PRACE NAUKOWE Akademii im. Jana Długosza w Częstochowie
Technika, Informatyka, Inżynieria Bezpieczeństwa 2018, t. VI, s. 185–197

http://dx.doi.org/10.16926/tiib.2018.06.14

Krzysztof Gawkowski
Katedra Bezpieczeństwa Wewnętrznego
Uczelnia Techniczno-Handlowa im. H. Chodkowskiej w Warszawie
ul. Jutrzenki 135, 02–231 Warszawa
e-mail: krzysztof.gawkowski@uth.edu.pl

WPŁYWY NOWOCZESNYCH TECHNOLOGII INFORMATYCZNYCH NA ZDROWIE I JAKOŚĆ ŻYCIA CZŁOWIEKA

Streszczenie. Wpływ nowoczesnych technologii na życie człowieka od setek lat jest stałym elementem rozwoju cywilizacji. Od wielu dziesięcioleci innowacyjne technologie stają się katalizatorem zmian i pozwalają na jeszcze szybszy rozwój. Człowiek i maszyna zaczynają żyć w pewnej symbiozie, a im gęstsza jest sieć połączeń między ludźmi i urządzeniami, tym łatwiejsze staje się życie, ale i zagrożeń jest zdecydowanie więcej. Kreując zapotrzebowanie na nowoczesność, musimy jednak pamiętać, że rozwój nie może być bezrefleksyjny, a technologia niesie wraz z postępem zarówno aspekty pozytywne, jak i negatywne dla ludzkiego życia oraz zdrowia. Bezpieczeństwo musi być priorytetem dla każdej z gałęzi rozwoju, a kluczem do spokojnego życia w nowoczesnym świecie powinno być wprowadzenie światowych regulacji prawnych, które wyprzedzą zagrożenia i zabezpieczą człowieka przed konsekwencjami niekontrolowanego rozwoju technologicznego.
Słowa kluczowe: rozwój, nowe technologie, cyberprzestrzeń, zdrowie, bezpieczeństwo.

INFLUENCE OF MODERN INFORMATION TECHNOLOGIES ON HEALTH AND QUALITY OF HUMAN LIFE

Abstract. The influence of modern technologies on human life for hundreds of years is a constant element of the development of civilization. For many decades, innovative technologies have been a catalyst for change and allow for even faster development. Man and machine begin to live in a certain symbiosis, and the denser is the network of connections between people and devices, the easier life becomes and the risks are much more. Creating the demand for modernity, however, we must remember that development can not be unreflective, and technology brings with it both positive and negative

aspects, for human life and health. Security must be a priority for each branch of development, and the key to a peaceful life in the modern world should be the introduction of global legal regulations that will overtake the threat and protect people from the consequences of uncontrolled technological development.
Keywords: development, new technologies, cyberspace, health, security.

Wstęp

W ciągu ostatnich lat szybki rozwój nowoczesnych technologii spowodował, że, z jednej strony życie stało się o wiele prostsze, z drugiej jednak narażone jest na nieznane niebezpieczeństwa, które czyhają na każdym rogu otaczającej nas cyberprzestrzeni. Nowe technologie wpływają na codzienne życie miliardów obywateli, poprawiają funkcjonowanie biznesu, wzmacniają prawa podstawowe i rozbudzają interakcje społeczne. Otwarta i wolna cyberprzestrzeń usuwa bariery już nie tylko między obywatelami i społecznościami, ale często całymi państwami. Rozwój technologiczny ma bardzo duży wpływ na wszystkie aspekty funkcjonowania społeczeństwa i jednocześnie pozwala na wymianę informacji oraz pomysłów w skali całego globu.

Szybki rozwój nie może być jednak bezrefleksyjny. Kreacji nowoczesnych technologii towarzyszyć powinna szeroka dyskusja o wpływie rozwoju technologicznego na bezpieczne życie człowieka i jakość środowiska naturalnego. W dosłownym znaczeniu bezpieczeństwo oznacza brak zagrożeń i poczucie pewności, ale podobnie jak wiele innych kategorii teoretycznych w naukach społecznych, nie posiada jednej, spójnej definicji[1]. Może zatem obejmować ono zjawiska fizyczne, ale postrzegane jest zarówno w perspektywie człowieka, jak i środowiska naturalnego. Rozwój nowoczesnych technologii i ich wpływ na zdrowie człowieka bez wątpienia w wielu ujęciach traktowany jest zatem jako potrzeba pierwotna, elementarna i naczelna. W klasycznej teorii potrzeb, znanej jako piramida Maslowa, bezpieczeństwo zajmuje nadrzędne miejsce, obok najważniejszych potrzeb fizjologicznych[2]. Biorąc pod uwagę strukturę klasyfikacji bezpieczeństwa, jednym z fundamentalnych jego aspektów jest bezpieczeństwo zdrowotne i cyberbezpieczeństwo.

Cyfrowa rewolucja w życiu człowieka

Rozbudowa potencjału technologicznego wydaje się być praktycznie nieograniczona. Sektor, w którym wykorzystanie nowoczesnych technologii dziś

[1] K. Malak, *Bezpieczeństwo jako kategoria i zjawisko społeczne*, „Piotrkowskie Zeszyty Międzynarodowe", 2007, nr 2, s. 91–95.
[2] A. Maslow, *A Theory of Human Motivation*, „Psychological Review" 1943, s. 370–396.

daje realną poprawę bezpieczeństwa człowieka jest branża zdrowotna. Obecnie jest już możliwe zamontowanie w domu czujników sprawdzających codzienne życie, a dzięki zastosowaniu technologii bezprzewodowego systemu monitorowania zdrowia pacjenta możliwe staje się jego wstępne diagnozowanie nawet w domu. Często zbierane są też dane medyczne poprzez czujniki znajdujące się np. w zegarku, przyklejane do powierzchni ciała lub wszczepiony chip. Zastosowanie takiego innowacyjnego i zarazem zdalnego systemu monitorowania parametrów życiowych człowieka, z wykorzystaniem medycznego sprzętu pomiarowego i transmisji danych, daje szanse na przekazanie lekarzowi zebranych danych w czasie rzeczywistym i bardzo szybką reakcję zwrotną[3]. Zmienia się również diametralnie sieć telefonii mobilnej, a konsumenci posługujący się smartfonami czy tabletami otrzymują interesujące ich informacje na temat zdrowej żywności czy dostępności lekarzy w dowolnym momencie. Nowoczesne narzędzia informatyczne wykorzystywane są także w administracji samorządowej i obecne są we wdrażaniu koncepcji inteligentnych miast, pozwalając między innymi minimalizować problemy zanieczyszczeń powietrza[4].

Rewolucja cyfrowa odbywa się na naszych oczach i kluczowym elementem musi być odpowiednie jej dostosowanie do potrzeb człowieka. Cyfryzacja, jak podaje *Oxford English Dictionary*[5], to adaptacja i wzrost wykorzystywania technologii cyfrowych lub komputerowych przez organizacje, sektory gospodarcze i kraje. Przynosi ona zarówno osobom prywatnym, jak i firmom wspomniane wcześniej wymierne korzyści, ale wiąże się również z różnorodnymi zagrożeniami. Najogólniej można je podzielić na: zagrożenia zdrowia (psychicznego i fizycznego) związane z użytkowaniem komputera i internetu, zagrożenia związane z uzależnieniami, zagrożenia społeczno-wychowawcze (obejmujące m.in. niebezpieczeństwa grożące dzieciom i młodzieży) i zagrożenia związane z szeroko pojętą cyberprzestępczością (z cyberterroryzmem włącznie) oraz rozmaitymi nadużyciami[6].

Do pierwszej z wymienionych grup zagrożeń zaliczyć można problemy zdrowotne wynikające z wielogodzinnego użytkowania komputera, np. problemy ze wzrokiem, słuchem, układem kostno-mięśniowym, schorzenia kciuka czy

---

[3] M. M. Baig, H. Gholam Hosseini, *Wireless remote patient monitoring in older adults. Engineering in Medicine and Biology Society (EMBC),* 35th Annual International Conference of the IEEE, Osaka, Japan 2013, s. 2429

[4] K. Gawkowski., *Administracja samorządowa w teorii i praktyce.* Wydawnictwo Adam Marszałek, Toruń, 2017, s. 218–219

[5] J. Pieriegud, *Cyfryzacja gospodarki i społeczeństwa - wymiar globalny, europejski i krajowy* [w:] J. Gajewski, W. Paprocki, J. Pieriegud (red.), *Cyfryzacja gospodarki i społeczeństwa. Szanse i wyzwania dla sektorów infrastrukturalnych*, Instytut Badań nad Gospodarką – Gdańska Akademia Bankowa, Gdańsk 2016, s. 12.

[6] J. Lizut (red.), *Zagrożenia cyberprzestrzeni. Kompleksowy program dla pracowników służb społecznych*, Wydawnictwo Wyższej Szkoły Pedagogicznej im. Janusza Korczaka, Warszawa 2014, s. 27–28.

nadgarstka. Często występują również alergie, zagrożenia ciąży, następstwa szkodliwego napromieniowania czy padaczka ekranowa[7]. Zalicza się do niej jednak również znacznie poważniejsze niebezpieczeństwa, np. tak zwaną cyfrową demencję[8], a także inspirowane lub spowodowane przez innych użytkowników sieci samookaleczenia[9] i samobójstwa[10] młodych ludzi. Według M. Spitzera, niemieckiego neurobiologa i autora publikacji *Cyfrowa demencja*, korzystanie z mediów elektronicznych przyczynia się do negatywnych zmian w ludzkim mózgu i, co za tym idzie, obniżenia sprawności umysłowej, np. zdolności uczenia się i zapamiętywania oraz koncentracji. Przewaga uczestniczenia w życiu społecznym za pośrednictwem mediów (internet, telefon) bywa też przyczyną jednego z nowych zjawisk autodestrukcyjnych – tzw. hikikomori – polegającej na unikaniu bezpośredniego kontaktu z innymi ludźmi, co może wiązać się z nieopuszczaniem pokoju czy mieszkania przez całe dnie, tygodnie, miesiące, a nawet lata. Hikikomori niejednokrotnie bywa też zapowiedzią samobójstwa, a innymi powodami, dla których ludzie dokonują samookaleczeń lub odbierają sobie życie bywa naśladownictwo osób opisanych w sieci, namowa grupy użytkowników określonych forów internetowych czy prześladowanie za pomocą narzędzi internetowych.

Kolejną grupę zagrożeń stanowią wszelkie niebezpieczne uzależnienia związane z wykorzystaniem nowoczesnych mediów. Chodzi tu zarówno o uzależnienia fizyczne, np. od różnego rodzaju substancji psychoaktywnych (narkotyki, leki, dopalacze, sterydy, napoje energetyzujące itp.), które można kupić przez internet[11], i o których istnieniu oraz działaniu można się dowiedzieć, korzystając z zasobów informacyjnych sieci, jak i o uzależnienia psychiczne (np. uzależnienia od komputera i internetu czyli infoholizm[12], uzależnienie od gier komputerowych[13]). Do podstawowych uzależnień internetowych oprócz

[7] M. Kopczewski, I. Dudziuk, *Zagrożenia, jakie niesie korzystanie z cyberprzestrzeni*, mit.weii.tu.koszalin.pl/ (*dostęp*: 25.11.2017).

[8] Ł. Tomczyk, *Cyfrowa demencja oraz inne formy e-zagrożeń jako nowe następstwa nieprawidłowego użytkowania nowych mediów* [w:] Andrzejewska A., Bednarek J. (red.) *Zagrożenia cyberprzestrzeni i świata wirtualnego*, Difin, Warszawa, 2014, s. 77–84.

[9] A. Andrzejewska, *Samobójstwa z inspiracji sieci* [w:] *Zagrożenia cyberprzestrzeni…*, op. cit., s. 121–136.

[10] P. Deputowski, *Internetowe kluby samobójców w świetle badań* [w:] A. Andrzejewska, J. Bednarek, S. Ćmiel (red.) *Człowiek w świecie rzeczywistym i wirtualnym. Wybrane patologie społeczno-wychowawcze w cyberprzestrzeni*, Wydawnictwo Wyższej Szkoły Gospodarki Euroregionalnej, Józefów 2013, ss. 235–250.

[11] A. Andrzejewska, *Internet źródłem informacji o substancjach odurzających i dopingujących* [w:] *Zagrożenia cyberprzestrzeni…*, op. cit., s. 185–202.

[12] A. Andrzejewska, J. Bednarek, *Uzależnienie od gier komputerowych* [w:] *Zagrożenia cyberprzestrzeni…*, op. cit., ss. 203–214.

[13] A. Andrzejewska, J. Bednarek, *Infoholizm* [w:] *Zagrożenia cyberprzestrzeni…*, op. cit., s. 215–231; D. Kołomyjski, *Fenomen zabijania w grach komputerowych* [w:] *Człowiek w świecie…*, op. cit., s. 251–264.

tradycyjnego uzależnienia komputerowego (czyli wewnętrznego przymusu spędzania czasu przy komputerze, powodującego nie tylko osłabienie relacji międzyludzkich, ale też często problemy ze snem, a nawet depresje, agresję, stany lękowe itp.) zalicza się również uzależnienie od sieci internetowej, a więc przymus bycia *online*, przymus pobierania informacji (*information overload*), socjomanię internetową (*cyberrelationship addiction*) i erotomanię internetową (*cybersexual addiction*).

Do podstawowych zagrożeń społecznych, wychowawczych i moralnych zaliczyć należy przede wszystkim wszelkie rodzaje cyberprzemocy[14] (np. flaming, cyberstalking[15], dyskredytacja czy podszywanie się pod inną osobę), ale też łatwy dostęp do nielegalnych stron internetowych związanych z przemocą[16], seksem (cyberpornografia, cyberpedofilia, prostytucja w sieci, seksting itp.), hazardem, nielegalną adopcją, handlem ludźmi i organami[17] czy stron rozmaitych sekt[18] i subkultur. Cyberagresji sprzyja anonimowość w sieci i powszechność mediów umożliwiająca jednocześnie powielanie ataków agresji przez kolejne osoby – np. rozpowszechniające i komentujące niezależnie od siebie zamieszczone przez tzw. hejtera, zdjęcie[19]. Najczęściej spotykane formy cyberagresji to wyzwiska i wulgaryzmy, poniżanie i ośmieszanie, zastraszanie i szantażowanie. Cyberagresja dotyczyć może znajomych użytkownika sieci, ale też może być skierowana na osoby zupełnie nieznane, na celebrytów, czy osoby pokrzywdzone w jakiś sposób (a więc „słabsze").

Z przeprowadzonego w 2010 roku badania „Modern Technology Usage and Internet Safety"[20] wynika m.in., że prawie połowa badanych dzieci i nastolatków uważa, iż Internet nie stanowi dla nich zagrożenia, choć ponad 40% przyznaje, że spotkało się z nieprzyjemnym materiałem pornograficznym dostępnym bez żadnych ostrzeżeń, niemal tyle samo spośród nich spotkało się z materiałami zawierającymi przemoc, ponad 20% było ofiarami cyberbullyingu, niemal 20% otrzymało propozycje seksualne od osób dorosłych i tyle samo odbierało niepokojące telefony i smsy. I choć podkreśla się, że wpływ pornografii na psychikę ludzką zależy na ogół od wieku, konstrukcji psychicznej, rodzaju materiałów, z którym się styka, to jednak na osoby bardzo młode wpływ ten jest na ogół bardzo negatywny[21], a czasem wręcz destrukcyjny. Z przeprowadzonych

[14] V. Lubkina, G. Marzano, *Cyberprzemoc* [w:] *Zagrożenia cyberprzestrzeni…*, op. cit., s. 85–98.
[15] A. Andrzejewska, *Stalking* [w:] *Zagrożenia cyberprzestrzeni…*, op. cit., s. 171–181.
[16] K. Bakalarczyk-Burakowska, *Specyfika zabijania pod wpływem mediów* [w:] *Człowiek w świecie*…, op. cit., s. 215–234.
[17] M. Cendrowski, *Współczesne uwarunkowania handlu ludźmi* [w:] *Człowiek w świecie*…, op. cit., s. 87–114.
[18] A. Andrzejewska, J. Bednarek, *Sekty* [w:] *Zagrożenia cyberprzestrzeni…*, op. cit., s. 163–170.
[19] B. Kałdon, *Cyberprzestrzeń jako zagrożenie dla człowieka XXI wieku*, „Seminare" 2016, nr 2.
[20] V. Lubkina, G. Marzano, *Cyberprzemoc* [w:] *Zagrożenia cyberprzestrzeni…*, op. cit.
[21] A. Andrzejewska, J. Bednarek, *Pornografia* [w:] *Zagrożenia cyberprzestrzeni…*, op. cit., s. 149–156.

w Polsce badań „Dziecko w sieci”[22] wynikało, że 87% dzieci podało obcemu swój adres e-mail (81% zrobiło to wielokrotnie), 64% numer telefonu (43% wielokrotnie), 42% adres zamieszkania (19% wielokrotnie), a 44% przesłało obcemu swoje zdjęcie (34% wielokrotnie). Ponadto 22% dzieci nie poinformowało nikogo o spotkaniach z osobami poznanymi przez internet. Młodzi ludzie nie zdają też sobie często sprawy z konsekwencji sekstingu – nie myślą o tym, że nawet te zrobione dla żartu nagie zdjęcia lub filmy mogą zostać skradzione, rozpowszechnione czy wykorzystane niezgodnie z prawem[23].

Niepokojące są również wyniki badania „Nastolatki 3.0”, przeprowadzonego przez NASK w 2016 roku. W badaniu można przeczytać, że „najczęstszymi, obserwowanymi przez młodzież negatywnymi zjawiskami, są: wyzywanie ich znajomych (59,7% deklaruje, że się z tym zetknęła) oraz poniżanie ich i ośmieszanie (58,1%). Rozpowszechnianie kompromitujących materiałów na temat swoich znajomych zauważyło 33,3% badanych. Jednocześnie straszenie znajomych zaobserwowało 34,2% badanych osób, a ich szantażowanie za pośrednictwem internetu aż 24,4%. Dość częste są także próby podszywania się pod inne osoby. Takie obserwacje deklaruje 40,5% badanych. Osób, które same doświadczyły powyższych konsekwencji jest wprawdzie mniej, ale ich liczba jest nadal zatrważająca”[24].

Najliczniejszą i najbardziej zróżnicowaną grupę zagrożeń stanowią nielegalne i noszące znamiona przestępczości działania związane z komputerami i siecią teleinformatyczną. Mogą one dotyczyć indywidualnych użytkowników, podmiotów gospodarczych i innych instytucji, wspólnot narodowych, państwowych, militarnych, gospodarczych itd. Najogólniej działania te można podzielić na dwa rodzaje, czyli dokonane przy użyciu komputera, za pomocą internetu, sieci teleinformatycznych[25] itp. oraz oddziałujące na komputery, sieci teleinformatyczne itp.

Na tym podziale opiera się m.in. jedna z pierwszych znanych definicji przestępczości komputerowej, wskazująca, iż jest nią „każde przestępcze działanie, w którym komputer stanowi albo narzędzie albo przedmiot zamachu”, a także współczesna definicja cyberprzestępczości, wg której cyberprzestępczość to „czyny przestępcze dokonane przy użyciu sieci łączności elektronicznej i systemów informatycznych lub skierowane przeciwko takim sieciom

[22] A. Andrzejewska, J. Bednarek, *Pedofilia w sieci* [w:] *Zagrożenia cyberprzestrzeni…*, op. cit., s. 141–148.

[23] A. Andrzejewska, J. Bednarek, *Seksting* [w:] *Zagrożenia cyberprzestrzeni…*, *op. cit.,* s. 157–162.

[24] *Nastolatki w internecie: smartfony, komunikacja i cyberprzemoc*, https://www.nask.pl/pl/aktualnosci/wydarzenia/wydarzenia-2016/432,Nastolatki-w-internecie-smartfony-komunikacja-i-cyberprzemoc.html (dostęp: 27.11.2017).

[25] Ł. Tomczyk, *Zagrożenia dla urządzeń mobilnych* [w:] *Zagrożenia cyberprzestrzeni…*, op. cit., s. 281–286.

i systemom”[26]. Dokonując analizy wpływu nowoczesnych technologii na życie i zdrowie człowieka, można posłużyć się też innym podziałem zagrożeń, rozróżniając pośród nich zagrożenia dla prywatności i zagrożenia dla własności.

Do zagrożeń prywatności zaliczyć należy wycieki danych osobowych z prywatnych baz danych, instytucji i urzędów, kradzieże informacji, zdjęć i dokumentów z komputerów czy telefonów osób prywatnych i instytucji, udostępnianie przez użytkowników sieci teleinformatycznych zdjęć, filmów czy informacji (prawdziwych lub fałszywych, a czasem krzywdzących i ośmieszających) o innych osobach[27] oraz kradzieże tożsamości czy umieszczenie danych żyjącej osoby na dedykowanym jej profilu w wirtualnej nekropolii[28]. Najczęściej spotykanymi zagrożeniami dla własności są: nieuprawnione korzystanie z dorobku intelektualnego innej osoby, kradzieże i oszustwa dokonywane za pomocą operacji elektronicznych (np. *phishing, pharming, skimming, vishing*[29], *fraudy bankowe*[30]), niszczenie danych i sprzętu elektronicznego przy pomocy złośliwego oprogramowania (np. wirusy, konie trojańskie, bomby logiczne, *malware*), komputerowy sabotaż. Osiem milionów Polaków wg danych z 2015 roku padło ofiarą cyberprzestępców[31], zaś koszty związane z nieuczciwą działalnością tych ostatnich wyniosły w naszym kraju blisko dziesięć miliardów złotych. W tym samym raporcie podano, że jedynie 28%. Polaków używa podstawowych programów zabezpieczających na smartfonach, 31% dzieli się z innymi swoimi hasłami dostępu do mediów społecznościowych, a 21% polskich rodziców pozwala swoim dzieciom korzystać ze swoich służbowych urządzeń.

Cyberprzestrzeń i nowoczesność

Klasyfikując zagrożenia wynikające z rozwoju nowoczesnych technologii należy dodać także cyberterroryzm, cyberszpiegostwo, uszkodzenia systemów zabezpieczeń sieci energetycznych[32] (które coraz częściej są atakowane przez cyberprzestępców), gazowych itp. oraz elektronicznych systemów sterowania rozmaitymi urządzeniami (samolotami, systemami regulacji ruchu ulicznego,

[26] M. Siwicki, *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo” 2012, nr 7–8.
[27] M. Bochenek, P. Bisialski, M. Różycka, A. Rywczyńska, K. Silicki, A. Wrońska, *Zagrożenia dla prywatności* [w:] *Zagrożenia cyberprzestrzeni…*, op. cit., s. 267–272.
[28] W. Duranowski, A. Durasiewicz, *Cmentarze danych* [w:] *Zagrożenia cyberprzestrzeni*…, op. cit., s.287–293.
[29] M. Bochenek, P. Bisialski, M. Różycka, A. Rywczyńska, K. Silicki, A. Wrońska, *Zagrożenia dla pieniędzy* [w:] *Zagrożenia cyberprzestrzeni…*, op. cit., s. 233–248.
[30] M. Staszczyk, *Nieuprawnione transakcje bankowe jako przejaw cyberprzestępczości*, „Finanse i Prawo Finansowe. Journal of Finance and Financial Law” 2015, vol. II, no. 1.
[31] Ibidem.
[32] J. Malko, H. Wojciechowski, *Sektor energetyczny i cyberbezpieczeństwo*, „Nowa Energia” 2015, nr 1.

śluzami itd.). W pewnych sytuacjach zagrożeniem tego typu może stać się nawet system sterujący elementami wyposażenia tzw. inteligentnych domów**.** **„**Przestępca może się dowiedzieć, gdzie jesteś, kiedy wrócisz do domu i wejść […] bez wyłamywania drzwi – ostrzegają eksperci IT. To wszystko jest możliwe, kiedy systemy, dzięki którym nasz dom jest inteligentny, nie są właściwie zabezpieczone. […] Poszczególne domowe urządzenia mogą stać się wrotami, przez które przestępcy przenikną do systemu informatycznego, dokonując kradzieży."[33]. Nawet telewizory czy samochody mogą stanowić zagrożenie dla właścicieli (np. w inteligentnych telewizorach wykryto złośliwą aplikację wykorzystującą lukę w zabezpieczeniach używanego systemu operacyjnego).

Zagrożenia występujące w cyberprzestrzeni można podzielić jeszcze w inny sposób – na takie, których źródłem jest technika (np. awarie sprzętu, zasilania itp.) i takie, których źródłem są ludzie. Do drugiej z tych grup zalicza się nie tylko zagrożenia spowodowane przez ludzkie błędy (wynikające np. z nieświadomości użytkowników lub lekceważenia obowiązków przez personel przedsiębiorstw i instytucji), ale wiele rodzajów działań, wynikających z najrozmaitszych motywacji i mających różny stopień zasięgu i szkodliwości.

Cyberterroryzm stanowi w XXI wieku jedno z najpoważniejszych zagrożeń bezpieczeństwa współczesnych państw oraz życia i zdrowia obywateli. Związek między rozwojem systemów teleinformatycznych i zmianami w sposobach działania terrorystów zauważono już w latach 90. XX wieku[34]. Od tej pory nowe technologie i internet wielokrotnie były wykorzystywane przez grupy terrorystyczne, zarówno te duże i znane, jak i te zupełnie niewielkie. Prowadzone w sieci teleinformatycznej wrogie działania przeciw Izraelowi podczas konfliktu w 2000 roku zostały nawet przez Palestyńczyków określone mianem „elektronicznego dżihadu". Głośny był również elektroniczny konflikt pomiędzy USA i Chinami z 2001 roku. W 2002 roku amerykańskie służby specjalne odkryły w komputerze członka Al-Kaidy dane świadczące o tym, że interesował się on amerykańskimi cyfrowymi systemami kontroli, a także narzędzia mogące służyć do przeprowadzenia ataku na te systemy. Rozproszeni po całym świecie agenci Al-Kaidy przyznają też, że byli szkoleni do przeprowadzania cyberataków na ważne elementy infrastruktury. Jeden z najgłośniejszych aktów cyberterroryzmu miał miejsce w Estonii w 2007 roku – zaatakowano na ogromną skalę obiekty infrastruktury krytycznej tego kraju. Zdaniem ówczesnego premiera Estonii testowano nowy model wojny cybernetycznej i był to pierwszy wypadek tak zmasowanego ataku na niepodległe państwo.

Oprócz ataków powodujących zakłócenia sieci teleinformatycznych

[33] *O tym właściciele inteligentnych domów powinni pamiętać*,http://innogy.forbes. pl/inteligentne-domy-zagrozenia,artykuly,202279,1,1.html (dostęp: 27.11.2017).

[34] N. Noga, *Cyberterroryzm – groźba realna*, Internetowy Biuletyn Instytutu Studiów nad Terroryzmem „e-Terroryzm.pl" 2013, listopad.

w sektorach o wysokim stopniu wrażliwości cyberterroryści mogą się również posłużyć dezinformacją, trollingiem, wrogą propagandą, zakłócaniem realizacji ważnych zadań administracji publicznej i wykorzystać luki technologiczne dające możliwość ataku na infrastrukturę krytyczną, która ma olbrzymie znaczenie dla zdrowia człowieka[35]. Sięgając do polskiej definicji ustawy o zarządzaniu kryzysowym, przez infrastrukturę krytyczną rozumie się „systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalne obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców". Cybrezagrożenia związane z nowoczesnymi technologiami mogą zatem objąć systemy zaopatrzenia w wodę i żywność, ochronę zdrowia, zaopatrzenie w paliwa i energię, transport i komunikację, sieci teleinformatyczne czy magazyny służące do przechowywania i składowania materiałów promieniotwórczych i chemicznych, w tym rurociągi z niebezpiecznymi substancjami[36].

Organizacje terrorystyczne posługujące się nowoczesnymi technologiami, które mają olbrzymi wpływ na życie i zdrowie człowieka można podzielić na trzy rodzaje. Używające nowych technik do prowadzenia tradycyjnej działalności (z Internetu korzystają np. jedynie w celu komunikowania się, zbierania informacji czy środków). Używające starych technik do nowej działalności (np. niszczą systemy informatyczne za pomocą siły fizycznej). Używające nowych technik do nowych działań (np. atakują w cyberprzestrzeni systemy informatyczne)[37].

Mamy też do czynienia z trzema poziomami zagrożenia cyberterroryzmem[38]:

- *simple-unstructured* – czyli dokonywaniem nieskomplikowanych włamań, za pomocą narzędzi skonstruowanych przez pojedyncze osoby, do indywidualnych systemów informacyjnych,
- *advanced-structured* – czyli dokonywaniem bardziej skomplikowanych ataków na złożone systemy i sieci komputerowe, przez cyberterrorystów mających możliwość analizy, modyfikacji swoich narzędzi, uczenia się nowych metod atakowania,
- *complex-coordinated* – czyli dokonywaniem skoordynowanych ataków na zintegrowane systemy obronne w celu ich totalnej destrukcji, przez

[35] K. Liedel, P. Piasecka, *Cyberbezpieczeństwo. Piąte pole walki. Diagnoza i rekomendacje*,bronislawkomorowski.org/wp.../Raport.-Cyberbezpieczeństwo-Piąte-pole-walki.pdf (dostęp: 26.11.2017).

[36] T. Małysa, *Informatyczna infrastruktura krytyczna i jej ochrona prawna*, Internetowy Biuletyn Instytutu Studiów nad Terroryzmem „e-Terroryzm.pl" 2013, listopad.

[37] N. Noga, *Podmioty i motywy działań w cyberprzestrzeni*, Internetowy Biuletyn Instytutu Studiów nad Terroryzmem „e-Terroryzm.pl" listopad,2013

[38] Ibidem.

cyberprzestępców dysponujących skomplikowanymi narzędziami i mającymi możliwość analizowania, samodoskonalenia i szkolenia się oraz kontrolowania i dowodzenia.

W rankingu największych zagrożeń USA (wg FBI) cyberterroryzm zajmuje trzecie miejsce, po ataku nuklearnym i broni masowego rażenia[39]. Nowoczesne narzędzia informatyczne umożliwiają bowiem oddziaływanie na systemy komputerowe (cywilne i wojskowe) przeciwnika i są w stanie nie tylko zakłócić, ale też uniemożliwić ich działanie. Niezwykle ważnym elementem w dziedzinie wykrywania i ścigania cyberterrorystów jest zatem współpraca międzynarodowa. W czasach, gdy technologie informacyjno-komunikacyjne stanowią jeden z najważniejszych elementów rozwoju pamiętać należy, że od daleko posuniętej kooperacji państw i rządów zależy, czy nowoczesne technologie będą człowiekowi służyć, czy przeciwko niemu zostaną wykorzystane.

Wnioski

Rozwój nowoczesnych technologii otwiera wiele możliwości i stanowi podstawę złożonych systemów, które napędzają gospodarkę w takich kluczowych sektorach jak: finanse, opieka zdrowotna, energetyka i transport. Wiele modeli biznesowych opiera się na innowacyjności, rozwoju technologicznym i sprawnym funkcjonowaniu systemów informatycznych. Przerwanie ich lub brak dostępu do już poznanych zasobów bez wątpienia negatywnie wpłynąłby na ludzkie życie i doprowadził do start rzędu miliardów dolarów.

Sięgając do danych Center for Strategic and International Studies (CSIS)[40], dowiadujemy się, że każdego roku działania cyberprzestępców powodują w skali światowej straty w wysokości ok. pół biliona dolarów. Codziennie atakowanych jest pięćset tysięcy stron internetowych i generuje się ponad trzydzieści mld maili o charakterze spamu. Dodatkowo warto podkreślić, że odnotowuje się kilkaset istotnych włamań do systemów teleinformatycznych, i w sumie szacuje się, że skradzionych w ostatnich latach mogło być prawie pięćset mln tożsamości[41]. Takie dane muszą budzić zaniepokojenie, bo oznaczają, że nowe technologie to nie tylko radość, ale smutek, często okraszony utratą zdrowia, a nawet życia.

Rozumiejąc, jaki wpływ dla ludzi mają nowe drogi rozwoju technologicznego, pamiętać należy, że każda zaawansowana technologia może być niebezpieczna. Podłączone do Internetu maszyny są zdolne do tworzenia ponad

[39] N. Noga, *Cyberterroryzm – nowe oblicze terroryzmu*, Internetowy Biuletyn Instytutu Studiów nad Terroryzmem „e-Terroryzm.pl" listopad,2013
[40] https://www.csis.org/analysis
[41] Internet Security Threat Report, Symantec, Mountain View, USA, 2016

2,5 tryliona bajtów dziennie. Chcąc w sposób policzalny określićj jaka jest to wielkość, wystarczy wyobrazić sobie, że 90%. danych na świecie zostało stworzonych w ciągu ostatnich dwóch lat. Ważne jest zatem, aby postęp szedł w parze z zaufaniem oraz z zapewnieniem obywatelom odpowiednich gwarancji dla ich życia i zdrowia.

Największą rolę w budowaniu wzajemnego zaufania obywatela do wykorzystywania w codziennym życiu nowych technologii mają struktury państwa. Każda osoba korzystająca z zasobów nowoczesności musi być świadoma zagrożeń, jakie mogą ją spotkać lub sama może je stworzyć, gdy w nieodpowiedzialny sposób będzie z nich korzystała. Zachowanie w sieci jednostki ma wpływ na bezpieczeństwo pozostałych użytkowników, a bez zaufania obywateli do budowanego systemu, nie jest możliwa wzajemna spójna kooperacja. Rozwój technologii będzie zapewniał bezpieczeństwo w sektorze publicznym, jak i prywatnym, jedynie w przypadkach, jeśli rządy poszczególnych państw poruszaną tematykę docenią i obejmą odpowiednim nadzorem oraz pomocą.

Literatura

[1] Andrzejewska A., Bednarek J., Zagrożenia cyberprzestrzeni i świata wirtualnego, Difin, Warszawa, 2014.

[2] Baig M. M., Gholam Hosseini H., *Wireless remote patient monitoring in older adults, Engineering in Medicine and Biology Society (EMBC)*, 35th Annual International Conference of the IEEE, Osaka, Japan, 2013.

[3] Bakalarczyk-Burakowska K., *Specyfika zabijania pod wpływem mediów* [w:] Andrzejewska A., Bednarek J., Ćmiel S. (red.), *Człowiek w świecie rzeczywistym i wirtualnym. Wybrane patologie społeczno-wychowawcze w cyberprzestrzeni*, Wydawnictwo Wyższej Szkoły Gospodarki Euroregionalnej, Józefów, 2013.

[4] Bochenek M., Bisialski P., Różycka M., Rywczyńska A., Silicki K., Wrońska A., *Zagrożenia dla pieniędzy* [w:] Andrzejewska A., Bednarek J. (red.), *Zagrożenia cyberprzestrzeni i świata wirtualnego*, Difin, Warszawa, 2014.

[5] Brzeziński M., *Kategoria bezpieczeństwa*, [w:] Sulowski S., Brzeziński M. (red.), *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, Warszawa, 2009.

[6] Cendrowski M., *Współczesne uwarunkowania handlu ludźmi* [w:] A. Andrzejewska, J. Bednarek, S. Ćmiel (red.) *Człowiek w świecie rzeczywistym i wirtualnym. Wybrane patologie społeczno-wychowawcze w cyberprzestrzeni*, Wydawnictwo Wyższej Szkoły Gospodarki Euroregionalnej, Józefów, 2013.

[7] Concise Oxford English Dictionary, Oxford University Press, Oxford, 2011.
[8] Deputowski P., *Internetowe kluby samobójców w świetle badań* [w:] Andrzejewska A., Bednarek J., Ćmiel S. (red.), *Człowiek w świecie rzeczywistym i wirtualnym. Wybrane patologie społeczno-wychowawcze w cyberprzestrzeni*, Wydawnictwo Wyższej Szkoły Gospodarki Euroregionalnej, Józefów, 2013.
[9] Duranowski W., Durasiewicz A., *Cmentarze danych* [w:] Andrzejewska A., Bednarek J. (red.), *Zagrożenia cyberprzestrzeni i świata wirtualnego*, Difin, Warszawa, 2014.
[10] Gawkowski K., Administracja *samorządowa w teorii i praktyce.* Wydawnictwo Adam Marszałek, Toruń, 2017.
[11] Kopczewski M., Dudziuk I., *Zagrożenia jakie niesie korzystanie z cyberprzestrzeni*, mit.weii.tu.koszalin.pl/ (dostęp: 25.11.2017).
[12] Kałdon B., *Cyberprzestrzeń jako zagrożenie dla człowieka XXI wieku*, „Seminare" 2016, nr 2.
[13] Lizut J. (red.), *Zagrożenia cyberprzestrzeni. Kompleksowy program dla pracowników służb społecznych*, Wydawnictwo Wyższej Szkoły Pedagogicznej im. Janusza Korczaka, Warszawa, 2014.
[14] Liedel K., Piasecka P., *Cyberbezpieczeństwo. Piąte pole walki. Diagnoza i rekomendacje,* bronislawkomorowski.org/wp.../Raport.-Cyberbezpieczeństwo-Piąte-pole-walki.pdf (dostęp: 26.11.2017).
[15] Lubkina V., Marzano G., *Cyberprzemoc* [w:] Andrzejewska A., Bednarek J. (red.), *Zagrożenia cyberprzestrzeni i świata wirtualnego*, Difin, Warszawa, 2014.
[16] Malak K., *Bezpieczeństwo jako kategoria i zjawisko społeczne*, „Piotrkowskie Zeszyty Międzynarodowe", 2007, nr 2.
[17] Malko J., Wojciechowski H., *Sektor energetyczny i cyberbezpieczeństwo*, „Nowa Energia", 2015, nr 1.
[18] Małysa T., *Informatyczna infrastruktura krytyczna i jej ochrona prawna*, Internetowy Biuletyn Instytutu Studiów nad Terroryzmem „e-Terroryzm.pl" listopad 2013.
[19] Maslow A., *A Theory of Human Motivation*, „Psychological Review", lipiec 1943, DOI: http://dx.doi.org/10.1037/h0054346
[20] Noga N., *Cyberterroryzm – groźba realna*, Internetowy Biuletyn Instytutu Studiów nad Terroryzmem „e-Terroryzm.pl" listopad 2013.
[21] Pieriegud J., *Cyfryzacja gospodarki i społeczeństwa - wymiar globalny, europejski i krajowy* [w:] Gajewski J., Paprocki W., Pieriegud J. (red.), *Cyfryzacja gospodarki i społeczeństwa. Szanse i wyzwania dla sektorów infrastrukturalnych*, Instytut Badań nad Gospodarką - Gdańska Akademia Bankowa, Gdańsk 2016.

[22] Siwicki M., *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7–8.
[23] Staszczyk M., *Nieuprawnione transakcje bankowe jako przejaw cyberprzestępczości*, „Finanse i Prawo Finansowe - Journal of Finance and Financial Law" 2015, vol. II, no. 1.
[24] Spitzer M., *Cyfrowa demencja*, Dobra Literatura, Słupsk, 2013.
[25] Tomczyk Ł.,*Cyfrowa demencja oraz inne formy e-zagrożeń jako nowe następstwa nieprawidłowego użytkowania nowych mediów* [w:] Andrzejewska A., Bednarek J. (red.) *Zagrożenia cyberprzestrzeni i świata wirtualnego*, Difin, Warszawa, 2014.
[26] Internet Security Threat Report, Symantec, Mountain View, USA, 2016
[27] *Nastolatki w internecie: smartfony, komunikacja i cyberprzemoc*, https://www.nask.pl/pl/aktualnosci/wydarzenia/wydarzenia-2016/432, Nastolatki-w-internecie-smartfony-komunikacja-i-cyberprzemoc.html (dostęp: 27.11. 2017).
[28] *O tym właściciele inteligentnych domów powinni pamiętać*, http://innogy.forbes.pl/inteligentne-domy-zagrozenia,artykuly,202279,1,1.html (dostęp: 27.11.2017).
[29] https://www.csis.org/analysis.