W służbie społeczeństwu. Polska w obronie praw człowieka na świecie i w kraju, red. J. Stala, M. Butrymowicz, Uniwersytet Papieski Jana Pawła II w Krakowie Wydawnictwo Naukowe, Kraków 2022 • s. 139–158
ISBN 978-83-7438-988-4 (druk) • ISBN 978-83-7438-989-1 (online)

DOI: https://doi.org/10.15633/9788374389891.09

Robert Janczewski
https://orcid.org/0000-0002-2011-0413
Akademia Marynarki Wojennej im. Bohaterów Westerplatte

Cyberbezpieczeństwo w życiu społecznym

W sposobach bycia człowiekiem zawiera się całokształt ludzkich działań, postaw, intencji, zamiarów, celów, motywacji, argumentów, wartości i powinności, myślenia i bezmyślności – słowem: całość ekspresji wewnętrznej prawdy o człowieku, manifestującej się w konkretnych uwarunkowaniach ludzkiego bycia i działania[1]. Tymczasem techniczny i technologiczny rozwój wielu społeczeństw XX i XXI stulecia przyczynił się do powstawania nieznanego dotychczas obszaru ich funkcjonowania. Ten fragment rzeczywistości został nazywany cyberprzestrzenią. Stał się jednym z wymiarów ludzkiego bycia i działania. Wiele społeczeństw (społeczności) uzależniło swoje funkcjonowanie od rozwiązań teleinformatycznych[2]. Pojawiła się nowa domena ludzkich działań, manifestacji postaw, eksponowania zamiarów, ustanawiania i realizacji celów, wzbudzania i zaspokojenia swoich potrzeb, przedstawiania argumentów, poszukiwania i wyrażania własnych wartości, kształtowania sposobów myślenia i dawania wyrazu swojej bezmyślności. Taki stan rzeczy przyniósł nowe spojrzenie na bezpieczeństwo społeczeństw. Koniecznością stało się budowanie i utrzymywanie szczególnego rodzaju bezpieczeństwa – cyberbezpieczeństwa.

Wieloaspektowość oraz współczesne warunki funkcjonowania społeczeństw przyczyniły się do wysiłku mającego na celu znalezienie rozwiązania zasadniczego problemu badawczego sformułowanego w postaci pytania: „Jaka jest charakterystyka cyberbezpieczeństwa w społeczeństwie?". Poszukiwanie odpowiedzi na pytanie zasadnicze wymagało doprecyzowania: „Czym jest cyberbezpieczeństwo?" oraz „Jakie są cyberzagrożenia w życiu społecznym?".

1 Zob. M. Drożdż, *Świadomość działania jako podstawa etycznego wartościowania*, „Studia Socialia Cracoviensia" 10 (2018) nr 2 (19), s. 11–20.

2 Teleinformatyka – dziedzina techniki zajmująca się wykorzystaniem telekomunikacji w informatyce i informatyki w telekomunikacji; zob. http://sjp.pwn.pl/slowniki/teleinformatyka.html (10.01.2020).

W literaturze przedmiotu pojawiły się publikacje tematyczne właśnie z zakresu cyberbezpieczeństwa. Wiele państw opublikowało narodowe strategie cyberbezpieczeństwa. Również w ramach licznych konferencji poświęconych cyberbezpieczeństwu toczone są zarówno przez naukowców, jak i praktyków, niejednokrotnie żarliwe, dyskusje. Padają słowa mające przedrostek „cyber-" lub wieloczłonowe terminy ze słowem „cybernetyczny" (odmieniane przez wszystkie przypadki). Pojawiają się jednak pytania: „Czy uczestnicy wymiany poglądów, posługując się «cybersłowami»[3], na pewno się rozumieją? Czy rozważania o cyberbezpieczeństwie przebiegają w jednolitej konwencji terminologicznej, we wzajemnym zrozumieniu?".

Sprawcą popularności terminów składających się z cząstki „cyber-" jest termin „cyberprzestrzeń", a nie jak można by się spodziewać „cybernetyka". Analiza i krytyka literatury wykazała, że „cyberprzestrzeń" to bardzo popularny termin. Jednak mimo swojej popularności nie ma jednej powszechnie uznanej definicji[4]. Nie został zatem jednoznacznie wskazany desygnat cyberprzestrzeni, co z pragmatycznego punktu widzenia stanowi barierę w budowaniu i utrzymywaniu bezpieczeństwa.

Zauważalny brak jednoznaczności w definiowaniu terminu „cyberprzestrzeń" pozwala sformułować wniosek, iż fragment nowej, powstałej w wyniku rozwoju cywilizacyjnego społeczeństw rzeczywistości określany mianem cyberprzestrzeni nie jest dostatecznie, jeśli w ogóle, zidentyfikowany i zbadany. Analiza i krytyka literatury wykazała również brak jednoznacznej konwencji terminologicznej w tym obszarze.

Zgodnie z Encyklopedią PWN[5] konwencją terminologiczną w metodologii jest porozumienie, umowa dotycząca używania terminów naukowych w tych samych znaczeniach. Konwencja terminologiczna ma niebagatelne znaczenie w tworzeniu, w określonym obszarze, nowych terminów i nadawaniu im znaczenia. Wyrazem konwencji terminologicznej jest tak zwana definicja syntetyczna (projektująca), która wprowadza nowy termin lub też nadaje staremu terminowi nowe, często tylko ściślej określone znaczenie (w tym ostatnim wypadku mówi się często o definicji regulującej), które obowiązuje później na mocy konwencji terminologicznej w zainteresowanych środowiskach; rzeczą dyskusyjną jest to,

3 Dla uporządkowania terminologii w niniejszym opracowaniu „cybersłowo" to wypowiedź ustna lub pisemna, znak językowy zawierający prefiks „cyber-" lub wyraz „cybernetyczny".

4 Zob. J. Unold, *Teoretyczno-metodologiczne podstawy przetwarzania informacji w cyberprzestrzeni*, Wrocław 2011.

5 Zob. https://encyklopedia.pwn.pl/haslo/konwencja-terminologiczna;3925437.html (31.01.2018).

na ile ustalający konwencję terminologiczną muszą odwoływać się do obiektywnej rzeczywistości i uprzednio istniejących nawyków językowych[6]. Jak pokazuje praktyka w przypadku „cyberrzeczywistości"[7], wprowadzane do nauki, jak również do życia społecznego terminy nie są niestety oparte na konwencji terminologicznej, lecz przejęte w domniemanym znaczeniu z języka potocznego. Wadą takiego rozwiązania jest to, że w języku potocznym są to opisy, a nie definicje. Doskonałym przykładem obrazującym powyższą hipotezę jest przywołane wyżej słowo „cyberprzestrzeń". Osoba słysząca lub wymawiająca je wielokrotnie w określonej, takiej samej sytuacji nabywa nawyku rutynowego używania go w powtarzających się uwarunkowaniach.

Aby mówić o znaczeniu cyberprzestrzeni dla bezpieczeństwa społeczeństwa, zasadne jest jednoznaczne określenie, czym właściwie jest owa przestrzeń. Wydaje się, wobec tego, iż dla porządku terminologicznego oraz dalszego wysiłku badawczego wystarczy odpowiedzieć na pytanie: „Co to jest cyberprzestrzeń?". Zatem.

1. Co to jest cyberprzestrzeń?

Termin „cyberprzestrzeń" ma wiele znaczeń. W literaturze przedmiotu cyberprzestrzeń definiowana jest w zależności od potrzeb. Różne dziedziny działalności człowieka używają tego pojęcia w różnorakich znaczeniach[8]. Taki stan rzeczy wynika z błędu popełnianego zarówno przez praktyków, jak i ludzi nauki. Analiza licznych, często różniących się definicji skłania do wniosku, że są one odpowiedzią na pytanie: „Co to jest cyberprzestrzeń?". Pozornie taka praktyka nie budzi zastrzeżeń. Jednak jest to jedynie pozór. Czy zatem tak postawione zapytanie jest właściwe? Otóż analiza owego zapytania dowodzi, że nie. Osoba zapytana w taki właśnie sposób, chcąc odpowiedzieć, musi rozumieć wszystkie słowa zawarte w pytaniu. Jeśli jest to pytanie egzaminacyjne, sprawdzające wiedzę uzyskaną z określonych źródeł, możemy wówczas domniemywać, że odpowiadający rozumie, o co został zapytany. W innych okolicznościach tak postawione pytanie jest bezprzedmiotowe. Bo jak odpowiedzieć na pytanie: „Co to jest cyberprzestrzeń?", nie znając znaczenia słowa „cyberprzestrzeń"?

6 Zob. https://encyklopedia.pwn.pl/haslo/konwencja-terminologiczna;3925437.html (31.01.2018).

7 Wyraz utworzony (przez autora) w celu oddania charakteru fragmentu rzeczywistości opisywanego zarówno przez praktyków, jak i (niestety) teoretyków, bez głębszej refleksji, za pomocą prefiksu „cyber-", przymiotnika „cybernetyczny" lub samodzielnego „cyber".

8 Zob. J. Unold, *Teoretyczno-metodologiczne*…, dz. cyt.

W niniejszym opracowaniu jako przykład braku spójności przedstawione zostaną definicje cyberprzestrzeni zawarte w kluczowych dokumentach dotyczących cyberbezpieczeństwa w Polsce.

W ogłoszonej 25 września 2002 roku Ustawie z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej cyberprzestrzeń zdefiniowano jako „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 zadania publiczne (Dz. U. z 2017 r. poz. 570), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami"[9]. Czytając tę definicję, za sprawą zawartych w niej odsyłaczy do innych aktów prawnych, można odnieść wrażenie, iż została napisana przez prawników dla prawników.

Następnie w dokumencie *Rządowy program ochrony cyberprzestrzeni RP na lata 2009–2011 – założenia* z 2009 roku cyberprzestrzenią nazwano „przestrzeń komunikacyjną tworzoną przez system powiązań internetowych"[10].

Natomiast w kierowanym w 2010 roku do uzgodnień resortowych projekcie *Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016. Wersja 1.1* cyberprzestrzenią nazwano „cyfrową przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami"[11]. Jak widać, jest to uproszczenie pierwszej definicji cyberprzestrzeni, która ukazała się w polskiej przestrzeni prawnej.

Tymczasem w *Polityce ochrony cyberprzestrzeni Rzeczypospolitej Polskiej* z 2013 roku cyberprzestrzeń została opisana jako przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, określone w art. 3 pkt 3 Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. Nr 64, poz. 565 z późn. zm.), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami, zgodnie z art. 2 ust. 1b Ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. Nr 156, poz. 1301 z późn. zm.), art. 2

9 Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, Dz.U. Nr 156, poz. 1301.

10 Departament Ewidencji Państwowych i Teleinformatyki MSWiA, *Rządowy program ochrony cyberprzestrzeni RP na lata 2009–2011 – założenia*, Warszawa 2009.

11 Departament Ewidencji Państwowych i Teleinformatyki MSWiA, *Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016. Wersja 1.1*, Warszawa 2010.

ust. 1a Ustawy z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Dz.U. Nr 113, poz. 985 z późn. zm.) oraz art. 3 ust. 1 pkt 4 Ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. Nr 62, poz. 558 z późn. zm.)[12].

Zauważalne jest, iż powyższa definicja została wzbogacona o kolejny akt prawny, czyli Dz.U. Nr 62, poz. 558, t.j. Dz.U. poz. 1897 – Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 15 września 2017 r. w sprawie ogłoszenia jednolitego tekstu ustawy o stanie klęski żywiołowej[13]. Swoistą ciekawostką jest fakt, iż w tym dokumencie autorzy podkreślili, że został on opracowany w Ministerstwie Administracji i Cyfryzacji we współpracy z Agencją Bezpieczeństwa Wewnętrznego na podstawie okresowych raportów o stanie bezpieczeństwa, publikowanych przez Rządowy Zespół Reagowania na Incydenty Komputerowe, oraz decyzji Przewodniczącego Komitetu Rady Ministrów do spraw Cyfryzacji nr 1/2012 z dnia 24 stycznia 2012 roku w przedmiocie powołania zespołu zadaniowego do spraw ochrony portali rządowych, a także omówionego 9 marca 2009 roku przez Komitet Stały Rady Ministrów dokumentu *Rządowy program ochrony cyberprzestrzeni RP na lata 2009–2011 – założenia*. O ile *Rządowy program*… wskazuje na cyberprzestrzeń jako „cyfrową przestrzeń przetwarzania i wymiany informacji", o tyle *Polityka ochrony cyberprzestrzeni*… jedynie na (już nie cyfrową) „przestrzeń przetwarzania i wymiany informacji".

W *Doktrynie cyberbezpieczeństwa Rzeczypospolitej Polskiej* określenie cyberprzestrzeni jest rozwinięciem definicji zawartej w Ustawie o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej. W tym dokumencie cyberprzestrzeń to

> przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami[14].

12 Zob. Ministerstwo Administracji i Cyfryzacji, *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*, Warszawa 2013.

13 W tym akcie prawnym cyberprzestrzeń zdefiniowana została identycznie jak w Ustawie z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej.

14 Biuro Bezpieczeństwa Narodowego, *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Warszawa 2015.

W *Krajowych ramach polityki cyberbezpieczeństwa Rzeczpospolitej Polski na lata 2017–2022*[15] oraz *Strategii cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*[16] cyberprzestrzenią jest przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami. Autorzy *Strategii…* określili, iż jej publikacja wpisuje się w kontynuację działań podejmowanych w przeszłości przez administrację rządową mających na celu podniesienie poziomu bezpieczeństwa w cyberprzestrzeni RP, w tym w ustalenia określone przez rząd w 2013 roku w dokumencie *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*.

Analiza przytoczonych powyżej dokumentów uwidocznia, iż w polskiej przestrzeni prawnej oraz dokumentach doktrynalnych cyberprzestrzeń opisywana jest w zasadzie tak samo. „W zasadzie", ponieważ interesujący jest jeden fakt. Autorzy *Polityki ochrony cyberprzestrzeni Rzeczypospolitej Polskiej* zadeklarowali, iż niniejszy dokument opracowano na podstawie między innymi publikacji *Rządowy program ochrony cyberprzestrzeni RP na lata 2009–2011 – założenia*, a w obu tych dokumentach cyberprzestrzeń zdefiniowana jest inaczej, czyli wskazane zostały różne jej desygnaty. Zatem wydaje się, że dla systemu cyberbezpieczeństwa społeczeństwa taki stan rzeczy jest niepożądany.

W Katowicach 10–12 maja 2017 roku odbyła się IX edycja Europejskiego Kongresu Gospodarczego. Jeden z obszarów tematycznych nosił nazwę: „Cyberbezpieczeństwo infrastruktury krytycznej". Na pierwszy rzut oka wydaje się, że nie ma nic nadzwyczajnego w takim sformułowaniu. Jednak analiza dokumentu *Narodowy program ochrony infrastruktury krytycznej – tekst jednolity* oraz załącznika 1 do niego: *Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje* (dalej: *Załącznik*) wykazała, że w żadnym z tych kluczowych dokumentów nie ma definicji ani cyberprzestrzeni, ani cyberbezpieczeństwa. W *Załączniku* odnajdziemy wprawdzie takie „cybersłowa" jak: „cyberprzestępczość", „cyberterroryzm", „cyberatak", a także sformułowanie: „Cyberataki na systemy IK stały się częścią konfliktów cybernetycznych cyberprzestrzeni, w tym konfliktów między państwami"[17], jednak żadne z powyższych nie zostało wyjaśnione. Czym są wobec tego cyberprzestępczość,

15 Zob. Ministerstwo Cyfryzacji, *Krajowe ramy polityki cyberbezpieczeństwa Rzeczpospolitej Polski na lata 2017–2022*, Warszawa 2017.

16 Zob. Ministerstwo Cyfryzacji, *Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*, Warszawa 2017.

17 Zob. Rządowe Centrum Bezpieczeństwa, *Narodowy program ochrony infrastruktury krytycznej – tekst jednolity*, załącznik 1, *Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje*, Warszawa 2015, s. 72, wprowadzony Uchwałą nr 210/2015 Rady Ministrów z dnia 2 listopada 2015 r. w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej z uwzględnie-

cyberterroryzm czy cyberatak w rozumieniu owych dokumentów? Można przypuszczać, że uczestnicy Europejskiego Kongresu Gospodarczego prowadzący debatę na temat cyberbezpieczeństwa infrastruktury krytycznej mimo iż wypowiadali te same cybersłowa, mogli mieć na myśli różne ich reprezentacje.

Warto w tym miejscu zwrócić uwagę na zapis „konflikt cybernetyczny cyberprzestrzeni". Podczas jego czytania nasuwają się pytania: „Co ów zapis oznacza? Czy każdy czytający rozumie go tak samo, skoro nie został nigdzie sprecyzowany?". Odpowiedź „nie" wydaje się oczywista, jednak możliwa jest sytuacja, w której istnieje prawdopodobieństwo, iż może jest on zrozumiały tak samo dla każdego. Bez przeprowadzenia badań niestety nie jest możliwe udzielenie jednoznacznej rozstrzygającej odpowiedzi.

2. Cyberbezpieczeństwo, czyli co?

W tekstach kultury funkcjonują terminy: „cyberbezpieczeństwo", „bezpieczeństwo cybernetyczne", „bezpieczeństwo w cyberprzestrzeni", „bezpieczeństwo cyberprzestrzeni". Analiza i krytyka literatury wykazała, że przez wielu autorów opracowań tematycznych przytoczone terminy niejednokrotnie traktowane są jak synonimy. Nie byłoby w tym nic dziwnego, gdyby nie to, że w istocie są to różne pojęcia. Brak konwencji terminologicznej widoczny jest nie tylko w opracowaniach beletrystycznych czy naukowych. Zauważalny jest również w polskich dokumentach doktrynalnych i planistycznych.

W serwisie internetowym Biura Bezpieczeństwa Narodowego (BBN) znajduje się *(Mini)słownik BBN. Propozycje nowych terminów z dziedziny bezpieczeństwa*[18]. Słownik ów zawiera robocze propozycje popularnych terminów, wykorzystywanych między innymi w pracach BBN, odnoszących się do teorii oraz praktyki bezpieczeństwa narodowego i międzynarodowego. Według pomysłodawców tego słownika jego publikacja wychodzi naprzeciw oczekiwaniom zgłaszanym między innymi na serwisach społecznościowych w związku z rozmowami o nowych zjawiskach, procesach i wyzwaniach z zakresu bezpieczeństwa. Wśród zawartych tam definicji jedna z nich określa, że cyberbezpieczeństwo RP (bezpieczeństwo RP w cyberprzestrzeni) jest

> transsektorowym obszarem bezpieczeństwa, obejmującym proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego

niem Uchwały nr 61/2016 Rady Ministrów z dnia 1 czerwca 2016 r. zmieniającej uchwałę w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej.

18 Zob. https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy-/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html (30.11.2019).

elementów (struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej oraz będących w ich dyspozycji systemów teleinformatycznych i zasobów informacyjnych)[19].

Lektura przedstawionej definicji skłania do wniosku, że „cyberbezpieczeństwo RP" to to samo co „bezpieczeństwo RP w cyberprzestrzeni". Ponadto w owej definicji na uwagę zasługuje zapis: „transsektorowy obszar bezpieczeństwa, obejmujący proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa […]". Zgodnie z nim bezpieczeństwo RP w cyberprzestrzeni odnosi się do cyberprzestrzeni państwa i jest ściśle z nią związane. Sformułowanie to odsyła nas do definicji cyberprzestrzeni RP zawartej w *Doktrynie cyberbezpieczeństwa Rzeczypospolitej Polskiej* z 22 stycznia 2015 roku[20], która precyzuje cyberprzestrzeń RP jako „cyberprzestrzeń[21] w obrębie terytorium państwa polskiego oraz w miejscach, gdzie funkcjonują przedstawicielstwa RP (placówki dyplomatyczne, kontyngenty wojskowe, jednostki pływające oraz statki powietrzne poza przestrzenią RP, podlegające polskiej jurysdykcji)".

Doświadczenie wskazuje, że zarówno wśród praktyków, jak i teoretyków nie ma zgodności co do istnienia cyberprzestrzeni RP. Spór toczony jest między innymi o kanały transmisyjne, a w zasadzie o ich przynależność terytorialną, na przykład przynależność transmisyjnego toru radiowego przenoszącego sygnały nad wodami międzynarodowymi.

Definicja zaproponowana w *(Mini)słowniku* wydaje się tożsama z definicją przedstawioną w *Doktrynie cyberbezpieczeństwa Rzeczypospolitej Polskiej*. Jednak jej analiza uwidocznia różnice. Zgodnie z *Doktryną…* cyberbezpieczeństwo RP (bezpieczeństwo RP w cyberprzestrzeni) to „proces zapewniania bezpiecznego funkcjonowania […]". Według autora definicji zaproponowanej w *(Mini)słowniku* cyberbezpieczeństwo RP (bezpieczeństwo RP w cyberprzestrzeni) jest „transsektorowym obszarem bezpieczeństwa, obejmującym proces zapewniania bezpiecznego funkcjonowania […]". Ponadto autor owej definicji (swoją drogą ciekawe dlaczego?) zastosował inne niż w *Doktrynie…* spójniki i partykuły. W *(Mini)słowniku* widnieje zapis: „podmiotów […] oraz […] systemów […] i zasobów […]", tymczasem w *Doktrynie…*: „podmiotów […],

19 https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/603-5,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html (30.11.2019).

20 Zob. Biuro Bezpieczeństwa Narodowego, *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, dz. cyt.

21 Cyberprzestrzeń w rozumieniu przytoczonej wyżej definicji zawartej w *Doktrynie cyberbezpieczeństwa Rzeczypospolitej Polskiej*.

a także […] systemów […] oraz zasobów […]". Na uwagę zasługuje również fakt, iż „doktrynalna" definicja uwzględnia „cyberprzestrzeń globalną" (czym ona by nie była). Natomiast „(mini)słownikowa" nie.

Krajowe ramy polityki cyberbezpieczeństwa Rzeczpospolitej Polski na lata 2017–2022 oraz *Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022* zostały, według zawartego w nich zapisu, opracowane przez grupę składającą się z przedstawicieli resortów: cyfryzacji, obrony narodowej, spraw wewnętrznych i administracji oraz przedstawicieli Agencji Bezpieczeństwa Wewnętrznego, Rządowego Centrum Bezpieczeństwa i Biura Bezpieczeństwa Narodowego. Zamierzeniem tych dokumentów jest określenie ramowych działań mających na celu uzyskanie wysokiego poziomu odporności krajowych systemów teleinformatycznych, operatorów usług kluczowych, operatorów infrastruktury krytycznej, dostawców usług cyfrowych oraz administracji publicznej na incydenty w cyberprzestrzeni.

Tymczasem desygnat cyberbezpieczeństwa wskazany w tych kluczowych dokumentach różni się od „doktrynalnego" i jest nim

> odporność systemów teleinformatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych, lub przetwarzanych danych, lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne[22].

Ponadto zgodnie z zapisami obydwu dokumentów „bezpieczeństwo sieci i systemów informatycznych", „cyberbezpieczeństwo" oraz „bezpieczeństwo teleinformatyczne" są synonimami.

Doskonałym przykładem ważnej roli konwencji terminologicznej w realizacji działań jest *Rządowy program ochrony cyberprzestrzeni RP na lata 2009–2011 – założenia*. Lektura owego programu dostarcza interesujących spostrzeżeń. W dokumencie czytamy, iż „w praktyce brak precyzyjnych definicji może powodować wątpliwości polegające na trudności w ustaleniu organu właściwego dla ścigania sprawców cyberprzestępstwa"[23]. Autorzy programu zaznaczyli, że jest on pierwszym rządowym dokumentem całościowo obejmującym kwestie „bezpieczeństwa przestrzeni cybernetycznej państwa". Jednocześnie przyjęcie programu stanowić miało jeden z elementów prewencyjnej polityki państwa,

22 Zob. Ministerstwo Cyfryzacji, *Krajowe ramy polityki cyberbezpieczeństwa*…, dz. cyt.; Ministerstwo Cyfryzacji, *Strategia cyberbezpieczeństwa*…, dz. cyt.

23 Departament Ewidencji Państwowych i Teleinformatyki MSWiA, *Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016*, dz. cyt., s. 10.

dzięki któremu uruchomione miały zostać procesy mogące w dużej mierze przyczynić się do zapobiegania naruszaniu w przyszłości „bezpieczeństwa cyberprzestrzeni państwa". Ponadto wdrożenie programu w latach 2009–2011, zgodnie z założeniami rządu, miało stać się kamieniem milowym w realizacji polityki państwa w obszarze „bezpieczeństwa jego cyberprzestrzeni". W przytoczonych zapisach pojawiają się wieloczłonowe terminy: „bezpieczeństwo przestrzeni cybernetycznej państwa" i „bezpieczeństwo cyberprzestrzeni państwa". Niestety żadne z tych określeń nie zostało sprecyzowane. Należy ponadto zwrócić uwagę na niekonsekwencję terminologiczną. Obok „cyberprzestrzeni" pojawia się „przestrzeń cybernetyczna". Czy to są synonimy? Nie wiadomo.

W programie można również przeczytać, że jako „cyberprzestrzeń państwa" przyjmuje się przestrzeń komunikacyjną tworzoną przez system wszystkich powiązań internetowych znajdujących się w obrębie państwa. Cyberprzestrzeń państwa w przypadku Polski określana jest również mianem cyberprzestrzeni RP. Jak widać, desygnat cyberprzestrzeni RP wskazany w wydanym później dokumencie, czyli *Doktrynie cyberbezpieczeństwa Rzeczypospolitej Polskiej*, nie koresponduje z tym wskazanym w *Rządowym programie*… Zasadne są zatem pytania: „Jaka jest charakterystyka fragmentu rzeczywistości nazwanego cyberprzestrzenią RP? Jakie czynniki go warunkują? Jakie są paradygmaty przedmiotowej rzeczywistości? I ostatecznie, czy cyberprzestrzeń RP to właściwa nazwa?".

W *Rządowym programie*… jest również zapis: „ataki na cyberprzestrzeń państwa". Jednak wzorem poprzednich terminów nie wiadomo, czym one są i czym się charakteryzują. W tym miejscu wypada wspomnieć, że w omawianym dokumencie są również określenia: „ataki o charakterze cyberterrorystycznym"; „ataki cyberterrorystyczne"; „cyberataki"; „ataki z cyberprzestrzeni"; „ataki na cyberprzestrzeń"; „ataki komputerowe"; „ataki wymierzone przeciwko krytycznym systemom i sieciom teleinformatycznym"; „ataki terrorystyczne wykorzystujące publiczne sieci teleinformatyczne"; „ataki na systemy informatyczne"; „ataki z publicznych sieci teleinformatycznych"; „ataki sieciowe"; „ataków symulujących działania cyberterrorystyczne"; „ataki cyberterrorystów". Przedstawiona mnogość terminów może sugerować, że mamy do czynienia z dużym wachlarzem ataków. Ale czy każdy z nich jest czymś innym? Czy może wszystkie stanowią to samo? Przedmiotowy dokument niestety tego nie wyjaśnia.

W skierowanym w 2010 roku do uzgodnień resortowych projekcie *Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016. Wersja 1.1* nie ma definicji cyberbezpieczeństwa. Pojawiają się natomiast sformułowania: „bezpieczeństwo cyberprzestrzeni"; „bezpieczeństwo cyberprzestrzeni RP"; „bezpieczeństwo w cyberprzestrzeni"; „bezpieczeństwo w obszarze cyberprzestrzeni"; „bezpieczeństwo teleinformatyczne"; „bezpieczeństwo w sieci Internet w Polsce"; „bezpieczeństwa krytycznej infrastruktury teleinformatycznej";

„bezpieczeństwo informacji". Niestety przedmiotowy dokument nie precyzuje, co powyższe określenia oznaczają.

Według najnowszego polskiego aktu prawnego: Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa „cyberbezpieczeństwo" rozumiane jest jako „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy"[24].

3. Przedrostek „cyber-"

W kontekście tematu niniejszego opracowania, dla ustalenia właściwej konwencji terminologicznej, należy wyraźnie podkreślić, że cząstka „cyber-" jest w języku polskim prefiksem. Jednak również w sprawie pochodzenia tego prefiksu pojawiają się różne wyjaśnienia.

Według Justyny Błaszczyk cząstka „cyber-" jest w języku polskim członem wyrazów złożonych wskazującym na ich związek z informatyką. Słowo „cyber" w polszczyźnie nie występuje, można jednak tę cząstkę interpretować jako powstałą od przymiotnika „cybernetyczny". W związku z tym derywaty słowotwórcze zaczynające się od „cyber-" należy interpretować jako wyrazy złożone[25].

Zgodnie z opinią Alicji Wódkowskiej „cyber-" jest cząstką słowotwórczą utworzoną od przymiotnika cybernetyczny. Dla zapisywania wyrazów zawierających cząstkę „cyber-" należy przyjąć ogólną zasadę systemową, według której (jak podaje *Wielki słownik ortograficzny PWN*) cząstki słowotwórcze pełniące funkcję tematów słowotwórczych w rzeczownikach złożonych pisze się z wyrazami pospolitymi łącznie. Zatem wyraz złożony z cząstki „cyber-" powinno się zapisać łącznie[26].

Maciej Olszewski, powołując się na *Wielki słownik wyrazów obcych i trudnych* pod redakcją Andrzeja Markowskiego i Radosława Pawelca, wyjaśnia, że cząstka „cyber-" tworzy wraz z rzeczownikami i przymiotnikami złożenia, których pisownia jest łączna. Wyrazy te są związane z komunikowaniem się przez sieć komputerową lub z wirtualną rzeczywistością, na przykład „cyberprzestrzeń", „cybermiłość". Jan Miodek w książce *Słowo jest w człowieku* podkreśla, że element „cyber-" jest otwarty na przyjęcie dowolnego członu utożsamiającego tak powstały

24 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. poz. 1560.

25 Zob. https://fil.ug.edu.pl/strona/15041/w_pewnym_tekscie_reklamowym_zabawce_tamagotchi_zostaly_nadane_nazwy_cyber-kurcze_i_cyber_kurcze (10.03.2020).

26 Zob. https://fil.ug.edu.pl/strona/15040/jak_powinno_zapisac_wyraz_zlozony_z_wyrazow_cyber_i_gadzet (10.03.2020).

derywat z nową rzeczywistością elektroniczną, na przykład program dla dzieci emitowany w telewizji publicznej nosił tytuł *Cybermysz*[27].

Powyższe wskazuje na pewną prawidłowość. Otóż mimo braku jednomyślności w interpretacji prefiksu „cyber-" nie budzi wątpliwości zasada, iż w języku polskim wyrazy poprzedzone tym morfemem pisze się łącznie.

Analiza pochodzenia prefiksu „cyber-" pozwoliła na sformułowanie wniosku, iż powszechnie powielane i przyjmowane znaczenie owego prefiksu jest znacznie uproszczone, a zakres semantyczny zredukowany. Ponadto wyraźnie zauważalny jest fakt, iż wiele znaczeń wyrazów utworzonych z prefiksem „cyber-" znaczeniowo odbiega od właściwego pierwotnego znaczenia samego prefiksu.

Analiza pojęć potwierdza spostrzeżenia Donaty Ochmann[28], iż niejednokrotnie pojęcia utworzone za pomocą morfemu „cyber-" są raczej slangiem bądź radosną twórczością językową. Zauważalna mnogość autorów cybersłów skłania do wniosku, że tworzenie takich słów jest w dobrym tonie. Daje ich autorom poczucie przynależności do pewnej „elitarnej" społeczności. Wytwarza poczucie bycia „na czasie", wpisania się w towarzystwo, w którym wypada bywać.

Andrzej Markowski i Radosław Pawelec również stoją na stanowisku, że cząstka „cyber-" tworzy wraz z rzeczownikami i przymiotnikami złożenia, których pisownia jest łączna. Zauważają także, że cząstka „cyber-" w języku polskim jest pierwszym członem wyrazów złożonych, a zatem łącznie piszemy też złożenia z nią, na przykład „cyberprzestrzeń", „cyberatak", „cyberzagrożenia". Badacze akcentują również, iż słowo „cyber" w polszczyźnie nie występuje, można jednak tę cząstkę interpretować jako powstałą od przymiotnika „cybernetyczny"[29].

Reasumując ów podrozdział, należy z całą mocą podkreślić, że w tak istotnych obszarach dla państwa, jak jego obronność i bezpieczeństwo brak konwencji terminologicznej stanowi poważną barierę.

4. Nowy wymiar życia społecznego

W czasie codziennego funkcjonowania w świecie najnowszych technologii i najnowocześniejszej techniki poczynania zarówno indywidualnych osób, jak i społeczeństw (społeczności) są monitorowanie. Informacje zbierane na ich temat mogą być pomocne w koordynacji i synchronizacji działań skierowanych przeciwko nim. Tradycyjne metody pozyskiwania informacji w określonych warunkach (na przykład w terenie zurbanizowanym o gęstej zabudowie) mogą być zawodne,

27 Zob. https://fil.ug.edu.pl/strona/15039/jedno_z_hasel_organizacji_greenpeace_brzmi_zostac_cyber-aktywista_rzeczownik_zostal_zapisany (8.02.2018).

28 Zob. D. Ochmann, *Złożenia z cyber- we współczesnym języku polskim*, „Język Polski" (2000) nr 1–2 (styczeń/kwiecień), s. 23–34.

29 Por. A. Markowski, R. Pawelec, *Wielki słownik wyrazów obcych i trudnych*, Knurów 2009.

nieskuteczne, a ich użycie znacznie ograniczone. Dlatego urządzenia będące elementami cyberprzestrzeni mogą zastąpić lub uzupełnić tradycyjne metody[30].

Ważną cechą wielu cyberaktywnych czujników jest ich zdolność do śledzenia osób lub pojazdów. Urządzenia mobilne, Wi-Fi, RFID[31] czy systemy oparte na kamerach (na przykład systemy rozpoznawania tablic rejestracyjnych pojazdów) mogą być wykorzystywane do gromadzenia danych i informacji rozpoznawczych. Rozpoznanie może być prowadzone w celu pozyskania informacji o jednym lub większej liczbie obiektów lub w celu identyfikacji i śledzenia określonych celów. Wykorzystując cyberprzestrzeń, można do zbierania informacji użyć geoogrodzenia (*geo-fence*). Oznacza to użycie odpowiednich urządzeń i oprogramowania (w tym aplikacji), które za pomocą globalnego systemu pozycjonowania (GPS – *globalpositioning system*) lub wspomnianej wyżej identyfikacji radiowej (RFID) mogą ustalić obwód lub barierę wokół obszaru geograficznego. Polega to na ustaleniu strefy lub ogrodzenia (wirtualnego) wokół miejsca, które pozostaje w obszarze operacyjnego zainteresowania. Oprogramowanie wykorzystane do geofencingu monitoruje, kiedy urządzenia emitujące falę elektromagnetyczną pojawiają się na ustalonym obszarze lub go opuszczają. Wówczas administratorzy owych urządzeń informowani są o zmianie statusu. Za pomocą tej metody możliwe jest zidentyfikowanie obiektów znajdujących się w określonym obszarze i w konsekwencji oddziaływanie na nie. Funkcja GPS może zostać zakłócona. Możliwy jest także atak GPS Spoofing, który polega na oszukaniu odbiornika GPS poprzez przesłanie sfałszowanego sygnału GPS. Odbiorca wówczas błędnie odczyta dane o własnej lokalizacji, nie wiedząc, że jego współrzędne są inne niż te, które wskazuje urządzenie[32].

Obecnie nikogo nie dziwi znaczna liczba kamer w terenach zabudowanych. Śledzenie życia miasta opiera się na kamerach wideo. Kamery są wszędzie. Niezależnie od tego, czy chodzi o zabezpieczenie obiektu, zapewnienie bezpieczeństwa publicznego, obserwację ulic w ruchu drogowym czy wykonywanie selfie, kamery nieustannie przechwytują dane. Jednak celowe przejęcie nad nimi kontroli, skonfigurowanie lub podporządkowanie ich za pośrednictwem odpowiednich działań w cyberprzestrzeni może posłużyć do wykrywania, rozpoznawania i śledzenia wielu obiektów. Metoda osiągnięcia zamierzonego celu zależy od systemu, należy pamiętać jednak, że wszystkie zależą od rozmieszczenia

30 Zob. R. Janczewski, *Znaczenie cyberprzestrzeni w działaniach hybrydowych*, w: *Zagrożenia hybrydowe*, red. L. Elak i in., Warszawa 2019.

31 RFID (*radio-frequency identification*) – ogólny termin używany do opisania technologii, która umożliwia automatyczną identyfikację obiektu przy użyciu fal radiowych.

32 Zob. R. Janczewski, *Znaczenie cyberprzestrzeni*…, dz. cyt.

kamer i mocy obliczeniowej (rozproszonej lub scentralizowanej) oraz sieci komunikacyjnych[33].

Niektóre systemy proponują wykorzystanie do komunikacji niewykorzystanych częstotliwości. Inne pozwalają użytkownikom wyszukiwać w swojej bazie dane na temat zdarzeń, generować alerty, a nawet przewidywać przyszłe zdarzenia. Po podłączeniu urządzeń wykorzystujących sztuczną inteligencję do nowoczesnych systemów i algorytmów przetwarzania sygnałów dane pochodzące z kamer mogą dostarczyć cennych informacji. Tego typu sieć czujników może umożliwiać stałą identyfikację i śledzenie zasobów zarówno ludzkich, jak i materialnych czy niematerialnych miasta[34].

Powszechnie wiadomo, że standard Wi-Fi wykorzystywany jest do budowy bezprzewodowych sieci komputerowych. Szczególnym zastosowaniem Wi-Fi jest budowanie sieci lokalnych (LAN – *localarea network*) opartych na komunikacji radiowej, czyli WLAN (*wirelesslocalarea network*). Również ten standard może zostać wykorzystany do prowadzenia działań skierowanych przeciwko społeczeństwu[35].

Udoskonalone algorytmy przetwarzania sygnałów oraz tańsza moc przetwarzania umożliwiają stosowanie różnych technik śledzenia opartych na promieniowaniu elektromagnetycznym. Również standard Wi-Fi może być wykorzystany do śledzenia ruchu. Sygnały Wi-Fi mogą być wykorzystywane do wykrywania ruchu ludzi, którzy mogą zostać obrani jako cel. Do wykrywania ruchu wykorzystywane są cechy sygnałów Wi-Fi takie jak siła odbieranego sygnału, jego faza, czas transmisji czy informacja o stanie kanału transmisyjnego. Systemy te mają ograniczony zasięg i możliwości, ale biorąc pod uwagę powszechną dostępność węzłów Wi-Fi w terenach o gęstej zabudowie, technologia ta może zostać wykorzystana w celu pozyskania informacji o ruchu obiektów pozostających w obszarze operacyjnego zainteresowania. Sygnały otrzymane z wielu źródeł (np. Wi-Fi, Bluetooth, 4G LTE, GPS, NFC) mogą posłużyć do mapowania ruchu obiektów w konkretnych rejonach czy obszarach[36].

Telefony komórkowe lub inne urządzenia, które łączą się z sieciami komórkowymi, zapewniają możliwości śledzenia. Każde z tych urządzeń dostarcza identyfikator do węzłów komórki, z którą się łączy, nawet jeśli urządzenie nie jest aktywnie transmisyjnie. Ta informacja jest łatwo dostępna w węzłach komórkowych i może być wykorzystana do śledzenia ruchów urządzeń. Z punktu pozyskiwania informacji o obiektach może to być pomocne w nominowaniu

33 Zob. R. Janczewski, *Znaczenie cyberprzestrzeni*…, dz. cyt.
34 Zob. R. Janczewski, *Znaczenie cyberprzestrzeni*…, dz. cyt.
35 Zob. R. Janczewski, *Znaczenie cyberprzestrzeni*…, dz. cyt.
36 Zob. R. Janczewski, *Znaczenie cyberprzestrzeni*…, dz. cyt.

celu. Dlatego należy zwiększyć ochronę na przykład tych przywódców, którzy posiadają takie urządzenia[37].

Godną uwagi w aspekcie roli cyberprzestrzeni w działaniach skierowanych przeciwko społeczeństwu implementacją sieci obliczeniowej opartej na Internecie rzeczy lub inaczej Internecie przedmiotów (IoT – *Internet of things*) jest idea inteligentnego miasta. Inteligentne miasto jest w swej istocie skomplikowanym systemem złożonym z niezwiązanych ze sobą usług kluczowych, takich jak system informacji o środowisku, inteligentna sieć energetyczna, informacje o podróżach, gospodarka odpadami, planowanie przestrzenne, inteligentne liczniki, reagowanie w sytuacjach kryzysowych czy inteligentne wydarzenia, które są integrowane we wspólną strukturę (zwykle poprzez wdrażanie stosu[38] technologii dużych zbiorów danych). Jednak pomimo postępujących trendów integracji systemów w różnych branżach, podobnie jak w inteligentnym mieście, systemy nadzoru wideo są wdrażane i administrowane nadal jako samodzielne systemy. Dane wideo pochodzą z każdej z osobna monitorującej kamery będącej częścią dużego wolumenu sensorów rejestrujących obraz. Niestety nie jest dokonywana agregacja danych i informacji oraz ich analiza. Wynika to głównie z powodu złożoności aspektów prawnych, technicznych, finansowych, społeczno-kulturowych, bezpieczeństwa czy wartości etycznych, takich jak na przykład:

- ochrona danych – właściciele systemów nadzoru wideo odpowiedzialni są za ochronę prywatności osób zarejestrowanych podczas monitoringu;
- własność danych – właściciele systemów nadzoru wideo obawiają się udostępniania wyników obserwacji, ponieważ mogliby utracić prawa do własności danych oraz kontrolę nad nimi;
- wysokie koszty inwestycyjne – systemy nadzoru były zazwyczaj instalowane w strukturze budynku. Właściciele systemów nadzoru wideo obawiają się, że wymiana systemu monitoringu może zakłócić wiele innych usług, a koszty inwestycji mogą być zbyt duże lub nieuzasadnione;
- niekompatybilność systemów – wynika z konfiguracji systemu przez producenta czy dostawcy, a także kodowania danych. Dane i informacje z jednej kamery mogą mieć format, który nie będzie zgodny ze standardami przyjętymi dla innego urządzenia rejestrującego obraz;
- bezproduktywne wykorzystanie przepustowości – ciągła transmisja obrazu przez kilka kamer w sieci może okazać się niecelowa, ponieważ obraz wideo może nie zawierać zdarzeń mających znaczenie dla monitorujących.

37 Zob. R. Janczewski, *Znaczenie cyberprzestrzeni*…, dz. cyt.

38 Stos (*stack*) – liniowa struktura danych, w której dane dokładane są na wierzch stosu i z jego wierzchołka pobierane; taki sposób zarządzania danymi nazywany jest buforem typu LIFO (*last in, first out*, czyli ostatni na wejściu, pierwszy na wyjściu).

W trakcie przygotowania się do działań w cyberprzestrzeni intruz może pozyskać dane i informacje, a następnie zdobytą wiedzę wykorzystać przeciwko podmiotowi, wobec którego to działanie zostanie skierowane. Wiele danych i informacji pozyskanych z, wydawać by się mogło, nieistotnych z punktu widzenia rozpoznania i oddziaływania usług może być wykorzystanych w scenariuszu działań hybrydowych[39].

Przykładem jest usługa inteligentne wydarzenie (*smart event*). Ta z pozoru niewinna usługa jest wysoce wyrafinowanym rozwiązaniem. Integruje w procesie planowania wydarzeń najnowocześniejsze rozwiązania technologiczne, takie jak analiza danych zgromadzonych w wielkich bazach lub wręcz hurtowniach danych, sztuczna inteligencja oraz wirtualna rzeczywistość. W rozwiązaniu *smart event* celem zastosowania najnowszych technologii jest zautomatyzowanie zarządzania wydarzeniami. Oferta skierowana jest zarówno dla menadżera, jak i uczestnika. Inteligentne panele kontrolne, widżety i dedykowane wydarzeniom aplikacje, systemy sprzedaży biletów online, beacony, aplikacje rzeczywistości rozszerzonej (AR – *augmented reality*) i rzeczywistości wirtualnej (VR – *virtual reality*) czy chatboty sprawiają, że rozwiązania do zarządzania zdarzeniami stają się źródłami informacji, na których podstawie możliwe jest budowanie baz danych o wydarzeniach, ich popularności (skupiska ludzkie), uczestnikach (sieć kontaktów), ich zainteresowaniach, podatności na nowe, czasem sensacyjne informacje. Zdobywane informacje ułatwiają konstruowanie fałszywych wiadomości (*fake news*) oraz budowanie socjotechnicznych cyberataków czy dobór wektora ataku. Z pozoru nieszkodliwe beacony mogą stać się narzędziem do przeprowadzenia cyberataku. Te niewielkich rozmiarów nadajniki (zwane latarniami) emitują pulsacyjnie sygnał Bluetooth i przeznaczone są do nawiązania połączenia z aplikacją w telefonie i wyświetlania potrzebnych (lub zmanipulowanych) informacji. Mogą również wpływać na nasze zachowanie, na przykład skierować nas w określone miejsce i wywołać jednocześnie panikę, co w dużych skupiskach ludzkich może być zgubne w skutkach. Beacony wykorzystują czwartą generację technologii Bluetooth (Bluetooth Smart lub Bluetooth Low Energy – BLE), która dostępna jest w nowych smartfonach i tabletach[40].

Chatboty (chatterboty lub linguaboty), czyli programy komputerowe stosowane do prowadzenia konwersacji w naturalnym języku człowieka, sprawiające wrażenie inteligentnych, również mogą posłużyć do przeprowadzania cyberataków. Chatboty mają na celu sprawić wrażenie, żeby rozmówca był przekonany, iż rozmawia z innym człowiekiem. Chatboty wykorzystywane są w serwisach

39 Zob. R. Janczewski, *Znaczenie cyberprzestrzeni*…, dz. cyt.
40 Zob. R. Janczewski, *Znaczenie cyberprzestrzeni*…, dz. cyt.

internetowych jako interaktywne, wirtualne postaci, pełniące funkcję konsultantów. Odpowiadają klientom na pytania z zakresu usług czy działalności określonej firmy. Manipulacja oprogramowania może z łatwością dostarczać niewłaściwych informacji, udzielać wiadomości o odpowiedniej, zamierzonej przez adwersarza osi narracji. Pojęcie chatterbota ściśle wiąże się ze sztuczną inteligencją. Należy jednak mieć świadomość, że takie cechy jak autonomiczność i zdolność adaptacji czynią ze sztucznej inteligencji niebezpieczną technologię. Dlatego o ochronie własnych zasobów, które mogą stać się dostępne poprzez cyberprzestrzeń, należy myśleć już teraz. Nabiera to szczególnego znaczenia w kontekście teorii kwantowej wykorzystanej do budowania komputerów przyszłości – komputerów kwantowych.

Należy również zwrócić uwagę na rzeczywistość rozszerzoną czy rzeczywistość wirtualną. Cyberprzestrzeń stwarza warunki do oddziaływania na systemy wykorzystujące obie technologie[41].

Rzeczywistość rozszerzona jest technologią, która na obiekty rzeczywiste nakłada grafikę komputerową. Takie nałożone warstwy cyfrowe mogą zawierać modele 3D, określone obiekty, dane tekstowe czy obrazy wideo. Scenariusz działań hybrydowych może obejmować oddziaływanie na systemy wykorzystujące rzeczywistość rozszerzoną. W medycynie, dzięki obrazowaniu medycznemu, możliwy jest dostęp do danych na temat zdrowia pacjenta, struktury i czynności jego narządów wewnętrznych. W lotnictwie instrumenty pokładowe pokazują lotnikom wiele istotnych z punktu widzenia bezpieczeństwa lotu danych, na przykład dotyczących ukształtowania terenu, który piloci widzą przed sobą. W motoryzacji kluczowe informacje lub obrazy, na przykład z komputera pokładowego, radia lub systemu nawigacji, wyświetlane są na przedniej szybie samochodu lub motocykla. Rozwiązanie to zwiększa możliwość zachowania bezpieczeństwa jazdy, ponieważ kierujący nie musi odrywać wzroku od drogi. Nieuprawniony dostęp do komputerów generujących elementy rzeczywistości rozszerzonej może być zgubny w skutkach, na przykład przyczynić się do katastrof w ruchu powietrznym lub lądowym[42].

Rzeczywistość wirtualna (lub inaczej fantomatyka) jest technologią wytwarzania rzeczywistości pozornej za pomocą informatyki (komputerów). Polega ona na multimedialnym tworzeniu komputerowej wizualizacji przedmiotów, przestrzeni i zdarzeń. Rzeczywistość wirtualna może być reprezentacją tak elementów świata realnego (symulacje komputerowe), jak i zupełnie fikcyjnego (gry komputerowe). Wpłynięcie na rzeczywistość wirtualną symulatorów lotów lub nawigacji okrętów poprzez nieuprawnioną modyfikację kodów źródłowych ich

41 Zob. R. Janczewski, *Znaczenie cyberprzestrzeni*…, dz. cyt.
42 Zob. R. Janczewski, *Znaczenie cyberprzestrzeni*…, dz. cyt.

oprogramowania może skutkować wyrabianiem podczas treningów i ćwiczeń nawyków opartych na błędnych parametrach. Modyfikacja oprogramowania przeprowadzającego symulacje projektów ważnych z punktu widzenia bezpieczeństwa i obronności państwa może doprowadzić do oddania do produkcji na przykład urządzeń mających nieprzewidywalne usterki[43].

Smartfony przeznaczone są głównie do komunikacji między ludźmi i są szczególnie łatwe w użyciu w sieciach społecznościowych, ale mogą stwarzać znaczne zagrożenie, jeśli mają również dostęp do sieci lokalnej.

Liczne aplikacje na urządzenia mobilne służą do łączenia się ze społecznościami wirtualnymi w celu udostępniania informacji lub mediów. W niektórych przypadkach sieci społecznościowe są przeznaczone dla urządzeń przenośnych i często koncentrują się na informacjach opartych na lokalizacji. Użytkownik urządzenia mobilnego, który ma dostęp do sieci lokalnej, nawet bez żadnego złośliwego oprogramowania zainstalowanego na urządzeniu może doprowadzić do wycieku danych z sieci lokalnej za pośrednictwem sieci społecznościowych.

Możliwe zagrożenia: inżynieria społeczna, nieumyślne ujawnienie danych dotyczących lokalizacji, przesyłanie lub pobieranie złośliwych linków lub plików oraz wyciek poufnych informacji.

Zakończenie

Jednym z negatywnych skutków informatyzacji funkcjonowania społeczeństwa jest zagrożenie jego bezpieczeństwa. Możliwości, jakie niosą najnowocześniejsze sieci i systemy teleinformatyczne oraz ich ogólnoświatowy zasięg, narażają społeczeństwa na cyberataki ze strony zarówno państwowych, jak i niepaństwowych przestępczych lub wrogich elementów. Podmioty przeprowadzające cyberataki stają się coraz bieglejsze i skuteczniejsze w unikaniu wykrycia. Dysponują coraz to skuteczniejszymi narzędziami, opartymi na szyfrowaniu wykorzystującym silne algorytmy oraz na bardziej zaawansowanych i wyrafinowanych taktykach, takich jak na przykład wykorzystywanie legalnych usług internetowych w celu ukrycia własnych działań oraz osłabienia dotychczasowych technik cyberbezpieczeństwa. Podmioty te ciągle rozwijają taktyki działań, aby ich narzędzia i oprogramowanie złośliwe były wciąż aktualne i skuteczne. Dzięki temu identyfikacja cyberzagrożeń (nawet tych znanych) może okazać się czasochłonna i wymagająca zaangażowania znacznych, wyspecjalizowanych do tego celu zasobów państwa.

Problem badawczy ujęty w postaci pytania „Jaka jest charakterystyka cyberbezpieczeństwa w społeczeństwie?" został rozwiązany. Wyniki badań pozwoliły

43 Zob. R. Janczewski, *Znaczenie cyberprzestrzeni*…, dz. cyt.

na sformułowanie wniosku, że cyberbezpieczeństwo nie ma jednej powszechnie uznanej definicji, jednak należy z pragmatycznego punktu widzenia przyjąć za ustawą, że jest to „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy".

Odpowiedź na pytanie „Jakie są cyberzagrożenia w życiu społecznym?" daje jednoznaczny obraz współczesnego świata. Otóż każdy sektor funkcjonowania społeczeństwa pozostaje w zainteresowaniu podmiotów wykorzystujących cyberprzestrzeń do przeprowadzenia wrogich działań przeciwko niemu. Działania skierowane były zarówno przeciwko siłom zbrojnym, jak i obiektom niebędącym militarnym potencjałem państwa. Wyzwania, przed którymi stoją państwa w dziedzinie najnowocześniejszych rozwiązań teleinformatycznych, w znacznie większym stopniu niż w innych dziedzinach dotykają szeroko zakrojonych międzynarodowych procesów gospodarczych, społecznych, kulturowych czy technologicznych.

W kwestii charakteru cyberataków przeprowadzonych przeciwko państwom badania pozwalają sformułować wniosek, że jednowymiarowy, terytorialny obraz konfliktu zmienił się w wielowymiarowy, wielopoziomowy kompleks działań militarnych i niemilitarnych służących osiąganiu niejednokrotnie zróżnicowanych celów. Możliwość anonimizacji działań przeciwko społeczeństwu niestety nie pozwala ze stuprocentową pewnością wskazać, czy cyberatak przeprowadzony został przez siły zbrojne wrogiego państwa czy nie.

W kontekście tematu niniejszego opracowania warto pamiętać o cyberatakach przeprowadzonych przeciwko państwom, które miały miejsce w ostatnich latach. Ocena rozwoju cyberprzestrzeni i ataków cybernetycznych pokazuje, że na początku ataki te miały na celu szpiegostwo i pozyskiwanie informacji, jednak z czasem były przeprowadzane z większą siłą i intensywnością. Wraz z rozwojem społeczeństw stało się oczywiste, że cyberatak umożliwia nie tylko wydobycie informacji, wykorzystanie ich do zakłócania procesów krytycznych, a nawet powodowania szkód fizycznych i śmierci, ale także wyrządzenie szkód psychicznych.

Przeciwko państwom przeprowadzono cyberataki o różnym charakterze. Były to cyberataki ukierunkowane, często sponsorowane przez inne państwo, choć niektóre z nich przeprowadziły podmioty prywatne. Cyberprzestrzeń została wykorzystana przeciwko społeczeństwom w celu przeprowadzenia działań szpiegowskich, zakłócenia ich prawidłowego funkcjonowania, sabotowania mechanizmów demokracji, na przykład wyborów prezydenckich, sabotowania właściwego działania infrastruktury krytycznej lub kradzieży zasobów finansowych czy wszelkich danych i informacji. Do ich przeprowadzenia wykorzystywano typowe narzędzia techniczne, a także metody socjotechniczne.

Bibliografia

Publikacje zwarte

Janczewski R., *Znaczenie cyberprzestrzeni w działaniach hybrydowych*, w: *Zagrożenia hybrydowe*, red. L. Elak i in., Warszawa 2019.

Markowski A., Pawelec R., *Wielki słownik wyrazów obcych i trudnych*, Knurów 2009.

Unold J., *Teoretyczno-metodologiczne podstawy przetwarzania informacji w cyberprzestrzeni*, Wrocław 2011.

Artykuły

Drożdż M., *Świadomość działania jako podstawa etycznego wartościowania*, „Studia Socialia Cracoviensia" 10 (2018) nr 2 (19), s. 11–20.

Ochmann D., *Złożenia z cyber- we współczesnym języku polskim*, „Język Polski" (2000) nr 1–2 (styczeń/kwiecień), s. 23–34.

Dokumenty

Biuro Bezpieczeństwa Narodowego, *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Warszawa 2015.

Departament Ewidencji Państwowych i Teleinformatyki MSWiA, *Rządowy program ochrony cyberprzestrzeni RP na lata 2009–2011 – założenia*, Warszawa 2009.

Departament Ewidencji Państwowych i Teleinformatyki MSWiA, *Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016. Wersja 1.1*, Warszawa 2010.

Ministerstwo Administracji i Cyfryzacji, *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*, Warszawa 2013.

Ministerstwo Cyfryzacji, *Krajowe ramy polityki cyberbezpieczeństwa Rzeczpospolitej Polski na lata 2017–2022*, Warszawa 2017.

Ministerstwo Cyfryzacji, *Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*, Warszawa 2017.

Rządowe Centrum Bezpieczeństwa, *Narodowy program ochrony infrastruktury krytycznej – tekst jednolity*, załącznik 1, *Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje*, Warszawa 2015.

Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, Dz.U. Nr 156, poz. 1301.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. poz. 1560.

Strony internetowe

https://encyklopedia.pwn.pl/ (31.01.2018).

https://fil.ug.edu.pl/ (10.03.2020).

https://sjp.pwn.pl/ (10.01.2020).

https://www.bbn.gov.pl/ (30.11.2019).