew woli użytkownika, głównie dla zdobycia własnych korzyści. Kradzież tożsamości pozornie wydaje się błahym zjawiskiem, jednak osoba, która ma dostęp do danych, może przysporzyć wielu kłopotów, które mogą dotoczyć np.:

- utworzenia w Internecie fałszywy profil;
- umieszczania w sieci lub wysyłania drogą elektroniczną obraźliwych komentarzy w imieniu danego użytkownika;
- zaciągania zobowiązań finansowych, np. kredytów w banku;
- dokonania zakupów w imieniu okradzionego użytkownika.

O jestestwie człowieka wg niektórych teorii decyduje społeczny charakter relacji, związany z koniecznością funkcjonowania wspólnotowego. Zwłaszcza niedobory jakościowe w interpersonalnych kontaktach w realnej rzeczywistości popychają jednostki do budowania znajomości w sieci. Sprzyja temu tendencja do możliwego odświeżonego, ulepszonego prezentowania siebie nieznanym cyberużytkownikom. Choć jakość opisywanych relacji jest zupełnie inna niż kontaktów

[8] E. Krzyżak-Szymańska, *Uzależnienia technologiczne wśród dzieci i młodzieży. Teoria, profilaktyka, terapia – wybrane zagadnienia*, Oficyna Wydawnicza „Impuls", Kraków 2018, s. 49.

bezpośrednich, to jednak siła więzi (rzeczywistej czy wyobrażonej) może angażować w znacznie silniejszy sposób niż dotychczas. Rodzi to oczywiście zagrożenie na poziomie intra i interkomunikacji. Możliwe wycofanie się z życia społecznego, brak siły, ochoty i motywacji przeciwstawiania się trudom życiowym wciągają w wymiar cyber, który z czasem staje się łatwiejszy do funkcjonowania, gdyż pozornie umożliwiający kontrolę sytuacji i zdarzeń. Jednym z patologicznych zachowań nałogowo częstych rozmów w mediach społecznościowych może być właśnie opisany machanizm konformistycznego uzaleznienia[9].

Anonimość i zatopienie w podstawowych błędach atrybucji umożliwiają rozprzestrzenianie się szeregu odmianom nękania internetowego. Co obrazują angielskobrzmiące pojęcia takie jak:

- cyberbulling – związany z powtarzalnym, świadomym i negatywnym działaniem komunikacyjnym w sferze cyber[10];
- cyberstalking – notoryczne, intensywne wysyłanie krzywdzących treści o charakterze zastraszania, które z różnych kanałów komunikacji cyfrowej zaburzają poczucie bezpieczeństwa u ofiary. Warto tutaj wspomnieć, że stalking traktowany jako napastliwe nękanie podlega regulacjom prawnym na mocy kodeksu karnego: *Kto przez uporczywe nękanie innej osoby lub osoby jej najbliższej wzbudza u niej uzasadnione okolicznościami poczucie zagrożenia, poniżenia lub udręczenia lub istotnie narusza jej prywatność, podlega karze pozbawienia wolności od 6 miesięcy do lat 8*[11]*;*
- happy slapping – umieszczanie w sieci, bez zgody uczestników nagrania, określonych materiałów audiowizualnych z udziałem poszkodowanego w celu ośmieszenia go, obrażenia, zdyskredytowania lub innej negatywnej reakcji;
- flaming – związany jest z budowaniem i kierowaniem negatywnej dyskusji, komentarzy, opinii na określonych forach dyskusyjnych itp. Istotą jest napędzanie obraźliwych, prześmiewczych, konfliktowych treści, jak przy zjawisku kuli śnieżnej, by to one dominowały w aktywności i przyćmiły, pierwotny, początkowy temat rozmowy.

Dokładna charakterystyka zagrożeń nie jest łatwa do określenia i analizy badawczej. Wydaje się jednak, że można zauważyć pewne wspólne elementy niezależne od kategorii klasyfikacji. Należą do nich po pierwsze negatywne intencje kluczowych nadawców. Pierwotnie umieszczona we wspólnej przestrzeni cyfrowej (kolejny wspólny element) informacja ma na celu wyrządzenie krzywdy. Fakt, że początkowa informacja często jest rozprzestrzeniana w późniejszym etapie przez niektórych nieświadomie, z ciekawości, tendencji konformistycznych, nie zmienia czołowej negatywnej intencji nadawczej. Cecha wspólną form mobbingu cyfrowego jest też regularność bądź niepowtarzalność emitowanych sygnałów negatywnych, nagrań, wiadomości, postów itp. Mnogość incydentów lub informa-

[9] S. Kozak, *Patologie komunikowania w Internecie*, Wydawnictwo Difin, Warszawa 2011, s. 167–185.

[10] Ł. Wojtasik, *Przemoc rówieśnicza z użyciem mediów elektronicznych – wprowadzenie do problematyki*, „Dziecko Krzywdzone", 1/2009, s. 8.

[11] *Ustawa z dnia 6 czerwca 1997 r. Kodeks karny* (Dz. U. 1997 Nr 88 poz. 553), art.190a. § 1.

cji w wyniku udostępniania za każdym razem dodaje wagi, tworząc każdorazowo nowy czynnik stresogenny, nie wspominając już o sile oddziaływań wyobrażeniowych, czyli przeświadczeniu ofiary, że wszyscy z jej otoczenia wiedzą o danym zdarzeniu i oceniają je negatywne. W takiej sytuacji prócz stygmatyzacji, bolesnego naznaczenia społecznego poszkodowanemu towarzyszy negatywna autoocena i utrata wiary w możliwość normalnego funkcjonowania. Z powyższych uwarunkowań wynika kolejna cecha przemocy elektronicznej związana z zaburzeniem równowagi sił stron poszkodowanego i agresora (agresorów).

Ludzka potrzeba funkcjonowania w środowisku z innymi przedstawicielami gatunku, budowanie swojej tożsamości w oparciu o przynależność grupową są mechanizmami wykorzystywanymi przez grupy przestępcze, sekty czy organizacje terrorystyczne.

W wielu przypadkach konsekwencje omawianych zjawisk doprowadzają do samobójstw, co jest ostatecznością zbyt częstą wśród poszkodowanych użytkowników sieci. Jak wskazują statystyki policyjne w 2019 roku w stosunku do lat poprzednich w każdej kohorcie wiekowej do 50 roku życia liczba zamachów samobójczych zwiększyła się[12], choć należy zaznaczyć, że brak jest dokładnych wskazań, co do motywów generowanych przez używanie cyberprzestrzeni. Zagrożeniem są też treści nakłaniające do samobójstw i wskazujące możliwości jego realizacji. Wszelkie formy nakłaniania do działań destrukcyjnych, rozumianych również jako rozpowszechnianie czy nakłanianie do rozpowszechniania, stosowania środków odurzających należą do zagrożeń społecznych w sieci.

Niezależnie od wieku użytkownika sieci, poczucie jego intymności jest istotnym i jednocześnie wrażliwym obszarem, stanowiącym częsty punkt ataku. Całe spektrum zagrożeń związanych z cielesnością człowieka, które w ramach nadużyć seksualnych zawsze towarzyszyły gatunkowi ludzkiemu, stanowi również współcześnie obraz cyberzagrożeń. Związane jest to z tzw. cybersekstingiem. Można tutaj mówić o z pozoru niewinnym tworzeniu, przesyłaniu czy gromadzeniu tzw. roznegliżowanych obrazów o różnym stopniu natężenia ordynarności. Od niewinnych fotografii po tzw. twardą pornografię. Mimo zakazu działań pornograficznych internet staje się patogennym obszarem działalności pedofilskiej[13].

Jednocześnie sieć jest wykorzystywana nieświadomie lub zupełnie dobrowolnie transakcji, których obiektem jest ciało.

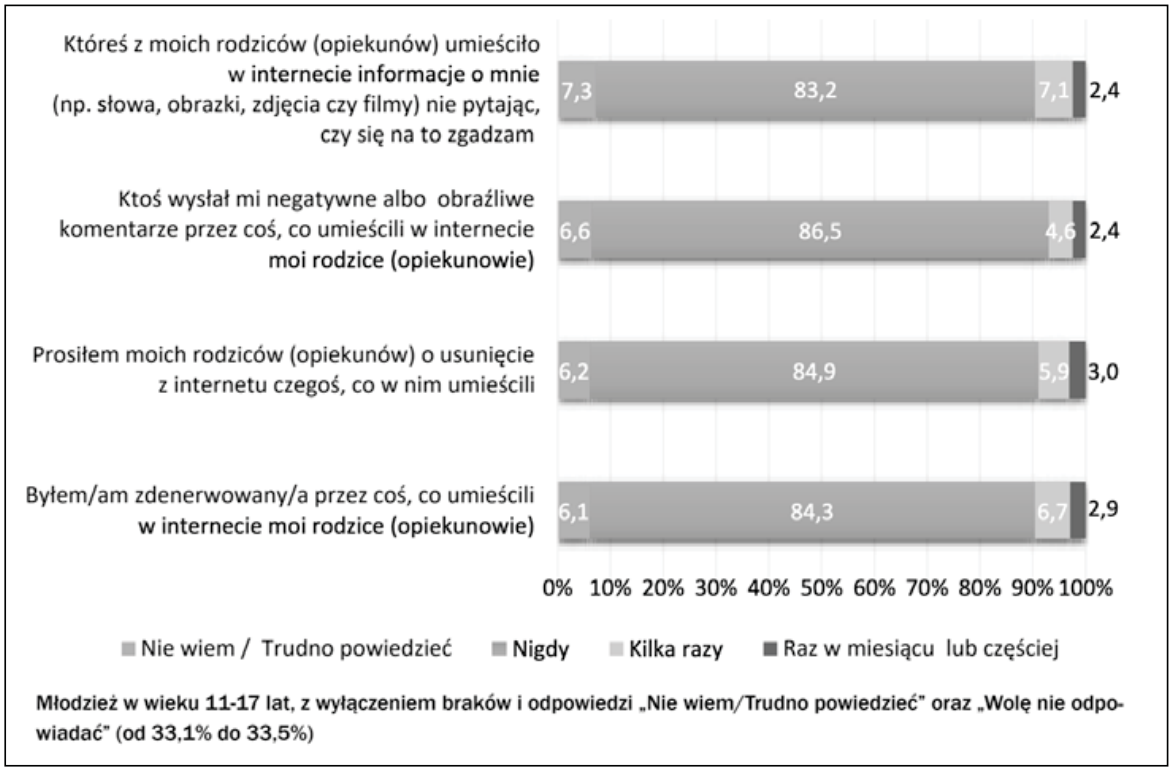
Równoległa do realnej, przestrzeń wirtualna sprzyja powstawaniu i rozprzestrzenianiu się zagrożeń zarówno wśród dzieci, dorastającej młodzieży, dorosłych i dojrzałych już członków społeczności ludzkiej. Środowisko zewnętrzne w świecie cyber, zlokalizowane poza określoną jednostką, instytucją, generuje niebezpieczeństwa podobnie jak wymiar intra, związany ze stabilnością psychofizyczną jednostki.

[12] Statystyki policyjne, file:///Users/darslowa/Desktop/zamachy_samobojcze_grupa_wiekowa_dzien_tygodnia_2017-2019%20(1).pdf, [dostęp 20.11.2020 r.].

[13] J. Carr, *Internet a wykorzystywanie seksualne dzieci i pornografia dziecięca*, „Dziecko Krzywdzone", 4/2005, s. 9.

W ogólnoeuropejskich badaniach nad bezpieczeństwem funkcjonowania dzieci w strefie cyber z 2018 r. poruszano zagadnienia, które nakreślają charakter współczesnego młodego cyberużytkownika. Abstrahując obszar Polski można na podstawie reprezentatywnej próby 1249 uczniów z 90 szkół stwierdzić, że młodzi ponad 82,5% codziennego kontaktu ze światem cyfrowym realizują przez telefon[14]. Z przedstawionych badań wyciągnięto następujące wnioski[15]:

- około co trzeci młodociany radzi się, kontaktuje z rodzicami w sprawie nurtujących go problemów w Internecie, jednak im starsze dziecko tym konsultacja z rodzicami jest coraz mniejsza;
- warto zaznaczyć rolę rodziców w świadomym edukowaniu nieletnich, co do zaistniałych zagrożeń, związanych z niebezpieczeństwem generowanym właśnie przez opiekunów. Reakcje nieletnich na wskazane zjawisko sharentingu przedstawiono na wykresie nr 1.



Wykres nr 1. Reakcja nieletnich na publikowane przez rodziców w Internecie treści dotyczących ich dzieci

Źródło: J. Pyżalski, A. Zdrodowska, K. Abramczuk, Ł. Tomczyk, Polskie badanie EU KIDS, Wydawnicto Naukowe UAM 2018, https://fundacja.orange.pl/files/user_files/EU_Kids_Online_2019_v2.pdf, s. 70. [dostęp: 23.11.2020].

Prawie co dziesiąty nieletni odczuwa złość z powodu nieuzgodnionego z nim publikowania materiałów przez rodziców i prosił opiekunów o usuniecie tych danych z sieci, gdyż odczuwał skutki uboczne w postaci negatywnych i obraźliwych

[14] J. Pyżalski, A. Zdrodowska, K. Abramczuk, Ł. Tomczyk, *Polskie badanie EU KIDS*..., op. cit., s. 19-20.
[15] Ibidem, s. 50-80.

komentarzy. Lepiej zatem nie umieszczać audiowizualnych dokumentów swoich pociech bez zgody dzieci.

- należy zwiększyć poziom posiadanych kompetencji cyfrowych wszystkich użytkowników Internetu;
- prawie co czwarte dziecko w wieku 11–16 lat miało w Internecie kontakt z treściami, które mogą szkodzić jego kształtującemu się systemowi wartości, im starsze dziecko tym większe prawdopodobieństwo kontaktu z treściami o podłożu seksualnym;
- chłopcy częściej niż dziewczęta są obiorcami treści o charakterze seksualnym
- czynnikami generującymi tzw. mowę nienawiści są zagadnienia związane z wyznaniem, narodowością oraz ogólnie rozumianą aparycją.

Miejscem, gdzie można spotkać się z poważnymi zagrożeniami korzystając z internetu jest dark web. Dark web, nazywany też mrocznym internetem, to głęboko ukryta sieć istniejąca obok dobrze znanej sieci zindeksowanej. Google nie znajdzie jej witryn, YouTube nie odtworzy zamieszczonych tam nagrań. Na dark web nie można trafić przypadkowo, gdyż dostępność zasobów możliwa jest wyłącznie za pomocą specjalnego oprogramowania. W gęstwinie prywatnych sieci zapewniających poziom anonimowości nieosiągalny w sieci zindeksowanej kwitnie handel narkotykami i bronią, reklamują się płatni zabójcy i hakerzy, gotowi włamać się do komputera wroga, a najbardziej zdeprawowani dewianci mogą zaspokoić apetyt, ściągając najdziwniejsze materiały pornograficzne. Dark web definiuje się jako celowo ukryte zasoby internetu. Składa się z wielu rozproszonych węzłów działających lokalnie, niewidocznych i niedostępnych z poziomu Internetu[16]. Istnieją tam strony chwalące się sprzedażą narządów, inne z kolei oferują dostęp do prawdziwych walk gladiatorskich, które kończą się śmiercią jednego z zapaśników, świadczą też usługi morderstwa na zlecenie albo za odpowiednią opłatą dają możliwość oglądania tortur. Nie brakuje też takich, które zapewniają, że posiadają dostęp do testów przeprowadzanych na ludziach albo dostarczą filmy snuff kręcone na zamówienie. W dark webie można znaleźć witryny specjalizujące się w działalności czarnorynkowej (broń, narkotyki, fałszerstwa, dane bankowe, skradzione towary i karty kredytowe, zmiana tożsamości, usługi), nielegalne fora pornograficzne, serwisy torrentowe, strony opozycjonistów i hejterów politycznych oraz społeczności hakerskie. Do wielu dostęp jest możliwy tylko za zaproszeniem, więc ich zawartość pozostaje tajemnicą.

Uwarunkowania formalno-prawne ochrony cyberprzestrzeni

Dynamiczny rozwój zagrożeń i incydentów naruszających bezpieczeństwo systemów i sieci komputerowych oraz użytkowników korzystających z usług ofe-

[16] https://ksiazki.wp.pl/do-darknetu-nikt-nie-trafia-przypadkiem-to-raj-dla-zwyrodnialcow-6383365980756097a [dostęp 01.12.2020].

rowanych przez nowoczesne technologie informatyczne powoduje, że zachowanie bezpieczeństwa przestrzeni tworzonej przez te systemy, usługi, wraz z relacjami z użytkownikami – zwanej cyberprzestrzenią – jest obecnie jednym z istotniejszym problemów na poziomie krajowym i międzynarodowym w kontekście konieczności zapewnienia niezakłóconego funkcjonowania państw, gospodarki i społeczeństwa[17]. Obraz wielu zagrożeń płynących z cyberprzestrzeni determinuje konieczność prowadzenia skoordynowanych działań na poziomie krajowym, które będą angażowały zarówno administrację państwową, jak też innych interesariuszy w postaci: podmiotów gospodarczych w różnych sektorach (w szczególności będących częścią infrastruktury krytycznej, ale także średnich i małych przedsiębiorstw), sektora badawczo-naukowego, organizacji pozarządowych, czy wreszcie samych użytkowników cyberprzestrzeni.

Podstawą rozwoju krajowego systemu cyberbezpieczeństwa jest dokonanie pełnego wdrożenia i oceny funkcjonowania przepisów ustanawiających ten system, w powiązaniu z innymi przepisami, w szczególności z Ustawą z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2019 r. poz. 1398), Ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742), Strategią Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej. Rezultatem dokonanej oceny może być konieczność przygotowania niezbędnych zmian przepisów, usuwających bariery dla skutecznej wymiany informacji oraz skoordynowanego i niezakłóconego reagowania na incydenty.

W dniu 1 sierpnia 2018 r. Prezydent RP podpisał ustawę o krajowym systemie cyberbezpieczeństwa. Jej zapis jest spójny z dyrektywę Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa 2016/1148), tzw. Dyrektywa NIS. Ustawa została opublikowana w Dzienniku Ustaw RP 13 sierpnia 2018 r. i zaczęła obowiązywać po 14 dniach od jej ogłoszenia tj. od 28 sierpnia 2018 r. Pełne wdrożenie Dyrektywy NIS wymagało ponadto przyjęcia dwóch rozporządzeń Rady Ministrów: w sprawie uznania incydentu za poważny, jak i w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych. Celem ustawy o krajowym systemie cyberbezpieczeństwa było opracowanie uregulowań prawnych umożliwiających implementacje dyrektywy NIS oraz utworzenie efektywnego systemu bezpieczeństwa teleinformatycznego na poziomie krajowym. Krajowy system cyberbezpieczeństwa ma na celu zapewnienie swobodnego, niezakłóconego i bezpiecznego korzystania z wymiaru cyber na poziomie krajowym, w szczególności:

- niezakłóconego świadczenia usług kluczowych i usług cyfrowych,
- osiągnięcie odpowiednio wysokiego poziomu bezpieczeństwa systemów teleinformatycznych służących do świadczenia tych usług[18].

[17] I. Jarosz, P. Jaroszewki, P. Kijewski, *System bezpieczeństwa cyberprzestrzeni RP*, Naukowa Akademicka Sieć Koputerowa, Warszawa 2015, s. 3

[18] *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (Dz.U. 2018 poz. 1560).

System obejmuje operatorów usług kluczowych (m.in.: z sektora energetycznego, transportowego, zdrowotnego i bankowości), dostawców usług cyfrowych, zespoły CSIRT (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego) oraz inne podmioty realizujące działania w obszarze cyberbezpieczeństwa. Do obowiązków operatorów kluczowych należy m.in.: analiza ryzyka zdarzeń, wdrażanie zabezpieczeń, komunikowanie i współpraca z CSIRT poziomu krajowego.

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022 jest krajową strategią w zakresie bezpieczeństwa systemów teleinformatycznych w rozumieniu Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii zwanej dalej Dyrektywą NIS. W szczególności Strategia wskazuje:

- cele w zakresie bezpieczeństwa teleinformatycznego;
- główne podmioty zaangażowane we wdrażanie strategii w zakresie bezpieczeństwa teleinformatycznego;
- ramy zarządzania służące realizacji celów krajowej strategii w zakresie bezpieczeństwa teleinformatycznego;
- na potrzebę zapobiegania i reagowania w odniesieniu do incydentów oraz przywracania stanu normalnego zakłóconego incydentem, w tym zasady współpracy pomiędzy sektorami publicznym i prywatnym;
- podejście do oceny ryzyka;
- kierunki podejścia do programów edukacyjnych, informacyjnych i szkoleniowych dotyczących cyberbezpieczeństwa;
- działania odnoszące się do planów badawczo-rozwojowych w zakresie bezpieczeństwa teleinformatycznego;
- podejście do współpracy międzynarodowej w zakresie cyberbezpieczeństwa.[19]

Ta Strategia wprowadzona w drodze uchwały Rady Ministrów, oddziałuje w sposób bezpośredni na podmioty administracji rządowej, a w sposób pośredni, po przyjęciu z inicjatywy Rady Ministrów przepisów prawa powszechnego, na pozostałe podmioty władzy publicznej, przedsiębiorców i obywateli.

Strategia Cyberbezpieczeństwa RP na lata 2019-2024 została zaakceptowana przez Radę Ministrów w dniu 22 października 2019 r., a 29 października podpisał ją premier Mateusz Morawiecki[20]. Obowiązuje od 31 października 2019 roku. Strategia zastępuje Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022. Głównym celem Strategii jest podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym. Na lepszą ochronę informacji wpłynie też

[19] *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022* (załącznik 1 do uchwałę nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017), s. 17.

[20] *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024* (załącznik nr 1 do uchwały nr 125 Rady Ministrów z dnia 22 października 2019), s. 6.

promowanie wiedzy i dobrych praktyk wśród obywateli. W dokumencie określono pięć celów szczegółowych[21]:

1. Rozwój krajowego systemu cyberbezpieczeństwa.
2. Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty.
3. Zwiększenie potencjału narodowego w zakresie bezpieczeństwa w cyberprzestrzeni.
4. Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa.
5. Zbudowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa.

W ciągu pół roku od przyjęcia dokumentu Minister Cyfryzacji, przy współpracy z członkami Rady Ministrów, kierownikami urzędów centralnych, Dyrektorem Rządowego Centrum Bezpieczeństwa opracowało i przedstawiło Plan Działań na rzecz wdrożenia Strategii Cyberbezpieczeństwa. W Planie Działań zostały określone konkretne działania dla organów administracji rządowej, wraz z harmonogramem ich realizacji oraz miernikami pozwalającym ocenić stan realizacji poszczególnych działań. Z uwagi na wzrost zagrożeń ze strony sieci publicznych, od których całkowita separacja jest niemożliwa, a także fakt rozproszonej odpowiedzialności za bezpieczeństwo teleinformatyczne, niezbędne jest koordynowanie działań w zakresie zapobiegania i zwalczania zagrożeń ze strony cyberprzestrzeni, które umożliwią szybkie i efektywne reagowanie na ataki wymierzone przeciwko systemom, sieciom teleinformatycznym i oferowanym przez nie usługom[22].

Podsumowanie

Internet jest platformą wymiany informacji, miejscem rozrywki, nauki i pracy. Za pośrednictwem sieci dokonuje się transakcji finansowych, kupuje w wirtualnych sklepach i obsługuje konta bankowe. Powstanie i rozwój społeczeństwa informacyjnego przyniosły ze sobą – poza bezspornymi korzyściami – także wiele zagrożeń bezpieczeństwa państwa i jego obywateli. Większość z nich jest związana z rozwojem cyberprzestrzeni. Liczba zagrożeń, na jakie może być wystawiony każdy użytkownik cyberprzestrzeni, jest bardzo duża, a skala ich szkodliwości rośnie w związku ze zjawiskiem narastającej migracji do cyberprzestrzeni. Niebezpieczeństwa wynikające z funkcjonowania w cyberprzestrzeni są realnym zagrożeniem nie tylko dla dzieci, lecz także dla osób dorosłych.

W toku prowadzonych analiz wydaje się, że istotne są szeroko rozprzestrzeniane podstawy edukacyjne, co do użytkowania zasobów cyber i możliwości Internetu ze wskazaniem zarówno ryzyka z tym związanego, jak i szans rozwoju. Dotyczy

[21] Ibidem, s. 8-9.

[22] https://rekrutacja.apsl.edu.pl/Rekrutacja/oferta/Studia-1-stopnia/bezpieczenstwo-narodowe/ochrona-cyberprzestrzeni [dostęp 03.12.2020].

to powinności określonych instytucji, jaki środowiska domowego, gdzie nieustannie ogromną rolę ogrywają rodzice, jak i bliscy znaczący. W sferze oddziaływania publicznego istotne są regulacje normujące zasady reagowania na zdefiniowane zagrożenia. Znaczące stają się programy i strategie, mające na celu minimalizowanie zagrożeń płynących z Internetu oraz edukacja ludzi korzystających z sieci. Nikt nie jest w stanie zatrzymać rozwoju technologii informacyjnych i dlatego należy dostosowywać ludzi do określania i realizowania ich potrzeb i zasad współużytkowania w cyberprzestrzeni, ze świadomością globalnych konsekwencji, których źródła mogą mieć potencjalnie nieistotne czynniki. Coraz więcej młodych polskich użytkowników świata wirtualnego (około 96%) łączy się z siecią każdego dnia, zaś wiodącym narzędziem są nie komputery stacjonarne, laptopy, konsole, czy tablety, ale smartfon[23]. Jednocześnie szkoły kształcące dzieci i młodzież do 17 roku życia w Polsce, wydają się być dość zachowawcze w krzewieniu postaw świadomego użytkownika cyberprzestrzeni. Wedle badań w tylko 4 na 10 przypadkach wskazań tematyka cyberbezpieczeństwa jest realizowana przez placówki edukacji w przytaczanej kohorcie wiekowej[24].

Literatura:

1. Aleksandrowicz T. R., *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, „Przegląd Bezpieczeństwa Wewnętrznego", nr 8/2016.
2. Carr J., *Internet a wykorzystywanie seksualne dzieci i pornografia dziecięca*, „Dziecko Krzywdzone", nr 4/2005.
3. Dębowski T., *Cyberbezpieczeństwo wyzwaniem XXI wieku*, ArchaeGrap, Łódź 2018.
4. Gibson W., *Neuromancer*, New York, Ace Books, 1984.
5. Jarosz I., Jaroszewki P., Kijewski P., *System bezpieczeństwa cyberprzestrzeni RP*, Naukowa Akademicka Sieć Komputerowa, Warszawa, 2015.
6. Kozak S., *Patologie komunikowania w Internecie*, Wydawnictwo Difin, Warszawa 2011.
7. Krzyżak-Szymańska E., *Uzależnienia technologiczne wśród dzieci i młodzieży. Teoria, profilaktyka, terapia – wybrane zagadnienia*, Oficyna Wydawnicza „Impuls", Kraków 2018.
8. Madej M., *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego,* [w:] M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Polski Instytut Spraw Międzynarodowych, Warszawa 2009.
9. Sienkiewicz P., *Terroryzm w cybernetycznej przestrzeni*, [w:] T. Jemioła, J. Kisielniecki, K. Rajchel. (red.), *Cyberterroryzm – nowe wyzwania XXI wieku*, Wyższa Szkoła Informatyki, Zarządzania i Administracji, Warszawa 2009.
10. Wojtasik Ł., Przemoc rówieśnicza z użyciem mediów elektronicznych – wprowadzenie do problematyki, „Dziecko Krzywdzone", nr 1/2009.
11. *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022* (załącznik 1 do uchwałę nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017).

[23] J. Pyżalski, A. Zdrodowska, K. Abramczuk, Ł. Tomczyk, Polskie badanie EU KIDS…, op. cit., s. 17-20, [dostęp: 19.12.2020].

[24] Ibidem, s. 52.

12. *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024* (załącznik nr 1 do uchwały nr 125 Rady Ministrów z dnia 22 października 2019).
13. *Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw* (Dz.U. Nr 222, poz. 1323).
14. *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (Dz.U. 2018 poz. 1560).
15. *Ustawa z dnia 6 czerwca 1997 r. Kodeks karny* (Dz. U. 1997 Nr 88 poz. 553).

Netografia:

16. https://dziendobry.tvn.pl/a/zagrozenia-w-internecie--jakie-sa-i-kogo-dotycza
17. https://ksiazki.wp.pl/do-darknetu-nikt-nie-trafia-przypadkiem-to-raj-dla-zwyrodnialcow-6383365980756097a.
18. https://rekrutacja.apsl.edu.pl/Rekrutacja/oferta/Studia-1-stopnia/bezpieczenstwo-narodowe/ochrona-cyberprzestrzeni.
19. Statystyki policyjne, file:///Users/darslowa/Desktop/zamachy_samobojcze_grupa_wiekowa_dzien_tygodnia_2017-2019%20(1).pdf.
20. file:///Users/darslowa/Desktop/zamachy_samobojcze_grupa_wiekowa_dzien_tygodnia_2017-2019%20(1).pdf,
21. saferinternet.pl/images/artykuly/projekty-edukacyjne/Kompendium_www.pdf.
22. J. Pyżalski, A. Zdrodowska, K. Abramczuk, Ł. Tomczyk, Polskie badanie EU KIDS, Wydawnictwo Naukowe UAM 2018, https://fundacja.orange.pl/files/user_files/EU_Kids_Online_2019_v2.pdf Raport