Sławomir Stalmach[1]
ORCID: 0000-0001-5679-4645

Cztery obszary cyberbezpieczeństwa — omówienie zakresu tematycznego

Wstęp

Cyberbezpieczeństwo kojarzy się z zapewnieniem bezpieczeństwa dla funkcjonowania infrastruktury, urządzeń i sprzętu elektronicznego, ale także z ochroną informacji oraz danych w internecie. Mniej więcej wiemy, jak zadbać o rzeczy materialne, takie jak nadajniki, serwery itd., ale mniej rozumiemy pojęcie środowiska internetowego, czyli cyberprzestrzeni, gdzie znajdują się treści, które chcemy ochronić. Równocześnie rozszerzają się pojęcia przestępczości i wojny hybrydowej, a więc mające swoje skutki zarazem w świecie materialnym i wirtualnym. Cyberbezpieczeństwo jest wyzwaniem dla zagrożeń hybrydowych.

Zakres definicyjny cyberbezpieczeństwa obejmuje cztery obszary, które powinny być omawiane wspólnie:

1. prawo dotyczące cyberprzestrzeni,
2. system bezpieczeństwa i instytucje odpowiedzialne za cyberbezpieczeństwo,
3. internet, rozumiany jako środowisko medialne,
4. przestrzeń internetu, która jest nowym środowiskiem społecznym.

Nie da się stworzyć spójnego systemu bezpieczeństwa w cyberprzestrzeni, gdy z jakiegoś powodu pominie się któryś z przedstawionych obszarów.

Obszar 1. Prawo dotyczące cyberprzestrzeni

Nie ma na razie jednolitego określenia cyberprzestrzeni, a próby definicji tego pojęcia mają ogólny charakter. Tak pisze Cezary Banasiński: „W literaturze brak jest powszechnie akceptowanego pojęcia informacji; w pewnym sensie jest to termin złożony, interdyscyplinarny, definiowany

[1] Sławomir Stalmach — zajmuje się analizą bezpieczeństwa informacyjnego w ramach Akademickiego Centrum Polityki Cyberbezpieczeństwa Akademii Sztuki Wojennej, a także pisze doktorat z socjologii w Collegium Civitas w Warszawie.
Adres do korespondencji: <s.stalmach@akademia.mil.pl>.

odmiennie w różnych naukach, niemający jednoznacznej, powszechnej definicji”[2].

Polskie prawo penalizuje przestępstwa występujące w cyberprzestrzeni w wielu aspektach, w tym dotyczące: kradzieży, fałszerstwa, zniszczenia, oszustwa, podżegania do działań przestępczych, stalkingu itd. Polska ratyfikowała w 2014 r. Konwencję Rady Europy o cyberprzestępczości[3]. Wprowadzono do polskiego prawa, głównie do kodeksu karnego[4], wiele zapisów dotyczących przestępczości związanej z sieciami i komputerami. Przykładowo, artykuł 267 § 1 kk stanowi: „Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2”[5].

Rzeczywistość zawsze wyprzedza prawodawstwo, szczególnie, gdy mamy do czynienia z dynamicznie zagęszczającą się przestrzenią internetową. Stale też pojawiają się nowe rodzaje naruszeń prawa, które obecnie najczęściej mają angielskie określenia, takie jak: *sniffing*, czyli przechwytywanie danych; *spoofing*, czyli podszywanie się pod inny element systemu informatycznego; *phishing*, czyli wyłudzanie poufnych danych i inne[6]. Piotr Kardas zauważa, że: „Wraz ze wzrostem liczby podmiotów uzyskujących dostęp do cybernetycznych systemów gromadzących i przetwarzających informacje, których symbolem jest obecnie sieć internetowa umożliwiająca praktycznie każdemu dostęp do informacji oraz możliwość jej kreatywnego kształtowania, pojawia się coraz więcej pól potencjalnych konfliktów, u podłoża których leży dostępność do źródeł informacji, a także możliwość ich wykorzystywania oraz wpływania na ich kształt”[7].

Definicja cyberbezpieczeństwa w polskim prawie

Katarzyna Chałubińska-Jentkiewicz zwraca uwagę, że zapisy prawne dotyczące cyberbezpieczeństwa w Polsce nie są zebrane w jedną całość. „Podkreślić należy, że przepisy prawne, które zaliczyć można dzisiaj do tych regulujących problematykę cyberbezpieczeństwa są bardzo często

[2] C. Banasiński, *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018, s. 21.

[3] Ustawa z 12 września 2014 r. o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w 23 listopada 2001 r. (DzU z 2014 r., poz. 1514).

[4] Ustawa z 6 czerwca 1997 r. — Kodeks karny (DzU z 1997 r., nr 88, poz. 553; dalej jako: k.k.).

[5] Tamże, art. 267 § 1.

[6] Więcej F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016.

[7] P. Kardas, *Oszustwo komputerowe w kodeksie karnym*, „Czasopismo Prawa Karnego i Nauk Penalnych” 2000, z. 1, s. 29.

rozproszone, obejmujące bardzo różne obszary życia. Problemu tego rozproszenia nie rozwiązała ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa”[8].

Pomimo tych zastrzeżeń należy zauważyć, że w ustawie o krajowym systemie cyberbezpieczeństwa podjęto próbę zdefiniowania określenia cyberbezpieczeństwa jako: „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy”[9].

Niemal równolegle do ustawy o krajowym systemie cyberbezpieczeństwa przyjęto Strategię Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024[10]. Tak o Strategii mówił Marek Zagórski, minister cyfryzacji: „Przyjęcie w 2018 r. ustawy o krajowym systemie cyberbezpieczeństwa stworzyło podstawy prawne i organizacyjne dla zbudowania, po raz pierwszy w historii, kompleksowego systemu cyberbezpieczeństwa w Polsce. System ten będzie ciągle rozwijany, co zostało jasno wskazane w jednym z celów szczegółowych określonych w Strategii. Ponadto, wskazano na priorytety rządu RP w obszarze bezpieczeństwa informacji”[11].

Następnie, w Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, która została przyjęta w maju 2020 r., wyróżniono cyberbezpieczeństwo w pierwszym filarze, opisującym bezpieczeństwo państwa i obywateli. Cyberbezpieczeństwo uplasowano nie bez kozery pomiędzy zapisami dotyczącymi sił zbrojnych Rzeczypospolitej Polskiej oraz przestrzenią informacyjną, co wskazuje na ich nierozerwalny związek. „W kontekście rewolucji cyfrowej należy uwzględnić szczególną rolę cyberprzestrzeni oraz przestrzeni informacyjnej”[12].

Specyficzne zadania zapisane w Strategii Bezpieczeństwa Narodowego, które są związane ze sferą cyberbezpieczeństwa to:

„4. Podniesienie poziomu odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji:

4.1 Zwiększać poziom odporności systemów informacyjnych wykorzystywanych w sferze publicznej i prywatnej oraz militarnej i cywilnej oraz osiągnąć zdolność do skutecznego zapobiegania, zwalczania oraz reagowania na cyberzagrożenia.

---

[8] K. Chałubińska-Jentkiewicz, *Cyberodpowiedzialność*, Toruń 2019, s. 16.

[9] Ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (DzU z 2018 r., poz. 1560), art. 2 pkt 4.

[10] Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, <https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024>, 18 grudnia 2020 r.

[11] Tamże, s. 2.

[12] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, <https://www.bbn.gov.pl/pl/wydarzenia/8806,Strategia-Bezpieczenstwa-Narodowego-Rzeczypospolitej-Polskiej.html>, 18 grudnia 2020 r.

4.2 Wzmacniać defensywny potencjał państwa poprzez zapewnienie ciągłego rozwoju krajowego systemu cyberbezpieczeństwa.

4.3 Uzyskać zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni.

4.4 Rozwijać krajowe zdolności w obszarze testowania, badania, oceny i certyfikacji rozwiązań i usług z obszaru cyberbezpieczeństwa.

4.5 Rozwijać kompetencje, wiedzę oraz świadomość zagrożeń i wyzwań wśród kadr administracji publicznej oraz w społeczeństwie w obszarze cyberbezpieczeństwa.

4.6 Wzmacniać i rozbudowywać potencjał państwa m.in. poprzez rozwój rodzimych rozwiązań w zakresie cyberbezpieczeństwa oraz prowadzenie finansowanych przez państwo prac badawczo-rozwojowych w obszarze nowoczesnych technologii, m.in. uczenia maszynowego, Internetu Rzeczy, szerokopasmowych sieci łączności stacjonarnej i mobilnej (5G i kolejnych generacji), w tym także współpracę z uczelniami i instytucjami naukowymi oraz przedsiębiorstwami — zarówno z sektora publicznego, jak i prywatnego”[13].

Natomiast opisane w Strategii specyficzne zadania związane z przestrzenią informacyjną to:

„5. Zapewnienie bezpiecznego funkcjonowania państwa i obywateli w przestrzeni informacyjnej:

5.1 Na poziomie strategicznym zbudować zdolności do ochrony przestrzeni informacyjnej (w tym do systemowego zwalczania dezinformacji), rozumianej jako przenikające się warstwy przestrzeni: wirtualnej (warstwa systemów, oprogramowania i aplikacji), fizycznej (infrastruktury i sprzętu) i poznawczej (kognitywnej).

5.2 Stworzyć jednolity system komunikacji strategicznej państwa, którego zadaniem powinno być prognozowanie, planowanie i realizowanie spójnych działań komunikacyjnych, przy wykorzystaniu szerokiej gamy kanałów komunikacji i mediów oraz wykorzystywać narzędzia rozpoznania oraz oddziaływania w różnych obszarach bezpieczeństwa narodowego.

5.3 Aktywnie przeciwdziałać dezinformacji poprzez budowę zdolności i stworzenie procedur współpracy z mediami informacyjnymi oraz społecznościowymi, przy zaangażowaniu obywateli i organizacji pozarządowych.

5.4 Dążyć do zwiększenia świadomości społecznej o zagrożeniach związanych z manipulacją informacją poprzez edukację w zakresie bezpieczeństwa informacyjnego”[14].

Na koniec oczywiste zalecenie, które znalazło się w Strategii Bezpieczeństwa Narodowego: „Zapisy zawarte w niniejszym dokumencie powinny znaleźć rozwinięcie i odzwierciedlenie w krajowych dokumentach strategicznych w dziedzinie bezpieczeństwa narodowego i rozwoju Polski”[15].

[13] Tamże, s. 20.

[14] Tamże, s. 21.

[15] Tamże, s. 5.

Obszar 2. System bezpieczeństwa i instytucje odpowiedzialne za cyberbezpieczeństwo

Najważniejszymi pojęciami, które definiują krajowy system cyberbezpieczeństwa są: infrastruktura krytyczna, cyfrowe usługi kluczowe oraz sposoby reagowania na tzw. incydenty bezpieczeństwa komputerowego.

System bezpieczeństwa w naszym kraju przewiduje ochronę infrastruktury obejmującej systemy łączności i sieci teleinformatycznych, ponieważ są to zasoby, które mają podstawowe znaczenie dla bezpiecznego funkcjonowania gospodarki i społeczeństwa. W tym kontekście mówi się o tzw. infrastrukturze krytycznej, czyli o obiektach, urządzeniach, instalacjach i systemach. Art. 3. 2) ustawy o zarządzaniu kryzysowym[16] definiuje, co należy rozumieć pod pojęciem infrastruktury krytycznej, a więc są to: „(…) systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie 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”[17].

Natomiast ustawa o krajowym systemie cyberbezpieczeństwa z 2018 r. wprowadza pojęcie cyfrowych usług kluczowych i ich operatorów[18].

Operatorami stają się podmioty (zarówno przedsiębiorcy, jak i podmioty publiczne), które:

— świadczą usługi kluczowe,
— świadczenie tych usług jest zależne od systemów informacyjnych,
— incydent w tym podmiocie miały istotny skutek zakłócający dla świadczenia tej usługi.

Operatorami są zatem podmioty, które prowadzą działalność gospodarczą m.in.: w zakresie transportu, zarządzania drogami, wydobywania kopalin, wytwarzania, przesyłania i dystrybucji energii elektrycznej, zarządzania infrastrukturą energetyczną, wytwarzania i przesyłania ciepła, magazynowania i przesyłania paliw ciekłych i gazowych, obrotu i dystrybucji produktów leczniczych, bankowości i infrastruktury rynków finansowych oraz dostarczania usług cyfrowych. Pełen wykaz usług kluczowych znajduje się w rozporządzeniu Rady Ministrów z 11 września 2018 r.[19]

Kolejnym bardzo ważnym pojęciem dla systemu bezpieczeństwa w cyberprzestrzeni jest określenie, czym jest incydent bezpieczeństwa komputerowego oraz jakie instytucje są obowiązane do reakcji na incydent. Ogólnie, w tym aspekcie, definiuje się, że: „incydent to zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo”[20]. Natomiast tzw.

[16] Ustawa z 26 kwietnia 2007 r. o zarządzaniu kryzysowym (DzU z 2007 r., nr 89 poz. 590).

[17] Tamże, art. 3. 2).

[18] Ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (DzU z 2018 r., poz. 1560; dalej jako: ustawa o krajowym systemie cyberbezpieczeństwa).

[19] Rozporządzenie Rady Ministrów z 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (DzU z 2018 r., poz. 1806).

[20] Ustawa o krajowym systemie cyberbezpieczeństwa, art. 2. 5.

obsługa incydentu to: „czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu”[21].

Zespoły reagowania na incydenty działają na obszarach samorządów i w poszczególnych przedsiębiorstwach, natomiast na poziomie krajowym wyróżnia się trzy zespoły. Ich nazwa, czyli CSIRT, jest skrótowcem od angielskiego określenia: *Computer Security Incident Response Team* (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego). Są to zespoły: CSIRT NASK, CSIRT GOV oraz CSIRT MON.

Pierwszy z nich działa w strukturach NASK, czyli Naukowej i Akademickiej Sieci Komputerowej — państwowego instytutu badawczego. Odpowiada m.in. za koordynację incydentów zgłaszanych przez samorząd terytorialny, uczelnie i poszczególnych obywateli. Drugi jest prowadzony przez Agencję Bezpieczeństwa Wewnętrznego i nadzorowany przez resort odpowiadający za cyfryzację. Odpowiada za koordynację incydentów zgłaszanych przez główne organy władzy publicznej. Trzeci zespół prowadzi Ministerstwo Obrony Narodowej dla podmiotów podległych bezpośrednio ministrowi obrony.

Przykładowo, zadaniem Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT GOV) jest: „(...) rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z 26 kwietnia 2007 r. o zarządzaniu kryzysowym[22]”.

Zasoby internetowe

Internet dzieli się na część ogólnodostępną i część zamkniętą. Ta pierwsza, otwarta, to pasaż w galerii handlowej, gdzie właściciele witryn wystawiają na widok publiczny towar, który chcą zareklamować. Druga część zamknięta to bazy danych, mechanika obsługi poszczególnych witryn, półprodukty, wersje robocze itd. Stosunek obu części do siebie wynosi przypuszczalnie jeden do dziesięciu (zasoby internetowe są bardzo trudne do oszacowania[23]). To, co widzimy, jest ledwie małą częścią tego, czego nie widzimy, bo należy to do tajemnic właścicieli poszczególnych stron internetowych. Szczególnym fragmentem internetu są zasoby, do których

[21] Tamże, art. 2. 10.

[22] Ustawa z 26 kwietnia 2007 r. o zarządzaniu kryzysowym (DzU z 2007 r., nr 89, poz. 590); Portal internetowy CSIRT GOV, <https://csirt.gov.pl/>, 11 grudnia 2020 r.

[23] O. Wasiuta, R. Klepka (red.), *Vademecum bezpieczeństwa informacyjnego,* Kraków 2019.

droga dojścia jest specjalnie i automatycznie anonimizowana. Ten wycinek internetu bywa różnie nazywany, np.: *dark web* (mroczna sieć), tor lub sieć cebulowa (skrót tor pochodzi od angielskiej nazwy: *The Onion Router* — cebulowy trasownik, czyli rodzaj urządzenia łączącego różne sieci komputerowe). Wbrew pozorom wejście do tego fragmentu internetu nie jest trudne, a zabezpieczenie w postaci trasowania cebulowego (warstwowego) daje złudne poczucie bezkarności. Jednak, czy to w internecie, czy to w realu, ukrywanie przestępczej działalności spotyka się z reakcją policji i służb specjalnych. Nie ma czegoś takiego jak nielegalny internet, natomiast niektóre treści istniejące w sieci są niewątpliwie nielegalne. Dotyczy to m.in. handlu narkotykami i bronią, rozpowszechniania treści pornograficznych z udziałem dzieci, nawoływania do działań terrorystycznych.

Do zwalczania wrogich i przestępczych działań w cyberprzestrzeni są zobligowane: policja oraz wszelkie agencje obronne, cywilne i wojskowe, takie jak Agencja Bezpieczeństwa Wewnętrznego, czy Służba Kontrwywiadu Wojskowego. Warto wyróżnić policyjne Biuro do Walki z Cyberprzestępczością, które ma tworzyć warunki do „efektywnego wykrywania sprawców przestępstw popełnionych przy użyciu nowoczesnych technologii teleinformatycznych”[24]. Także należy wspomnieć o planach powołania nowego rodzaju sił zbrojnych w Polsce, a mianowicie Wojsk Obrony Cyberprzestrzeni. Na razie są to tylko działania projektowe, podejmowane przez zespoły naukowców. Np. Akademickie Centrum Polityki Cyberbezpieczeństwa, działające w ramach Akademii Sztuki Wojennej w Warszawie, wskazuje, że: „W przypadku szczególnego zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego spowodowanymi działaniami w cyberprzestrzeni, które nie może być usunięte poprzez użycie zwykłych środków konstytucyjnych — w czasie stanu wyjątkowego — mogłyby zostać <<uruchomione>> działania Wojsk Obrony Cyberprzestrzeni”[25]. Według autorów z Akademickiego Centrum Polityki Cyberbezpieczeństwa, Wojska Obrony Cyberprzestrzeni powinny zostać utworzone jako kolejny, szósty rodzaj sił zbrojnych, obok: wojsk lądowych, powietrznych, specjalnych, marynarki wojennej i wojsk obrony terytorialnej[26].

Obszar 3. Internet, jako środowisko medialne

Internet niemal od samego swojego początku, a więc od początku lat 90. XX w.[27], stał się środowiskiem dla wszystkich rodzajów mediów. Prasa, radio i telewizja są zawieszone w internecie, choć niektóre nadal uparcie utrzymują specyficzne dla siebie formy docierania do odbiorców poprzez papier gazetowy, czy eter radiowy i telewizyjny.

[24] Biuro do Walki z Cyberprzestępczością, <https://policja.pl/pol/kgp/bwc/33358,Biuro-do-Walki-z-Cyberprzestepczoscia.html>, 11 grudnia 2020 r.

[25] *Ekspertyza w zakresie obowiązujących aktów normatywnych regulujących środowisko prawne działania nowotworzonych Wojsk Obrony Cyberprzestrzeni. Wnioski i rekomendacje,* Warszawa 2020, s. 38.

[26] Tamże, s. 36.

[27] Historia internetu (2020), <https://pl.wikipedia.org/wiki/Historia_Internetu>, 11 grudnia 2020 r.

Na marginesie, w ogóle trudno o jednobrzmiącą definicję mediów, a wielu autorów prezentuje różne jej wersje[28]. Dieter Mersch w swojej książce pt. *Teorie mediów* opisuje sferę medialną w sposób bardzo niejednoznaczny i enigmatyczny: „Ni to jednostkowość, ni ogólność, ni forma, ni materia, ni postać, ni treść, ni figura, ni tło — zajmuje przestrzeń nieokreśloną, wymykającą się zwykłym podziałom"[29].

Internet na nowo gwałtownie przyspieszył proces nazywania, czym są media: od elitarnego dostawcy informacji, przez środki masowego przekazu, do serwisów społecznościowych. Do niedawna media kojarzyły się nam z przekazem treści od redaktorów do określonych odbiorców (np. kupujących periodyki), następnie redaktorzy zaczęli podawać informacje do powszechnego odbiorcy (stąd: środki masowego przekazu), a obecnie mogą już wszyscy, a nie tylko redaktorzy, przekazywać treści do wszystkich, za pomocą mediów społecznościowych. Można powiedzieć, że w środowisku internetowym jesteśmy zarówno odbiorcami, jak i nadawcami komunikatów. Dzięki mediom w internecie możemy przebywać zarazem w środowisku lokalnym, jak i globalnym. Anthony Giddens mówił, że jest to nasza dialektyka lokalności i globalności (*dialectic of the local and global*), czyli „gra wzajemnych oddziaływań między uczestnictwem w kontekstach lokalnych a tendencjami globalnymi"[30]. Manuel Castells nową internetową rzeczywistość medialną nazywa: „masową komunikacją zindywidualizowaną, która w znaczny sposób zwiększyła autonomię komunikowania podmiotów wobec korporacji komunikacyjnych, ponieważ użytkownicy stali się jednocześnie nadawcami i odbiorcami przekazów"[31]. Media internetowe przyczyniły się także w dużym stopniu do tego, że obecnie bardziej wierzymy opisom medialnym niż naszym zmysłom. Możemy zakwestionować każdy autorytet naukowy, bo internet natychmiast dostarczy nam argumentów, dzięki którym będziemy mogli popierać lub negować poszczególne wypowiedzi. To wskazuje na płodne podłoże do manipulacji.

Fake news jest to fałszywa informacja rozpowszechniana w mediach, szczególnie internetowych; zwykle służy dezinformacji lub dyfamacji. Walka z tego typu fałszywkami jest trudna, bo, jak mówi stare powiedzenie, kłamstwo wiele razy powtarzane staje się prawdą. Niemniej jednak powstaje wiele inicjatyw, którym celem jest wychwytywanie i odkłamywanie *fake newsów*. Oto kilka z nich, które zajmują się śledzeniem dezinformacji w polskiej przestrzeni medialnej:

— portal FakeNews.pl, prowadzony przez Fundację Przeciwdziałamy Dezinformacji[32];
— portal Stowarzyszenia Demagog[33];

[28] M. Mersch, *Teorie mediów*, Warszawa 2010, s. 8.

[29] Tamże, s. 27.

[30] A. Giddens, *Nowoczesność i tożsamość. „Ja" i społeczeństwo w epoce późnej nowoczesności*, Warszawa 2012.

[31] M. Castells, *Władza komunikacji*, Warszawa 2013, s. 16.

[32] Portal FakeNews.pl, <https://fakenews.pl/>, 18 grudnia 2020 r.

[33] Portal Stowarzyszenia Demagog, <https://demagog.org.pl/>, 18 grudnia 2020 r.

— serwis Stop Dezinformacji, prowadzony przez Fundację Panoptykon[34];
— projekt: Sprawdzam , prowadzony przez francuską agencję AFP (działa od kwietnia 2019 r., jako jeden pierwszych tego typu projektów w Polsce)[35];
— portal Konkret24, prowadzony przez telewizję TVN[36];
— portal FakeHunter, uruchomiony przez Polską Agencję Prasową[37].

W mniejszym stopniu są podejmowane próby opisywania i demaskowania całych strategii fałszowania rzeczywistości, kampanii dyfamacyjnych, czy tworzenia tzw. baniek medialnych. Brakuje także refleksji na temat bezpieczeństwa informacyjnego państwa. Joanna Taczkowska-Olszewska zauważa, że: „Bezpieczeństwo informacyjne nie jest pojęciem prawnym, co oznacza, że w polskim systemie prawnym brak jest aktów prawa powszechnie obowiązującego, w których ustawodawca zdecydował się na użycie tego terminu. Tym bardziej nie jest możliwe odnalezienie legalnej definicji tego pojęcia. Zarazem jednak nie sposób nie zauważyć, że termin ten uzyskał autonomię zarówno na gruncie nauki o bezpieczeństwie, jak również stał się nośnikiem koncepcji i rozwiązań o charakterze normatywnym”[38].

Powstanie mediów społecznościowych wytworzyło wrażenie, że każdy z nas w równym stopniu może być redaktorem i wydawcą. Nic bardziej mylnego. Współczesny świat medialny jest nadal (a może bardziej niż przedtem?) uzależniony od wielkich graczy, czyli koncernów i korporacji posiadających wielki kapitał i wyspecjalizowane narzędzia. Wśród największych wyróżnia się obecnie firmy dominujące w cyberprzestrzeni, a mianowicie: Google, Amazon, Facebook, Apple i Microsoft.

Niektórzy z użytkowników Facebooka mogli się już zderzyć z tzw. standardami społeczności[39]. Nie zastosowanie się do nich może skutkować restrykcjami ze strony właściciela tego serwisu społecznościowego. Działania zwykle poprzedza komunikat mniej więcej o następującej treści: „Z powodu ciągłego naruszania naszych Standardów społeczności publikacja Twojej strony może zostać cofnięta. Ograniczyliśmy już dystrybucję Twojej strony i nałożyliśmy na nią ograniczenia”. Działania wielkich koncernów internetowych, które monopolizują rynki, w tym mediów społecznościowych, budzą zastrzeżenia poszczególnych państw. Na przykład, w grudniu 2020 r. rząd Stanów Zjednoczonych złożył pozew do sądu, w którym

[34] Serwis Stop Dezinformacji, <https://panoptykon.org/stop-dezinformacji-przewodnik>, 18 grudnia 2020 r.

[35] Projekt: Sprawdzam, <https://sprawdzam.afp.com/list>, 18 grudnia 2020 r.

[36] Portal Konkret24, <https://konkret24.tvn24.pl/>, 18 grudnia 2020 r.

[37] Portal FakeHunter, <https://fakehunter.pap.pl/>, 18 grudnia 2020 r.

[38] J. Taczkowska-Olszewska, *Bezpieczeństwo informacyjne jako kategoria prawna. Ujęcie teoretyczne* [w:] W. Kitler, J. Taczkowska-Olszewska, *Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne*, Warszawa 2017, s. 47.

[39] Standardy społeczności, <https://www.facebook.com/communitystandards/>, 14 grudnia 2020 r.

„oskarżono Facebooka o działania antykonkurencyjne i wykorzystywanie dominacji rynkowej do gromadzenia danych konsumentów”[40].

Również w Polsce zaczyna się proces definiowania zagrożenia, które jest związane z bezpieczeństwem informacyjnym w dobie globalizacji. Patrycja Szostok pisze: „Doktryna bezpieczeństwa informacyjnego, aby być kompletna, powinna również zwrócić uwagę, co czyni się niezwykle rzadko, na bezpieczeństwo medialne państwa. (...) Bezpieczeństwo medialne to także względna niezależność od zewnętrznych źródeł informacji, co wymaga utrzymywania nakładów na rodzime agencje informacyjne, oraz ustawodawstwa, regulującego udział podmiotów zagranicznych w rynkach medialnych czy też ograniczającego możliwość koncentracji kapitału. Są to kwestie, którym poświęca się uwagę w odrębnych aktach prawnych, jednak rzadko uwzględnia się je jako element bezpieczeństwa informacyjnego państw, co wydaje się niedopuszczalnym przeoczeniem w dobie globalizacji mediów i zagrożeń z niej płynących”[41].

Obszar 4. Internet, jako nowe środowisko społeczne

Internet jest od dawna analizowany jako nowe środowisko społeczne oraz tym samym jako przedmiot i obszar badań psychologii społecznej. Jan Zając i Krzysztof Krejtz piszą: „Fenomen Internetu polega jednak na tym, że ze społecznego punktu widzenia jest on obecnie czymś znacznie więcej niż jedynie technologią komunikacyjną. Dla wielu grup społecznych stał się naturalnym środowiskiem funkcjonowania społecznego, pozwalającym na zaspokojenie większości społecznych potrzeb i motywacji. Służy nie tylko do poszukiwania informacji, lecz również do zawierania i podtrzymywania znajomości i bliskich związków. Co więcej, sieć jest także środowiskiem tworzenia się nowych społeczności oraz norm społecznych i kulturowych”[42].

Sęk w tym właśnie, że na naszych oczach powstają nowe zjawiska wywołane przez związki zawarte w sieci, a póki co nie umiemy ich odpowiednio opisać i zdefiniować. Anthony Giddens pisał o epoce, w której się znajdujemy, w sposób następujący: „Czymś, co w najbardziej oczywisty sposób odróżnia epokę nowoczesną od wszystkich poprzedzających ją okresów, jest niesłychany dynamizm. Nowoczesny świat <<ucieka>>: nie tylko tempo zmian jest nieporównywalnie szybsze niż w przypadku jakiegokolwiek wcześniejszego systemu, ale niespotykany jest także ich zasięg i radykalny wpływ, jaki wywierają na zastane praktyki i zachowania społeczne”[43].

[40] *Rząd USA pozwał Facebooka. Czego dotyczą oskarżenia?*, <https://wiadomosci.dziennik.pl/swiat/artykuly/8039686,rzad-usa-pozew-facebook-mark-zuckerberg-oskarzenia-monopol.html>, 14 grudnia 2020 r.

[41] P. Szostok, *Bezpieczeństwo informacyjne państwa a społeczeństwo informacyjne* [w:] K. Czornik, M. Lakomy, M. Stolarczyk, *Dylematy polityki bezpieczeństwa Polski na początku drugiej dekady XXI wieku,* Katowice 2014, s. 422.

[42] J. Zając, K. Krejtz, *Internet jako przedmiot i obszar badań psychologii społecznej,* „Psychologia Społeczna”, t. 2, Warszawa 2007, s. 191.

[43] A. Giddens*, Nowoczesność i tożsamość. „Ja” i społeczeństwo w epoce późnej nowoczesności*, Warszawa 2012, s. 30.

Jean Baudrillard, twórca teorii symulakrów, wskazuje na głębokie przenikanie się świata realnego z nierzeczywistym. Zawsze nieznany nam świat oswajaliśmy przez nadanie mu opisu, jakiegoś określenia lub znaku. Tych sztucznych znaków jest jednak już tak dużo, że przestajemy je rozumieć i kojarzyć z ich pierwotnym znaczeniem. Z czasem więc zaczynają one żyć własnym życiem. „Abstrakcją nie jest już dzisiaj mapa, sobowtór, zwierciadło albo pojęcie. Symulacja nie dotyczy jakiegoś terytorium, bytu referencyjnego albo substancji. Jest natomiast generowaniem, przy pomocy modeli, nierzeczywistej i pozbawionej oparcia realności — hiperrealności”[44]. Dzięki tej teorii łatwiej zrozumieć, czym jest świat wirtualny w erze internetu. Świat wyobrażony w sieci naśladuje prawdziwe istnienie i w konsekwencji powoduje u odbiorców rozdwojenie lub podwojenie ich rzeczywistości. Niestety można to porównać do sytuacji chorego, który tak dobrze symuluje chorobę, że na nią wreszcie zapada.

Rzeczywistość wirtualna wpływa na zachowania poszczególnych osób oraz grup społecznych. To jest terytorium do szeregu analiz i badań naukowych, także w kontekście bezpieczeństwa jednostek i społeczeństw. Jeszcze innym zjawiskiem, które wymaga uwagi w tym aspekcie, jest sztuczna inteligencja i samouczące się maszyny. Perspektywa, że maszyny przejmą kontrolę nad światem, jest nadal z dziedziny *science fiction*, czyli fantastyki naukowej. Jednakże, na przykład coraz częściej bywa, że bierzemy udział w wymianie myśli i wrażeń na jakimś forum dyskusyjnym, a tymczasem wcale nie rozmawiamy z drugim człowiekiem, a jedynie z maszyną, która wiernie udaje naszego interlokutora. To już jest nowa rzeczywistość. Ten sztuczny rozmówca w internecie nazywa się bot, który w sposób automatyczny próbuje naśladować ludzkie zachowania. Gdy ktoś używa botów do manipulacji, to wtedy, my odbiorcy, mamy do czynienia ze zwykłym ambarasem, albo... z groźną sytuacją z obszaru cyberbezpieczeństwa.

Wnioski końcowe

W kontekście cyberbezpieczeństwa przedstawione cztery obszary, a więc: prawo, system obrony, media w internecie oraz nowa rzeczywistość wirtualna, muszą być analizowane łącznie. Poczucie bezpieczeństwa w cyberprzestrzeni można zbudować jedynie wtedy, gdy konsekwentnie będzie się brało pod uwagę każdy z tych zakresów.

Na naszych oczach cyberprzestrzeń się rozszerza i równocześnie zagęszcza. Na płaszczyznę wirtualną przenosimy coraz więcej naszej aktywności publicznej, biznesowej i prywatnej. Musimy się więc liczyć z tym, że stale będą pojawiać się nowe rodzaje naruszeń prawa w obszarze cyberrzeczywistości.

[44] J. Baudrillard, *Precesja symulakrów* [w:] R. Nycz (red.), *Postmodernizm. Antologia przekładów*, Kraków 1997, s. 176.

Bezpieczeństwo w cyberprzestrzeni zapewni zbudowanie całościowego systemu, którego strażnikami będą odpowiednie instytucje państwowe i prywatne. Muszą one zadbać o infrastrukturę krytyczną, usługi cyfrowe i niezagrożony obieg informacji, a także wypracować sposoby reagowania na wszelkie incydenty związane z bezpieczeństwem komputerowym.

Internet jest środowiskiem dla wszystkich mediów. Dlatego bezpieczeństwo cyberprzestrzeni jest tak ważne, jak ochrona naszych informacji. Obecny Internet stał się nowym środowiskiem społecznym. Sieć internetowa zastępuje wielu internautom dotychczasowe związki międzyludzkie. Nie wiadomo, w jakim stopniu i dlaczego, zanurzenie się w sieci wywiera na nas tak duży wpływ. Jeszcze większą zagadką może być powstanie sztucznej inteligencji, która może się rozwinąć na bazie internetu. Również te aspekty muszą być brane pod uwagę podczas tworzenia całościowego systemu cyberbezpieczeństwa.

Bibliografia

Literatura

Banasiński C., *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018.

Baudrillard J., *Precesja symulakrów* [w:] R. Nycza (red.) *Postmodernizm. Antologia przekładów*, Kraków 1997.

Castells M., *Władza komunikacji*, Warszawa 2013.

Chałubińska-Jentkiewicz K., *Cyberodpowiedzialność*, Toruń 2019.

Ekspertyza w zakresie obowiązujących aktów normatywnych regulujących środowisko prawne działania nowotworzonych Wojsk Obrony Cyberprzestrzeni. Wnioski i rekomendacje, Warszawa 2020.

Giddens A., *Nowoczesność i tożsamość. „Ja" i społeczeństwo w epoce późnej nowoczesności*, Warszawa 2012.

Grzebiela K., *Pojęcie i istota bezpieczeństwa informacyjnego*, „Kultura Bezpieczeństwa. Nauka-Praktyka-Refleksje" 2018, nr 30.

Kardas P., *Oszustwo komputerowe w kodeksie karnym*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, z. 1.

Mersch M., *Teorie mediów*, Warszawa 2010.

Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016.

Szostok P., *Bezpieczeństwo informacyjne państwa a społeczeństwo informacyjne* [w:] Czornik K., Lakomy M., Stolarczyk M., *Dylematy polityki bezpieczeństwa Polski na początku drugiej dekady XXI wieku*, Katowice 2014.

Taczkowska-Olszewska J., *Bezpieczeństwo informacyjne jako kategoria prawna. Ujęcie teoretyczne* [w:] Kitler W., Taczkowska-Olszewska J., *Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne*, Warszawa 2017.

Zając J., Krejtz K., *Internet jako przedmiot i obszar badań psychologii społecznej*, Psychologia Społeczna, t. 2, Warszawa 2007.

Akty prawne

Ustawa z 6 czerwca 1997 r. — Kodeks karny (DzU z 1997 r., nr 88, poz. 553).
Ustawa z 26 kwietnia 2007 r. o zarządzaniu kryzysowym (DzU z 2007 r., nr 89, poz. 590).
Ustawa z 12 września 2014 r. o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r. (DzU z 2014 r., poz. 1514).
Ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (DzU z 2018 r., poz. 1560).
Rozporządzenie Rady Ministrów z 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (DzU z 2018 r., poz. 1806).

Inne

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, BBN, Warszawa 2020,<https://www.bbn.gov.pl/pl/wydarzenia/8806,Strategia-Bezpieczenstwa-Narodowego-Rzeczypospolitej-Polskiej.html>, 18 grudnia 2020 r.
Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, Portal Gov.pl, <https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024>, 18 grudnia 2020 r.
Biuro do Walki z Cyberprzestępczością, <https://policja.pl/pol/kgp/bwc/33358,Biuro-do-Walki-z-Cyberprzestepczoscia.html>, 11 grudnia 2020 r.
Portal internetowy CSIRT GOV, <https://csirt.gov.pl/>, 11 grudnia 2020 r.
Historia internetu (2020), Historia internetu, <https://pl.wikipedia.org/wiki/Historia_Internetu>, 11 grudnia 2020 r.
Portal FakeHunter, <https://fakehunter.pap.pl/>, 18 grudnia 2020 r.
Portal FakeNews.pl, <https://fakenews.pl/>, 18 grudnia 2020 r.
Portal Konkret24, <https://konkret24.tvn24.pl/>, 18 grudnia 2020 r.
Portal Stowarzyszenia Demagog, <https://demagog.org.pl/>, 18 grudnia 2020 r.
Projekt: Sprawdzam, <https://sprawdzam.afp.com/list>,18 grudnia 2020 r.
Rząd USA pozwał Facebooka. Czego dotyczą oskarżenia?, <https://wiadomosci.dziennik.pl/swiat/artykuly/8039686,rzad-usa-pozew-facebook-mark-zuckerberg-oskarzenia-monopol.html>, 14 grudnia 2020 r.
Serwis Stop Dezinformacji, <https://panoptykon.org/stop-dezinformacji-przewodnik>, 18 grudnia 2020 r.

Standardy społeczności, <https://www.facebook.com/communitystandards/>, 14 grudnia 2020 r.

Słowa kluczowe: cyberbezpieczeństwo, cyberprzestrzeń, prawo cyberprzestrzeni, internet, media, sztuczna inteligencja

Streszczenie: Artykuł przedstawia pokrótce cztery obszary, które należy uwzględniać podczas analiz, czym jest cyberbezpieczeństwo. Po pierwsze jest to: przestrzeń prawa dotycząca cyberprzestrzeni, po drugie: budowany system bezpieczeństwa państwa, po trzecie: specyfika mediów w środowisku internetowym, po czwarte: nowa rzeczywistość wirtualna, powstająca w cyberprzestrzeni. W kontekście cyberbezpieczeństwa wszystkie te zakresy badawcze muszą być traktowane łącznie.