DOI: 10.4467/27204383TER.22.006.15422

ORCID: 0000-0003-4649-589X

ANNA ROŻEJ

Rola i znaczenie informacji pochodzących ze źródeł otwartych w zwiększaniu podatności na zagrożenia bezpieczeństwa w cyberprzestrzeni, ze szczególnym uwzględnieniem cyberterroryzmu

Abstrakt

Celem artykułu jest przedstawienie, jak w ostatnich latach wzrosły rola i znaczenie informacji pochodzących ze źródeł otwartych w sytuacji przeniesienia znacznej części funkcjonowania społeczeństw do świata Internetu. Niestety, wraz z tym trendem pojawiły się także nowe zagrożenia, w tym o charakterze cyberterrorystycznym, które wymagają podjęcia natychmiastowych działań, aby móc ograniczyć ich oddziaływanie na bezpieczeństwo informacyjne.

Słowa kluczowe:

bezpieczeństwo informacyjne, źródła otwarte, infosfera, zagrożenia, walka informacyjna, infrastruktura krytyczna

W ciągu ostatnich kilkunastu lat dynamicznie zmieniające się otoczenie funkcjonowania człowieka sprawiło, że zaszły radykalne zmiany niemal w każdym środowisku, w tym w środowisku bezpieczeństwa. Pamiętne ataki na World Trade Center w Nowym Jorku oraz Pentagon w Waszyngtonie, od których minęło już ponad 20 lat, należy uznać za wyznacznik zmian w postrzeganiu bezpieczeństwa w skali globalnej. Bezpośrednio po zamachach większość państw należących do NATO, w tym Polska, została zmuszona do wprowadzenia w życie elementów narodowych systemów gotowości obronnej. Tragedia ta stała się też źródłem głębokiej refleksji społeczności międzynarodowej, obejmującej zarówno przyczyny, jak i konsekwencje tego wydarzenia, któremu, mając na uwadze stosunki międzynarodowe, można przypisać charakter przełomowy. Zamachy na World Trade Center i Pentagon były przyczyną gruntownego przeorientowania wszystkich systemów narodowych krajów zachodnich, zwłaszcza pod kątem współpracy z innymi państwami oraz organizacjami międzynarodowymi, w tym również w ramach NATO. Można stwierdzić, że był to pewnego rodzaju przełom od czasów zimnej wojny. Dopiero zamachy z 2001 r. sprawiły, że dostrzeżono potrzebę reformy systemów bezpieczeństwa narodowego, które tkwiły rozwiązaniami w XX w. i były nieprzystosowane do wyzwań świata postmilenijnego.

Zamach na symbole amerykańskiej potęgi w sposób jednoznaczny udowodnił, że „(...) dzisiejsze zagrożenia posiadają inną naturę i skalę niż dotychczas, a współczesna odpowiedź na te zagrożenia jest nieadekwatna. Broń projektowana w celu przeciwstawienia się zagrożeniom w końcu ostatniego tysiąclecia nie będzie w stanie sprostać im w pierwszych dekadach XXI wieku. Nowe, często o asymetrycznym charakterze, zagrożenia dla bezpieczeństwa globalnego wymagają nowego myślenia”[1].

Jednocześnie także legalne organizacje działające w skali ponadpaństwowej zyskują na sile i wpływach, dysponując technicznymi możliwościami dostosowania się do nowego środowiska bezpieczeństwa. Spekulanci giełdowi, handlowcy, korporacje międzynarodowe, firmy świadczące usługi internetowe mają obecnie możliwości znaczącego globalnego wpływu na życie codzienne obywateli wielu państw. Globalizacja oraz rewolucja w technologii informatycznej dały tym instytucjom przewagę. Ich kontrola jest sprawowana bardziej za pośrednictwem

[1] R. Hall, C. Fox, *Ponownie przemyśleć bezpieczeństwo*, „Przegląd NATO” zima 2001/2002, s. 8.

rynków finansowych niż przez struktury globalne, a zakłócenia powstają według takiej samej zasady. Dlatego też nie powinno dziwić, że tradycyjne mechanizmy państwa oparte na idei granic, porządku, władzy, policji, struktur siłowych są zagrożone. Wydają się one także ze swojej natury niezdolne do przeciwstawienia się współczesnym wyzwaniom dla bezpieczeństwa. W miarę jak owa niezdolność staje się coraz bardziej widoczna, narasta rozczarowanie poprzednim systemem i może powstać przekonanie, że wszystko w dziedzinie bezpieczeństwa zmierza ku gorszemu, na co oczywiście nie można pozwolić.

Najczęściej bardzo trudno jest zidentyfikować przywódcę lub region, na których można by skoncentrować zainteresowanie w celu przeciwstawienia się zagrożeniom. Co więcej, skala tych zagrożeń jest tak duża, że staje się to niebezpieczne dla wielu krajów. Zagrożenia te nie znają bowiem granic państwowych i kontynentalnych. Istnieje też zasadnicza trudność we właściwej identyfikacji zjawisk (organizacji, przywódców) w celu podjęcia skutecznego im przeciwdziałania. Zagrożenia te mogą podważać istotę i podwaliny funkcjonowania instytucji narodowych i międzynarodowych, a także zniszczyć gospodarki wielu państw.

Konieczność nowego podejścia do bezpieczeństwa była nagląca, gdyż terroryzm jest tylko jednym z wielu nietradycyjnych wyzwań dla bezpieczeństwa. Stanowią je też: konflikty etniczne i religijne, przemyt narkotyków, masowe migracje, regionalna niestabilność, pranie brudnych pieniędzy, działania różnych grup ekstremistycznych, kradzież informacji, a także sama dezinformacja. Tymczasem pojawiła się właśnie cybersfera, która osiągnęła ogromny dynamizm rozwoju, sprawiając, że wybrane mocarstwa dostrzegły potrzebę zreformowania systemów obronnych. W związku z tym zaczęły powstawać m.in. odrębne rodzaje wojsk – wojska cybernetyczne. Cybersfera wpłynęła na przeorientowanie akcentów w bezpieczeństwie ze zwalczania fizycznego na podejmowanie reakcji i rozwój zasobów do realizacji kontrataków na cyberataki, a także prowadzenie działań wyprzedzających w cyberprzestrzeni.

Uwzględniając rozpatrywaną problematykę, przyjęto, że przedmiotem badań przeprowadzonych w ramach niniejszego artykułu będą informacje pochodzące ze źródeł otwartych przeanalizowane w kontekście potencjalnych zagrożeń. Przedstawiony przedmiot badań jest wyznacznikiem celów procesu badawczego, które są postrzegane w ujęciu teoretycznym oraz praktycznym. Cel teoretyczny ma polegać na rozwinięciu oraz uzupełnieniu treści odnoszących się zarówno do teorii,

jak i praktyki cyberbezpieczeństwa w szczególnym przypadku, jakim jest korzystanie z internetowych źródeł otwartych. Osiągnięcie celu teoretycznego ma przyczynić się do realizacji celu praktycznego, jakim będą użyteczne rozwiązania w zakresie zapewnienia oraz utrzymania bezpieczeństwa informacyjnego. Zaprezentowana sytuacja problemowa, przedmiot badań i ich cel wyraźnie określają główny problem badawczy, który sprowadza się do odpowiedzi na następujące pytanie: czy globalne upublicznienie i ogólna dostępność dla wszystkich użytkowników Internetu w tym samym czasie informacji pochodzących ze źródeł otwartych, a dotyczących bezpieczeństwa państwa wpłynęły na zwiększenie ich podatności na ataki o charakterze cybernetycznym? Rozwiązanie problemu badawczego będzie uwarunkowane rozwiązaniem problemów szczegółowych, sprowadzających się do odpowiedzi na następujące pytania:

1. Jakie zmiany nastąpiły w środowisku bezpieczeństwa?
2. Jak zmieniło się nastawienie do Internetu w ciągu ostatnich kilku lat?
3. Jaka jest istota źródeł otwartych i na czym polega ich specyfika?
4. Jakie są potencjalne zagrożenia wynikające z korzystania z informacji pochodzących ze źródeł otwartych?
5. Jakie działania prewencyjne są możliwe, aby zapobiec zagrożeniom bezpieczeństwa informacyjnego?

Wstępne wnioski z obserwacji oraz analizy dostępnych dokumentów i literatury przedmiotu, a także określony cel badań i problemy badawcze zdeterminowały założoną hipotezę roboczą, dzięki której będzie możliwe przeprowadzenie procesu badawczego: rozwój Internetu oraz zwiększenie zainteresowania źródłami otwartymi są związane ze wzrostem zagrożeń o charakterze cyberterrorystycznym.

Jak mawiał Henry Kissinger – wybitny amerykański polityk i dyplomata, doradca do spraw bezpieczeństwa narodowego prezydenta Richarda Nixona: „Bezpieczeństwo jest fundamentem wszystkiego, co czynimy”[2], i trudno się z tak postawioną tezą nie zgodzić. Jednak w dobie ogromnego rozwoju technologicznego, dostępu do zaawansowanych procesów oraz urządzeń może się wydawać, że troska o bezpieczeństwo schodzi na dalszy plan. Istotne są posiadane narzędzia, możliwości, a nie jedna z najważniejszych wartości, czyli bezpieczeństwo. W związku

[2] H. Kissinger, *Dyplomacja*, Warszawa 2016, s. 23.

z przeniesieniem niemal każdego aspektu życia do świata Internetu jesteśmy narażeni na wiele zagrożeń o charakterze cybernetycznym, a poziom poczucia bezpieczeństwa, zwłaszcza bezpieczeństwa teleinformatycznego, znacznie się obniżył. Istnieje ogromne ryzyko, że zgromadzone przez nas dane, przetwarzane informacje staną się obiektem zainteresowania ze strony cyberprzestępców.

Jeden z pierwszych teoretyków sztuki wojennej, żyjący 25 wieków temu w Chinach Sun Tzu, w swoim traktacie *Sztuka wojny* stwierdza, że „(...) najwyższą umiejętnością w sztuce wojennej jest podporządkowanie sobie nieprzyjaciela bez walki”[3]. Podaje jednocześnie wiele wskazówek, jak ów pożądany stan osiągnąć. Dążąc do uzyskania powodzenia w wojnie, należy m.in. dyskredytować wszystko, co dobre w kraju przeciwnika, wciągać przedstawicieli warstw rządzących przeciwnika w przestępcze przedsięwzięcia, podrywać ich dobre imię i w odpowiednim momencie rzucić ich na pastwę pogardy rodaków. Zasadne jest też dezorganizowanie działalności rządu przeciwnika oraz wywoływanie waśni i niezgody między obywatelami wrogiego kraju. Należy także zwrócić uwagę na indyjski traktat *Arthaśastra* autorstwa Ćanakji Kautilji. Ten indyjski filozof oraz teoretyk wojny poza przypisaniem dużej roli w polityce zagranicznej szpiegom i zdrajcom wprowadził regułę prowadzenia wojny, zgodnie z którą jej rozpoczęcie ma być dopuszczalne jedynie w sytuacji, gdy z analizy porównawczej obu stron wynika pewność zwycięstwa. Gwarantami sukcesu są takie czynniki, jak: mądrość, plan, silna i dobrze wyszkolona armia, wysokie morale oraz ogólny potencjał. Kautilja zaznaczył również, że podbitą ludność należy traktować łagodnie, aby móc nad nią trwale panować.

W środowisku bezpieczeństwa informacyjnego podłoża zmian należy się dopatrywać zwłaszcza w rewolucji informacyjnej, która wprowadziła do obiegu różne technologie pozwalające na pozyskiwanie oraz dystrybucję informacji na masową skalę. To zjawisko miało przełomowy charakter, z uwagi na globalną skalę oddziaływania tych technologii. Powyższe konsekwencje rewolucji informacyjnej powodujące ogrom zmian sprawiły, że infosfera rozumiana jako synonim przestrzeni informacyjnej i środowiska informacyjnego stała się przedmiotem nauk o bezpieczeństwie[4]. W środowisku naukowym infosfera jest rozumiana

[3] Sun Tzu, *Sztuka wojny*, Gliwice 2004, s. 57.

[4] B. Sosińska-Kalata, *Obszary badań współczesnej informatologii (nauki o informacji)*, „Zagadnienia Informacji Naukowej” 2013, nr 2, s. 9–41.

jako całość zasobów informacyjnych, do których dany podmiot ma dostęp. Analiza społeczeństwa informacyjnego w aspekcie systemu cybernetycznego wskazuje zaś, że infosfera dzieli się na warstwę lokalną, która odpowiada lokalnym zasobom informacyjnym powstającym wraz z rozwojem lokalnej społeczności, oraz warstwę globalną złożoną z zasobów globalnych, będącą czymś znacznie większym niż sumą informacyjną zasobów lokalnych[5]. Początków społeczeństwa informacyjnego upatruje się w latach 60. i 70. XX w. Powstało ono w wyniku rewolucji przemysłowej, podczas której wprowadzono do użytku komputer oraz nastąpił rozwój informatyzacji[6]. Po raz pierwszy pojęcia „społeczeństwo informacyjne" (jap. *johoka shakai*) użył Japończyk Tadao Umesao, określając w ten sposób społeczeństwo, które zaczęło używać komputera do komunikacji w epoce rozwoju techniki cyfrowej i mikroelektroniki. Pojęcie to następnie zostało rozwinięte przez Daniela Bella, który uważał, że dla ówczesnego społeczeństwa zasobami strategicznymi były wiedza oraz informacja, a nie – jak do tej pory – praca i kapitał[7].

W ostatnich latach infosfera, poza tym, że jej permanentną cechą stał się globalizm, zyskała ogromnie na znaczeniu poprzez objęcie znacznie większej ilości dostępnych informacji o charakterze powszechnym niż jeszcze kilka lat temu. Wyzwaniem stały się nie tylko masowość i nadmiar informacji, ale przede wszystkim ich cechy, takie jak niewiarygodność, irrelewantność oraz nieprawdziwość. Mnogość kanałów oraz źródeł informacyjnych sprawia, że wskazane cechy obecnie się nasilają.

Ponadto rewolucja informacyjna oraz towarzyszące jej rozwijająca się intensywnie technologia, dynamika życia, a także w ostatnim czasie pandemia wywołana wirusem SARS-CoV-2 sprawiły, że niemal całość życia codziennego została przeniesiona do świata Internetu, co z jednej strony daje ogromne możliwości, z drugiej jednak generuje wiele zagrożeń bezpieczeństwa w skali krajowej i międzynarodowej. „Gdy tylko nowe techniki informacyjne rozprzestrzeniły się i zostały przejęte przez różne kraje, różne kultury, różnorodne organizacje i rozmaite cele, nastąpiła eksplozja różnego rodzaju zachowań i użytków, co zwrotnie

[5] P. Sienkiewicz, *Społeczeństwo informacyjne jako system cybernetyczny*, w: *Społeczeństwo informacyjne. Wizja czy rzeczywistość?*, t. 1, L.H. Haber (red.), Kraków 2004, s. 79.

[6] J.S. Nowak, *Społeczeństwo informacyjne – geneza i definicje*, w: *Społeczeństwo informacyjne. Krok naprzód, dwa kroki wstecz*, P. Sienkiewicz, J.S. Nowak (red.), Katowice 2008, s. 25.

[7] http://www.bbc.uw.edu.pl/Content/20/08.pdf [dostęp: 25 XI 2021].

przyczyniło się do powstania technologicznych innowacji, przyspieszając tempo i rozszerzając zasięg technologicznej zmiany, a także różnicując jej źródła"[8]. Przytoczone stwierdzenie hiszpańskiego socjologa Manuela Castellsa świadczy o tym, że współczesne społeczeństwo jest rzeczywiście społeczeństwem informacyjnym, które zostało prawie całkowicie zdominowane przez systemy telekomunikacyjne służące do przesyłania, odbierania oraz przetwarzania informacji. Informacja jest aktualnie nieodłącznym elementem życia społecznego, gospodarczego, a także jest obecna w każdym obszarze funkcjonowania człowieka.

Należy zauważyć, że przejawy życia społecznego są najintensywniejsze w dużych przestrzeniach, takich jak na przykład ośrodki miejskie, lotniska czy szlaki komunikacyjne. Współczesne społeczeństwa udowadniają, że miejsca te wcale nie muszą realnie istnieć. Wystarczy, że stanowią one jedynie infrastrukturę czy platformę komunikacyjną, która stwarza warunki, aby organizacje czy różnego rodzaju inne podmioty mogły się ze sobą łączyć w czasie rzeczywistym[9]. Zmiany w społeczeństwie w czasach rewolucji informacyjnej dostrzegał też teoretyk komunikacji Marshall McLuhan. Uważał on, że dzięki bliskim relacjom typu online świat przybiera charakter globalnej wioski, w której ludzie mają możliwość łączenia się i komunikowania w czasie rzeczywistym. Niedługo trzeba było czekać, a nastała era komputerów osobistych, Internetu, smartfonów, bez których już nikt dzisiaj nie wyobraża sobie funkcjonowania. Dzięki powstałym rozwiązaniom technologicznym istnieje możliwość komunikowania się z dowolnymi osobami niezależnie od miejsca pobytu.

Ogromny dynamizm procesów, jakie zaszły w ciągu ostatnich kilkudziesięciu lat, sprawił, że obecnie największym zbiorem informacji jest właśnie Internet, na który składa się część jawna – powszechnie dostępna, oraz ciemna – tzw. Darknet, do którego dostęp jest nieco ograniczony, jednak przy użyciu odpowiednich technologii również możliwy.

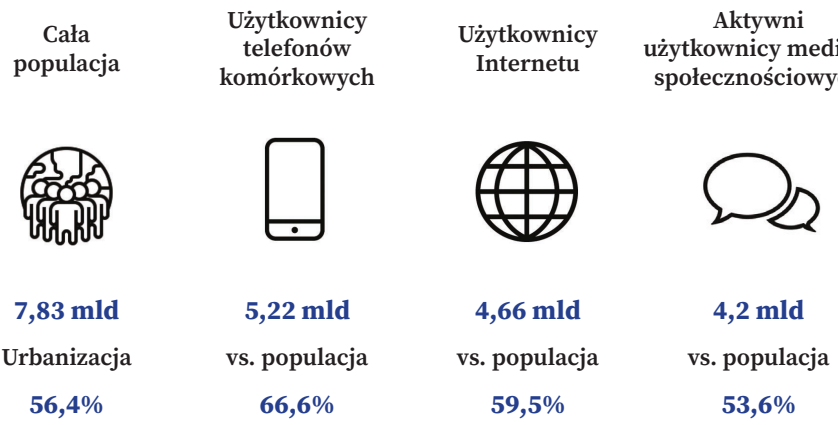
O tym, jak pożądanym źródłem informacji jest Internet, mogą świadczyć dane z raportu opublikowanego w 2018 r. przez ITU (ang. International Telecommunication Union)[10]. Otóż już wówczas ponad

[8] A. Elliott, *M. Castells: Społeczeństwo sieci*, w: A. Elliott, *Współczesna teoria społeczna. Wprowadzenie*, Warszawa 2011, s. 23–24.

[9] Tamże, s. 311–319.

[10] *Measuring the Information Society Report*, t. 1, Geneva 2018.

połowaświatowej populacji miała dostęp do Internetu. Pod koniec 2018 r. korzystało z niego prawie 51,2 proc., czyli 3,9 mld ludzi. Stanowiło to istotny krok w kierunku jeszcze większego rozwoju globalnego społeczeństwa informacyjnego. Szacowano, że w krajach rozwiniętych 4 osoby na 5 miały bezpośredni i nieograniczony dostęp do sieci. W krajach rozwijających się dostęp do Internetu miało ok. 45 proc. społeczeństwa, a w krajach najsłabiej rozwiniętych jedynie 20 proc. Jednak, zgodnie z przewidywaniami ITU, nieustannie obserwuje się tendencję wzrostową w dostępie do sieci. Potwierdzają to dane podane w Global Digital Report[11] dotyczące stanu cyfryzacji społeczeństwa w styczniu 2021 r., które przedstawia rysunek 1.



Rys. 1. Stan cyfryzacji na świecie w styczniu 2021 r.

Źródło: DataReportal, DataReportal – Global Digital Insights.

Charakteryzując dane przedstawione na rysunku 1, należy stwierdzić, że:

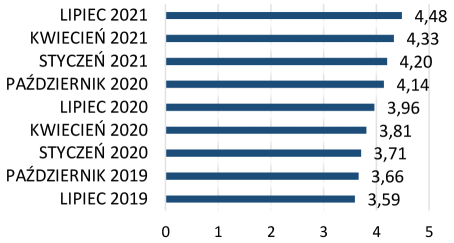
- **Ludność:** liczba ludności na świecie wynosiła 7,83 mld.
- **Telefonia komórkowa:** z telefonu komórkowego korzystało 5,22 mld ludzi, co stanowiło 66,6 proc. populacji na świecie. Liczba użytkowników mobilnych zwiększyła się od stycznia 2020 r. o 1,8 proc. Całkowita liczba połączeń mobilnych wzrosła o 72 mln, osiągając na początku 2021 r. poziom 8,02 mld.

[11] https://datareportal.com/reports/digital-2021-global-overview-report [dostęp: 26 XI 2021].

- **Internet:** z Internetu korzystało 4,66 mld ludzi na świecie , co stanowiło 59,5 proc. światowej populacji. Daje to wzrost o 316 mln w ciągu roku.
- **Media społecznościowe:** na świecie było 4,2 mld użytkowników mediów społecznościowych. Liczba ta wzrosła o 490 mln od stycznia 2020 r. Liczba użytkowników mediów społecznościowych stanowiła ponad 53 proc. światowej populacji.

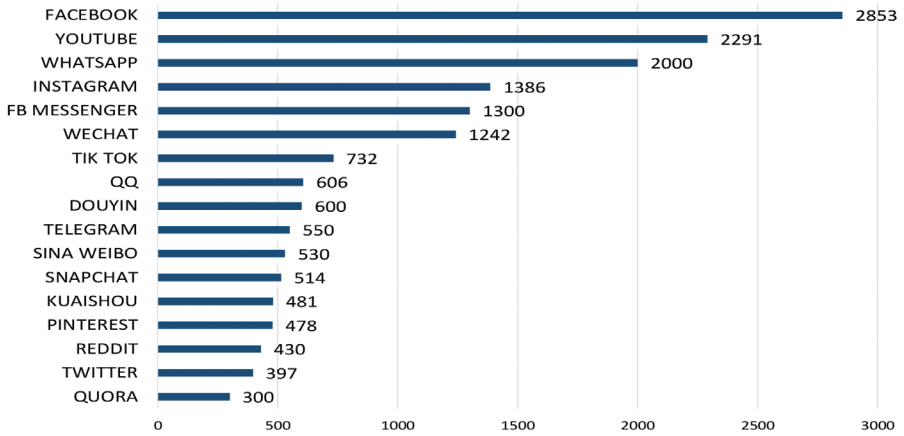
Ponadto o tym, że Internet jest jednym z najbardziej powszechnych źródeł danych, świadczą również poniższe fakty:

1. Liczba użytkowników mediów społecznościowych nieustannie wzrasta. W lipcu 2021 r. wynosiła ok. 4,48 mld (rysunek 2).
2. Platformy należące do rodziny Facebooka (Facebook, WhatsApp, Instagram, Messenger) cieszą się olbrzymim zainteresowaniem (rysunek 3).
3. Wydłuża się czas korzystania z Internetu (rysunek 4).
4. Wydłuża się czas korzystania z mediów społecznościowych (rysunek 5).



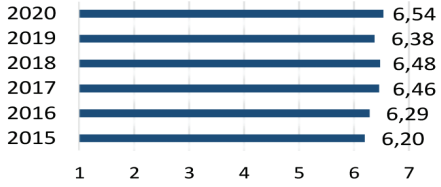
Rys. 2. Wzrost liczby użytkowników (w miliardach) mediów społecznościowych na świecie w latach 2019–2021.

Źródło: DataReportal, DataReportal – Global Digital Insights.



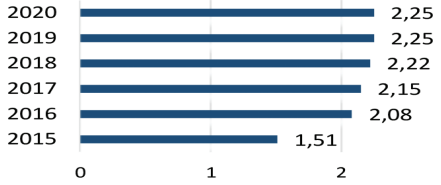
Rys. 3. Liczba użytkowników (w milionach) najpopularniejszych portali społecznościowych na świecie (dane z lipca 2021 r.).

Źródło: DataReportal, DataReportal – Global Digital Insights.



Rys. 4. Wzrost w latach 2015–2020 dziennego czasu (w godzinach) przeznaczanego na korzystanie z Internetu przez użytkowników w wieku 16–64 lat.

Źródło: DataReportal, DataReportal – Global Digital Insights.



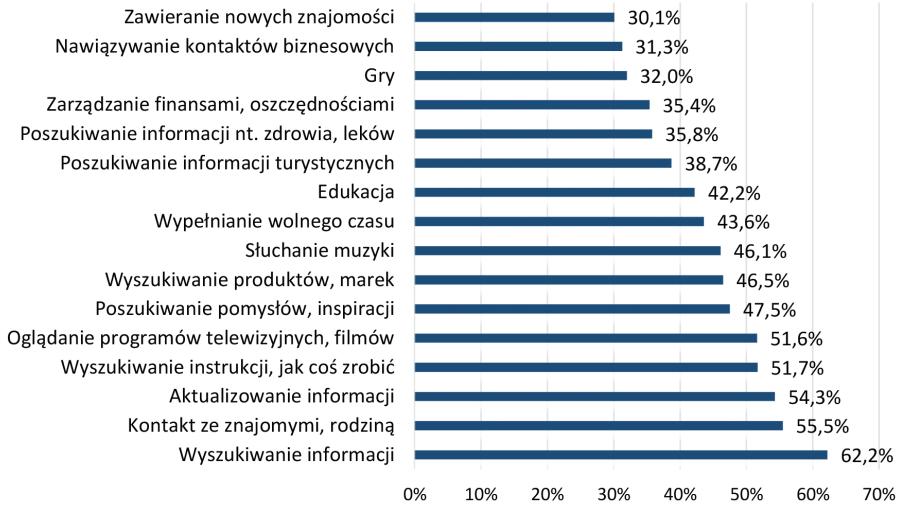
Rys. 5. Wzrost w latach 2015–2020 dziennego czasu (w godzinach) przeznaczanego na korzystanie z mediów społecznościowych przez użytkowników w wieku 16–64 lat.

Źródło: DataReportal, DataReportal – Global Digital Insights.

Do najpopularniejszych powodów, dla których ludzie korzystają z Internetu, zalicza się:

- poszukiwanie informacji;
- chęć bycia w kontakcie ze znajomymi i rodziną;
- chęć posiadania aktualnych danych i informacji;
- poszukiwanie wskazówek co do wykonania określonych czynności;
- oglądanie filmów, telewizji.

Szczegółowe dane zostały przedstawione na rysunku 6.



Rys. 6. Główne powody skłaniające użytkowników w wieku 16–64 lat do korzystania z Internetu.

Źródło: DataReportal, DataReportal – Global Digital Insights.

Na podstawie przedstawionych powyżej danych wskazujących na ogromną aktywność społeczeństwa globalnego w Internecie oraz nieustanny jej wzrost należy stwierdzić, że wspomniana sieć jest największym zbiorem informacji, często o charakterze strategicznym. Nic więc dziwnego, że informacja stała się najważniejszym zasobem decydującym o funkcjonowaniu i powodzeniu niemal każdej organizacji czy przedsiębiorstwa. Jest to zasób, który stanowi podstawę działalności, zapewnia przewagę konkurencyjną, a także daje poczucie

bezpieczeństwa. Powszechność informacji oraz ich niemal nieograniczona dostępność wynikają m.in. stąd, że często ich źródłem pochodzenia są źródła otwarte. Naukowcy oraz eksperci z obszaru działań wywiadowczych definiują źródła otwarte (ang. *open source*) jako podmiot bądź przedmiot cechujący się walorami, które umożliwiają generowanie informacji pozwalającej na ich legalne przetwarzanie, w tym utrwalanie, przesyłanie czy gromadzenie[12]. Informacje pochodzące ze źródeł otwartych mają charakter pierwotny bądź wtórny, co może generować również pewne ograniczenia. Otóż informacja, która pochodzi ze źródła pierwotnego, może mieć ograniczenia związane z możliwościami jej rozpowszechniania, jeśli na przykład będzie informacją niejawną bądź prywatną. Jeżeli jednak informacja pozyskiwana jest ze źródeł wtórnych – ogólnodostępnych, jej jawność nie jest już problemem[13]. Należy zauważyć, że pomimo iż informacje pochodzące ze źródeł otwartych są dostępne, to odbiorca rzadko ma pełną wiedzę o ich źródłach oraz właściwościach. W innej definicji zwraca się uwagę, że źródła otwarte to ogół pisemnych, audiowizualnych bądź informatycznych środków rozpowszechniania informacji[14]. Otwarte źródła informacji można klasyfikować na kilka sposobów, biorąc pod uwagę związek, jaki zachodzi między wagą informacji a wartością źródła. W praktyce jednak najczęściej uwzględniany jest rodzaj medium przekazu informacji, co może wynikać stąd, że media różnią się między sobą jakością, a tytuły są publikowane w różny sposób. Na przykład w Internecie użytkownik może znaleźć informacje, które ukazały się w telewizji bądź w prasie, i odwrotnie. Informacje te mogą występować w artykułach o różnych tytułach.

Rozwój technologiczny, a także wzrost dostępu do Internetu sprawiły, że ewoluowały także otwarte źródła informacji. Przykłady takich źródeł zostały przedstawione w tabeli.

---

[12] B. Saramak, *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy*, Warszawa 2015, s. 22–23.

[13] Ch. West, *Competitive intelligence,* New York 2001, s. 50.

[14] J. Oleński, *Ekonomika informacji*, Warszawa 2001, s. 49.

Tabela. Przykłady otwartych źródeł informacji.

ŹRÓDŁA OTWARTE			
Domeny (np. rejestry, listy, WHOIS)	Mapy (np. Wojewódzkie Systemy Informacji Przestrzennej)	Osoby (np. nazwiska – nazwiska-polskie.pl, Biuletyn Informacji Publicznej)	Użytkownicy/loginy (np. Albicla, Allegro, Fotka)
Serwisy społecznościowe (np. Facebook, Albicla, Fotka)	Serwisy randkowe (np. Sympatia, eDarling)	Firmy/organizacje (np. CEIDG, eKRS, Rejestr.io)	Społeczeństwo (np. Bank Danych Lokalnych – GUS, Baza Demografia – GUS)
Biznes/gospodarka (np. Allegro, GPW)	Archiwa (np. Inwentarz Archiwalny IPN, Narodowe Archiwum Cyfrowe)	Tłumaczenia (np. Elektroniczny Słownik Języka Polskiego)	Rejestry publiczne (np. Bank Danych, Biuletyn Zamówień Publicznych)
Prawo (np. Dzienniki Urzędowe, Internetowy System Aktów Prawnych)	Uczelnie (np. POL-on, RAD-on)	Transport (np. CEPiK API, EPKT Spotters)	Dark web (Aktywne strony TOR)
Dokumenty (np. chomikuj.pl)	Wideo (np. Kamery.edu.pl)	Zdjęcia (np. Fotosik.pl)	Numery telefonów
Książki telefoniczne (np. Dostawca usług, Kto dzwonił)	SIGNIT (np. WebSDR)	OpSec (np. Generatory IT, GenApps)	Baza Wiedzy (np. blogi, kursy, prezentacje)

Źródło: Opracowanie własne.

Każde z powyższych źródeł możemy podzielić na poszczególne podkategorie, a elementem łączącym je wszystkie jest Internet. Do informacji wyszukiwanych w sieci należy jednak podchodzić z dużą ostrożnością i nie zapominać o innych źródłach – tych z kategorii drukowanych, takich jak chociażby książki, dzienniki czy czasopisma. Ponadto warto zauważyć, że Internet to nie tylko serwisy informacyjne, lecz także bardzo popularne portale społecznościowe, które zapewniają funkcjonowanie różnych środowisk tematycznych, grup zainteresowań, a także słowniki, encyklopedie, fora czy blogi. Wszystkie te źródła zawierają wiele różnych informacji. Ponadto źródła otwarte pozwalają dotrzeć do zdjęć prywatnych, zdjęć satelitarnych, a także danych geolokalizacyjnych. Pomimo że wskazane źródła cechują się przede wszystkim otwartością,

dostępnością oraz jawnością, to ostrożność nakazuje podchodzić do nich z racjonalnym dystansem oraz je weryfikować.

Warto mieć świadomość, że usługi przeszukiwania Internetu (ang. *search service*), czyli jedna z najpopularniejszych funkcjonalności użytkowania sieci, bazują na wykorzystaniu wyspecjalizowanych oprogramowań, które odpowiadają za eksplorację baz internetowych. Do najbardziej popularnych mechanizmów zalicza się:

- mechaniczne indeksowanie wyrazów i fraz – AltaVista/Yahoo, Google, HotBot;
- arbitralne katalogowanie dokumentów zgodnie z przyjętą klasyfikacją tematyczną – Yahoo;
- usługi przeszukujące dokumenty z grup dyskusyjnych – AltaVista Usenet;
- metasearch – narzędzie wykorzystujące pojedyncze wyszukiwarki – MetaCrawler, MetaFIND;
- wyszukiwanie korzystające ze specjalistycznych baz danych – Alphasearch;
- inne.

Pomimo istnienia tak specjalistycznej technologii przy przeglądaniu źródeł otwartych, w tym stron internetowych, należy za każdym razem ocenić je pod względem ich wiarygodności. W tym celu warto zadać sobie pięć podstawowych pytań: kto?, co?, gdzie?, kiedy?, dlaczego?

Chcąc znaleźć odpowiedź na pytanie: kto? – można dokonać analizy strony pod kątem wyszukiwania autorów, konkretnych nazwisk czy szczegółowych informacji. Dobrą praktyką jest też sprawdzenie typów domen – .com/.org/.gov/kod kraju, a także ocena, czy dany typ jest odpowiedni dla przedstawionych treści. Jeśli strona, z której są pobierane informacje, to strona osobista albo strona użytkownika portalu społecznościowego, należałoby zidentyfikować, kto jest odpowiedzialny za wprowadzenie danych treści, a także, jeśli jest taka możliwość, przeanalizować kod źródłowy strony, gdzie często jest zapisane nazwisko autora. W następnej kolejności, aby zweryfikować wiarygodność informacji, należałoby sprawdzić, do kogo należy serwer, na którym jest umieszczona dana strona, oraz czy zebrane informacje są ze sobą spójne. Dobrą metodą na sprawdzenie wiarygodności danych treści jest poszukiwanie opinii innych użytkowników, a także prześledzenie rozpowszechniania danej informacji, chociażby przez weryfikację liczby udostępnień.

Sprawdzając daną stronę, należy zwrócić uwagę na zawarte w niej treści, czyli spróbować odpowiedzieć na pytanie: co? Aby móc ocenić prawdziwość zamieszczonych treści, trzeba zweryfikować źródła, daty oraz czy treści nie są zmienione w odniesieniu na przykład do cytowanych źródeł. Bardzo istotną cechą informacji jest jej aktualność, czyli odpowiedź na pytanie: kiedy? W związku z tym powinno się sprawdzić, kiedy dana informacja została zamieszczona, kiedy była aktualizowana bądź jak często jest aktualizowana. Zebranie odpowiedzi na powyższe pytania pozwoli ocenić, czy informacje pochodzące ze źródeł otwartych są przede wszystkim prawdziwe, wiarygodne i aktualne.

Z danych statystycznych przedstawionych w pierwszej części artykułu wynika, że wobec rosnącej liczby populacji z dostępem do Internetu jest on narzędziem służącym do zamieszczania, poszukiwania oraz wymiany informacji. Co więcej, zasoby internetowe są w łatwy i szybki sposób uzupełniane przez użytkowników Internetu. W związku z tym każdy może być zarówno odbiorcą informacji, jak i ich autorem. Chcąc zidentyfikować atrybuty źródeł otwartych, należy wskazać:

- dostępność,
- niski koszt pozyskania,
- niepewną wiarygodność,
- brak zależności,
- niskie ryzyko,
- jawność.

Powyższe cechy poniekąd odpowiadają na pytania dotyczące liczby źródeł otwartych, a przede wszystkim liczby gromadzonych i przetwarzanych w nich informacji. Przykładem może być chociażby portal społecznościowy Facebook.com, który obecnie ma ok. 2,8 mld aktywnych użytkowników miesięcznie, a dziennie odwiedza go ok. 1,84 mld osób. Od początku 2021 r. liczba użytkowników Facebooka wzrosła o ok. 12 proc. Skala ta obrazuje, jak wiele informacji jednocześnie pojawia się na portalu.

Przedstawione dotychczas informacje wskazują, że zasięg oraz dostępność źródeł otwartych są ogromne. Obecnie ponad połowa ludności na całym świecie ma dostęp do Internetu za pomocą komputerów, smartfonów czy innych urządzeń. Rewolucja technologiczna, jaka nastąpiła w tym zakresie, bez wątpienia podniosła jakość życia, a przez to również kompetencje cyfrowe społeczności międzynarodowej. Trudno już wyobrazić sobie życie zawodowe czy prywatne bez dostępu do sieci. Gdy spojrzy się przez pryzmat rozwoju w obszarze gospodarczym

i społecznym, obecna sytuacja powinna być powodem jedynie do zadowolenia i dumy. Dostęp do tak wielu informacji to podstawa dalszego rozwoju, nowych możliwości oraz szans.

Niestety, rozwój cyberprzestrzeni, w której dochodzi do przetwarzania ogromnej ilości informacji, niesie za sobą także rozwój cyberterroryzmu. Tak jak cyberprzestrzeń pozbawiona jest wszelkich granic, podobnie terroryzm ma nieograniczony zasięg, co pozwala cyberprzestępcom podejmować i skutecznie przeprowadzać w sieci Internet działania o charakterze cyberterrorystycznym. Permanentną cechą cyberterroryzmu jest niewidoczność jego działania, a także poniekąd skutków, czego nie da się powiedzieć o terroryzmie w formie konwencjonalnej. Najczęściej użytkownik Internetu nie dostrzega cyberataku i nie zdaje sobie z niego sprawy. Atak ujawnia się w przypadku zablokowania na przykład systemów teleinformatycznych obiektów strategicznych odpowiadających chociażby za infrastrukturę krytyczną. Te zagrożenia są niestety bardzo słabo mierzalne albo wręcz niemierzalne. Problem polega również na tym, że cyberterrorysta jest to przeciwnik, wobec którego trudno zastosować jakiekolwiek konwencje międzynarodowe o działaniach zbrojnych państw, gdyż tak naprawdę nie wiadomo, kto jest przeciwnikiem. Potrzeba powstania legislacji w tym obszarze jest na pewno priorytetem każdego państwa, jak i organizacji międzynarodowych. Rozwój cyberprzestrzeni spowodował, że państwa straciły możliwość walki z tym niewidocznym przeciwnikiem, nie ma także podstaw prawnych, aby uruchomić współpracę międzynarodową w celu identyfikacji wroga i jego statusu.

Jeszcze zaledwie kilkanaście lat temu byliśmy jako społeczeństwo pod wielkim wrażeniem rozwoju teleinformatycznego i cyfryzacji wielu obszarów. Jednak nowe zagrożenia bezpieczeństwa XXI w., takie jak m.in. cyberprzestępczość, a także cyberterroryzm, doprowadziły do zweryfikowania takiego entuzjastycznego podejścia. Pod pojęciem „cyberprzestępczości" należy rozumieć każde nielegalne zachowanie realizowane za pomocą działań elektronicznych nakierowanych na bezpieczeństwo systemów komputerowych i danych w nich przetwarzanych. To także nielegalne działania podejmowane za pomocą lub względem systemu komputerowego czy sieci, w tym takie przestępstwa, jak nielegalne posiadanie, oferowanie lub rozpowszechnianie informacji za pomocą systemu komputerowego lub sieci. Do tego typu przestępstw można zaliczyć m.in. oszustwa, fałszerstwa, szpiegostwo przemysłowe, sabotaż i wymuszenia poprzez piractwo komputerowe i inne przestępstwa przeciwko własności

intelektualnej. Cyberterroryzm zaś obejmuje ataki na bezpieczeństwo publiczne, życie oraz walkę elektroniczną skierowaną przeciwko infrastrukturze krytycznej. Cyberterroryzm wykorzystuje nowe technologie informacyjne lub cyberprzestrzeń również do działań tradycyjnych[15].

Wcześniej cyberterroryzm bardziej był kojarzony z systemami bankowymi, kradzieżą tożsamości czy zawirusowaniem systemów komputerowych. Przykładem skali ówczesnego cyberterroryzmu mogą być wydarzenia, do jakich doszło w Estonii w 2007 r. Przy okazji próby przeniesienia pomnika tzw. Brązowego Żołnierza, który upamiętniał radzieckich wojskowych, rozegrała się zimna wojna o charakterze cybernetycznym. Wówczas to nie konflikty na ulicach były poważnym zagrożeniem, ale masowe ataki na rządowe oraz prywatne serwery. Spowodowały one powszechny paraliż poprzez blokady systemów bankowych, serwisów informacyjnych, stron rządowych. Skalę tych wydarzeń oddają słowa byłego prezydenta Estonii Toomasa Hendrika Ilvesa, który stwierdził, że: „W obecnych czasach nie potrzeba pocisków, żeby niszczyć infrastrukturę. Można to zrobić on-line". Społeczeństwo estońskie przekonało się wtedy, że Internet daje wiele możliwości, ale może też odebrać zdolność do prawidłowego funkcjonowania. Przeniesienie życia do świata Internetu powoduje, że cyberterroryzm nieustannie się rozwija i swoim zasięgiem obejmuje kolejne obszary działania. Według literatury przedmiotu „cyberterroryzm" „(...) to zjawisko o politycznie motywowanym ataku bądź też groźba ataku wycelowana w system informatyczny, określone dane. Cel ataku może być różny: od zniszczenia informacji po np. ich udostępnienie dla osiągnięcia wyznaczonych celów politycznych czy społecznych. Obecnie cyberterroryzm to nie tylko typowe ataki terrorystyczne w cyberprzestrzeni, współcześnie to działania również takie, jak propaganda, dezinformacja, szpiegostwo, inwigilacja w sieci, manipulacja informacją, nazywana miękkim cyberterroryzmem"[16].

Należy zauważyć, że w cyberprzestrzeni występują wszystkie negatywne zjawiska, z jakimi można spotkać się na co dzień w „prawdziwym życiu". Kradzież, oszustwo, manipulacja, szpiegostwo to przykłady zagrożeń, z jakimi można mieć do czynienia w cyberprzestrzeni. Przykładem może być również fizyczne zniszczenie serwerów, przyczyniające się do

[15] http://unicjin.org/documents/congr10/10e.pdf [dostęp: 27 XI 2021].

[16] M. Grzelak, *Szpiegostwo i inwigilacja w Internecie*, w: *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, K. Liedel, P. Piasecka, T. Aleksandrowicz (red.), Warszawa 2014, s. 164–181.

powstania zakłóceń w pracy systemów. Podobny cel hakerzy mogą osiągnąć przez wprowadzenie złośliwego oprogramowania typu malware. Tym złośliwym oprogramowaniem może być wirus, koń trojański, ransomware, exploit, rootkit, keylogger czy backdoor. Wszystkie te przykłady malware'u są w stanie doprowadzić do blokady systemów teleinformatycznych i pozbawić użytkowników dostępu do informacji. Ich sposób działania jest przy tym utajniony, przez co są bardzo trudne, a w pewnych sytuacjach wręcz niemożliwe do wykrycia.

Warto zwrócić uwagę, że udostępniane często na masową skalę informacje, dane w źródłach otwartych zostają w cyberprzestrzeni już na zawsze, nie ma możliwości ich trwałego usunięcia. Dotyczy to również danych umieszczanych o nas samych na różnego rodzaju portalach społecznościowych, urzędów, które udostępniają dane publiczne, czy wszystkich innych organizacji. Ten zbiór danych jest później powszechnie dostępny, łatwy do pozyskania bez pozostawiania praktycznie żadnych śladów. To powoduje, że pozyskanie informacji do przeprowadzenia ataków może przestępcom zająć dosłownie chwilę. Ludzie poniekąd przyzwyczaili się już do bezrefleksyjnego zamieszczania informacji w Internecie, bez zastanowienia się, jaki ma to wpływ chociażby na ich prywatne bezpieczeństwo. Ponadto portale społecznościowe, ale także już witryny internetowe, przyzwyczaiły użytkowników sieci do wyrażania reakcji i swoich emocji pod zamieszczanymi postami bądź artykułami. Jednak niewiele osób sprawdza, czy polubiony przez nie post nie został później zamieniony w post nacechowany treściami negatywnymi, przestępczymi i czy nie jest wykorzystywany do popełnienia czynów zabronionych. Do takich scenariuszy są wykorzystywane np. akcje charytatywne przekonujące użytkownika, że za każdego „lajka" jest wpłacana określona kwota na leczenie danej osoby. W ten sposób dochodzi do masowych oszustw, a uzyskane pieniądze są przeznaczane na zupełnie inne cele.

Kolejnym zagrożeniem informacji jest ich przepływ generowany przez poszczególne portale społecznościowe czy narzędzia służące do pozyskiwania informacji ze źródeł otwartych. Dostępna dokumentacja niektórych portali wskazuje, że wysyłane żądania nie są kierowane do docelowych źródeł danych, a do serwerów pośredniczących. Bardzo często lokalizacje tych serwerów znajdują się na terenie Stanów Zjednoczonych, co ze względu na legislację może mieć negatywny wpływ na atrybut bezpieczeństwa informacji, jakim jest poufność. Ponadto wysyłanie żądań do serwerów pośredniczących budzi wątpliwości, czy

nie są one przypadkiem kierowane do niepożądanych lokalizacji. Ze względu na możliwość istnienia serwerów pośredniczących użytkownik nie ma żadnej pewności, czy zwracane wyniki nie są modyfikowane bądź częściowo odfiltrowywane. Przesyłanie informacji w postaci tekstowej stwarza też zagrożenie łatwego przejęcia ich w wyniku działań hakerskich. Jest to niebezpieczne zwłaszcza wtedy, gdy wyciek dotyczy informacji strategicznych bądź informacji przetwarzanych przez jednostki odpowiedzialne za zapewnienie bezpieczeństwa kraju[17].

Portale społecznościowe stały się jednym z podstawowych kanałów wymiany informacji. Często jesteśmy nawet zapewniani o komunikacji szyfrowej, inaczej zwanej bezpieczną. Należy jednak zwrócić uwagę, że nie jest to najbezpieczniejszy sposób wymiany informacji. Nie jest tajemnicą, że administracja serwisów internetowych, społecznościowych przegląda je i wykorzystuje w zależności od potrzeb. Przykładem może być portal Facebook, który wykorzystał dane ok. 87 mln użytkowników Cambridge Analytica. Działanie to polegało na przekazaniu zdjęć oraz prywatnych rozmów do działu, który zajmuje się analizą osobowości i strategiami wpływania na masowe zachowania ludności.

Niestety, ujawnienie prywatnych wiadomości nawet przez bliżej nam nieznaną administrację stron internetowych czy portali społecznościowych to nie jest optymistyczna perspektywa. Dodatkowym zagrożeniem pozostaje możliwość przekazywania informacji, wiadomości różnego rodzaju instytucjom, w tym także rządowym, bądź służbom zagranicznym.

Warto mieć świadomość, że w przypadku działań cyberprzestępców bądź co gorsza cyberterrorystów mogą oni mieć dostęp do poniższych danych:

- numerów telefonów;
- numerów kont bankowych;
- loginów i haseł do komputerów, kont bankowych, domen;
- informacji prywatnych;
- informacji o prawach własności przemysłowej i intelektualnej;
- wiedzy o planowanych projektach.

W najmniej szkodliwym przypadku pozyskane dane, pochodzące z prywatnych rozmów na platformach komunikacyjnych, informacji z portali społecznościowych czy różnych innych witryn internetowych,

[17] Przegląd dokumentacji przeprowadzony przez analityków Inseqr sp. z o.o.

są wykorzystywane do przygotowania, a następnie przedstawienia najrozmaitszych produktów w postaci reklam pojawiających się na przeglądanych stronach internetowych. Te działania mają na celu oczywiście pobudzenie zainteresowania użytkownika, a w konsekwencji nakłonienie go do zakupu. Mechanizmy sztucznej inteligencji pozwalają obecnie różnym asystentom internetowym na podsłuchiwanie naszych rozmów w celu np. dopasowania reklamy produktu mogącego nas zainteresować. Dlatego też warto zwracać uwagę na poufność prowadzonych rozmów oraz rozważyć zabezpieczenie smartfonów podczas ważnych spotkań. Przykładem produktu, który może zapewnić naszym rozmowom poufność, są dostępne już na rynku tzw. szumiki. Są to skrzynki akustyczne, które pełnią funkcję bezpiecznego depozytu urządzeń mogących przechwytywać lub przesyłać dźwięk. Rozwiązania takie bardzo często uniemożliwiają podsłuch za pomocą elektronicznych urządzeń zaopatrzonych w funkcję dyktafonu. Dodatkowo zapobiegają nasłuchowi, jaki może być prowadzony przez asystentów wbudowanych w systemy mobilne.

Poważnym zagrożeniem dla odbiorców informacji pochodzących ze źródeł otwartych jest dezinformacja, przede wszystkim ze względu na zakres jej oddziaływania. Kiedy pojawiają się terminy „dezinformacja", „fake news", ludzie zwykle myślą o postach w mediach społecznościowych z nieco fantastycznymi, nieprawdopodobnymi historiami. Jednak fałszywe wiadomości to o wiele więcej niż przesadzone tytuły artykułów w mediach społecznościowych. Dezinformacja może wydawać się nowym zjawiskiem, ale jedynymi nowościami są wykorzystywana platforma i środowisko, w którym jest ona rozprzestrzeniana. Tak naprawdę to zjawisko istnieje od wieków, a Internet jest tylko nowszym środkiem komunikacji, który może być wykorzystywany do rozpowszechniania kłamstw i dezinformacji.

Istotą dezinformacji jest taki sposób przekazania informacji – prawdziwej lub fałszywej, aby wprowadzić w błąd przeciwnika lub konkurenta i skłonić go do zachowania zgodnego z naszymi oczekiwaniami i korzystnego dla nas. Dezinformacja nie jest prostym kłamstwem, czyli przekazaniem fałszywej informacji, ale prawdziwym podstępem. Zazwyczaj akcja szerzenia dezinformacji polega na przekazywaniu wielu informacji, z których większość jest prawdziwa, a tylko jedna – kluczowa dla wywołania zakładanego efektu – jest informacją fałszywą. Zdarza się też, że akcja dezinformacyjna jest przeprowadzana na podstawie informacji

prawdziwych, lecz podanych w taki sposób, że konkurent uznaje je za fałszywe. Dodatkowo w celu zwiększenia skuteczności podczas stosowania dezinformacji wykorzystuje się kilka niezależnych od siebie źródeł i kanałów informacyjnych. Pomimo że, jak wspomniano już wcześniej, dezinformacja nie jest nowym zjawiskiem, to bez wątpienia jej znaczenie wzrosło wraz z pojawieniem się mediów masowych. Jak słusznie zauważył Tomasz Aleksandrowicz, nastąpiła weaponizacja informacji, co przyczyniło się do powstania broni masowej manipulacji[18]. Doskonałym przykładem użycia tej broni był wyciek poufnych informacji za pośrednictwem portalu WikiLeaks. Ten przypadek doskonale pokazuje, że zachowanie bezpieczeństwa danych w sieci to duże wyzwanie.

Analogicznie do trójkąta ognia, który zakłada, że niezbędne są trzy czynniki – tlen, paliwo i energia, aby doszło do rozprzestrzeniania się ognia w budynku, dezinformacja również wymaga trzech różnych elementów, aby odnieść sukces. Wspólnie tworzą one trójkąt fałszywych wiadomości, a brak chociaż jednego z nich spowoduje, że fałszywe wiadomości nie będą w stanie się rozprzestrzeniać i docierać do docelowych odbiorców.

Rys. 7. Trójkąt fałszywych wiadomości.

Źródło: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media [dostęp: 26 XI 2021].

Pierwszym elementem są narzędzia i usługi służące do manipulowania i rozpowszechniania wiadomości w odpowiednich sieciach społecznościowych. Na świecie jest dostępna szeroka gama narzędzi

[18] T.R. Aleksandrowicz, *Zagrożenia dla bezpieczeństwa informacyjnego państwa w ujęciu systemowym. Budowanie zdolności defensywnych i ofensywnych w infosferze*, Warszawa 2021, s. 32–49.

i usług, część z nich jest stosunkowo prosta (płatne polubienia/obserwatorzy itp.), inne są bardziej skomplikowane — niektóre usługi obiecują przekazanie ankiet online, kolejne zmuszają właścicieli witryn do usuwania historii.

Oczywiście aby te narzędzia były przydatne, muszą istnieć sieci społecznościowe jako platforma do szerzenia propagandy. Ponieważ ludzie spędzają w nich dużo czasu, aby uzyskać najnowsze informacje, nie można nie docenić ich znaczenia w rozpowszechnianiu fałszywych wiadomości. Istnieje jednak różnica między zwykłym publikowaniem propagandy a przekształcaniem jej w coś, co konsumuje docelowa publiczność. Badanie mediów społecznościowych stwarza również możliwość spojrzenia na relacje między botami a odbiorcami promocji w mediach społecznościowych, np. w serwisie Twitter, a dzięki temu daje wyobrażenie o zakresie i organizacji kampanii próbujących manipulować opinią publiczną.

Kampania propagandowa zawsze niesie ze sobą pytanie: dlaczego? Motywy, którymi kierują się osoby rozpowszechniające fake newsy, są różne. Czasami jest to po prostu chęć zdobycia pieniędzy poprzez reklamę, ale może chodzić również o cele kryminalne czy polityczne. Niezależnie od motywu, sukces każdej kampanii propagandowej ostatecznie mierzy się tym, jak bardzo wpływa ona na rzeczywisty świat.

Reasumując, o dezinformacji można mówić, gdy rozpowszechniane informacje:

- są całkowicie lub częściowo fałszywe, zmanipulowane lub wprowadzające w błąd;
- dotyczą kwestii ważnej z punktu widzenia interesu publicznego;
- mają wywołać niepewność lub wrogość, doprowadzić do polaryzacji społeczeństwa albo zakłócenia procesów demokratycznych;
- są rozpowszechniane lub wzmacniane za pomocą zautomatyzowanych i agresywnych technik, takich jak boty społeczne, sztuczna inteligencja (ang. *artificial intelligence*, AI), mikrotargeting lub trollowanie.

Dezinformacja może destabilizować sytuację w państwie, wywierać destrukcyjny wpływ na jego struktury administracyjne i decyzyjne, a także podważać podstawy społeczne, ekonomiczne oraz kulturowe. Według raportu *Freedom on the Net 2017: Manipulating Social Media to*

Undermine Democracy[19] coraz więcej krajów na świecie wykorzystuje media społecznościowe do działań dezinformacyjnych – zarówno do kształtowania swojej polityki wewnętrznej, jak i do wpływania na inne państwa. Przeciwdziałanie dezinformacji staje się wyzwaniem, przed jakim stoją nie tylko pojedyncze państwa, lecz także instytucje i organizacje międzynarodowe. Konieczność przeciwdziałania kampaniom dezinformacyjnym w Europie podkreśliła po raz pierwszy Rada Europejska w marcu 2015 r. Od tego czasu w strukturach Europejskiej Służby Działań Zewnętrznych (ang. European External Action Service) powstało kilka zespołów zajmujących się analizowaniem dezinformacji w Unii Europejskiej oraz krajach sąsiadujących ze wspólnotą.

Problem dezinformacji – na szczeblu ogólnopaństwowym i strategicznym – był poruszany w Biurze Bezpieczeństwa Narodowego podczas prac nad rekomendacjami do nowej Strategii Bezpieczeństwa Narodowego. Omawiano go również na forum międzynarodowym oraz w trakcie licznych spotkań eksperckich organizowanych w BBN. Z dyskusji wynika, że największymi wyzwaniami w środowisku informacyjnym są obecnie:

- brak zrozumienia wagi i charakteru problemu;
- brak sprawnego systemu komunikacji strategicznej i koordynacji działań w zakresie zwalczania dezinformacji na szczeblu krajowym;
- niski poziom umiejętności korzystania z mediów wśród wybranych grup społecznych;
- wypracowanie równowagi między wolnością słowa a przeciwdziałaniem dezinformacji;
- zbudowanie pozytywnej narracji oraz promocja państwa na zewnątrz.

Wszystkie te wyzwania mają charakter uniwersalny i w dużej mierze dotyczą także Polski jako państwa należącego do wspólnoty cywilizacji zachodniej podzielającej wartości demokratyczne. W ujęciu międzynarodowym dezinformacja jest najczęściej wymierzona właśnie w procedury demokratyczne i ma podważyć zaufanie obywateli do państwa. Takie działanie zagraża także bezpieczeństwu narodowemu. Działania dezinformacyjne wprowadzają obywateli w błąd i często wzbudzają

[19] https://freedomhouse.org/article/new-report-freedom-net-2017-manipulating-social-media-undermine-democracy [dostęp: 28 XI 2021].

w nich niepewność. Uniemożliwia im to m.in. podejmowanie suwerennych, opartych na wiarygodnych informacjach, decyzji wyborczych.

Przeciwdziałanie dezinformacji wymaga przede wszystkim:

- podnoszenia świadomości obywateli na temat zagrożeń dezinformacyjnych;
- budowania zdolności instytucjonalnych;
- podjęcia współpracy różnych instytucji z komórkami ds. komunikacji strategicznej w krajach i instytucjach UE i NATO;
- projektowania i wdrażania działań aktywnych, tj. prowadzenia projektów i kampanii informacyjnych;
- wsparcia polskich organizacji pozarządowych i podjęcia z nimi współpracy.

Aby rozpoznać dezinformację, należy:

1. Poznać źródło informacji (zrozumieć jego cele i intencje), dowiedzieć się, kto odpowiada za to źródło, kto jest jego właścicielem itp.
2. Czytać całość artykułu, a nie tylko nagłówek (aby zrozumieć cały materiał).
3. Sprawdzić autorów, aby zweryfikować, czy są oni wiarygodni. Nie zawsze jest to możliwe, ponieważ nie wszystkie artykuły są podpisane z nazwiska oraz nie wszyscy autorzy – nawet w wiarygodnych treściach – są podpisani. Jeśli jest taka możliwość, dobrze jest wyszukać nazwisko autorki czy autora i zobaczyć inne treści, które ta osoba tworzy.
4. Sprawdzić tę informację w innych źródłach (upewnić się, że podają te same dane).
5. Znaleźć datę publikacji (aby sprawdzić, czy informacje są aktualne).
6. Przemyśleć własne uprzedzenia (aby zobaczyć, czy nie wpływają one na nasz osąd).
7. Zapytać ekspertów (uzyskać potwierdzenie od niezależnych ludzi dysponujących wiedzą na dany temat).

W obliczu ogromnej liczby informacji, które na co dzień są przetwarzane w źródłach otwartych, powstaje problem w odróżnieniu prawdy od kłamstwa. Bardzo często mamy do czynienia z kreowaniem pewnych wizji, zwłaszcza przez media, zamiast z przedstawianiem wiarygodnych informacji. Ponadto dynamiczne tempo życia sprawia, że cykl życia informacji jest bardzo krótki. Informację, która pojawiła się

dzisiaj i poruszyła opinię publiczną, kolejnego dnia zastąpi inna, równie ważna. Dodatkowo przesyt różnych informacji sprawia, że procesy decyzyjne bywają niezwykle skomplikowane, a ludzie kierują się nie stanem rzeczywistym, a raczej społecznym postrzeganiem danych faktów. Do tego dochodzi jeszcze manipulowanie informacjami w celu osiągnięcia określonych korzyści. Za przykład może posłużyć szerzenie dezinformacji przez Rosję podczas wyborów prezydenckich w Stanach Zjednoczonych w 2016 r. Taki stan rzeczy to ogromny problem współczesnych społeczeństw. Obecnie bardzo trudno jest kontrolować obieg informacji publicznych, istnieje bowiem wiele narzędzi manipulacyjnych podważających w dużym stopniu wiarygodność przedstawianych informacji. Dodatkowo bardzo niepokojąca jest sytuacja, w której ataki informacyjne stają się rozpoznawalne dopiero w momencie osiągnięcia celu przez atakującego bądź nie są rozpoznawane wcale. Zasadne wydają się zatem słowa Sławomira Zalewskiego, który powiedział: „(...) stwierdzenie braku występowania zagrożeń nie eliminuje ich w przyszłości, ale też nie wyklucza, że działania stanowiące zagrożenie podejmowane są tu i teraz, tyle że zostały jeszcze nierozpoznane”[20].

Biorąc pod uwagę liczne zagrożenia informacji w cyberprzestrzeni, należy zauważyć, że największe państwa na świecie wprowadziły specjalne regulacje prawne mające na celu ochronę zasobów teleinformatycznych oraz przeciwdziałanie zagrożeniom w tym zakresie. Między innymi Rosja w ustawie o ochronie danych osobowych wraz z jej późniejszymi uzupełnieniami wprowadziła nakaz przechowywania danych osobowych Rosjan wyłącznie na terenie ich państwa[21]. Stany Zjednoczone ustanowiły CLOUD Act[22], który zobowiązuje amerykańskich dostawców usług o charakterze elektronicznym do ujawnienia na żądanie amerykańskiego sądu informacji dotyczących użytkowników tych usług, niezależnie od tego, czy są one przetwarzane w Stanach, czy w dowolnym innym państwie na świecie. Warto również zwrócić uwagę na ustawę o cyberbezpieczeństwie wprowadzoną w Chinach i ustawę wyznaczającą Narodowy Standard Bezpieczeństwa Informacyjnego. Otóż dokumenty te sankcjonują zasadę, że każdy sprzęt oraz oprogramowanie dostarczane na potrzeby

[20] S. Zalewski, *Bezpieczeństwo polityczne. Zarys problematyki*, Siedlce 2013, s. 148.

[21] https://gdpr.pl/panstwa-spoza-ue-a-rodo-czesc-i-rosja [dostęp: 28 XI 2021].

[22] https://epic.org/wp-content/uploads/privacy/cloud-act/cloud-act-text.pdf [dostęp: 28 XI 2021].

podmiotów rządowych bądź podmiotów z obszaru infrastruktury krytycznej muszą być audytowane przez wyznaczone i przygotowane do tego jednostki. Sprawdzeniu podlega też kod źródłowy oprogramowania kupowanego na potrzeby powyższych jednostek.

W 2014 r. proces skutecznego tworzenia systemu cyberbezpieczeństwa rozpoczęto na Ukrainie. Najważniejszym impulsem do podjęcia takich działań były cyberataki na sieć elektroenergetyczną, które doprowadziły do tymczasowych przerw w dostawie energii elektrycznej. W 2016 r. została zatwierdzona Strategia Cyberbezpieczeństwa Ukrainy w której podkreślono potrzebę prac legislacyjnych w zakresie krajowego systemu cyberbezpieczeństwa[23]. Uznano, że powyższe działania są podstawą bezpieczeństwa narodowego. Ponadto skupiono się na interakcji pomiędzy działaniami podejmowanymi przez organy państwowe, samorządowe, formacje wojskowe, instytucje naukowe, a także podmioty komercyjne. Pomimo wprowadzenia dokumentów legislacyjnych na Ukrainie istnieją ogromne problemy z rozwojem strategii cyberbezpieczeństwa. Wynikają one m.in. z braku skutecznej realizacji polityki cyberbezpieczeństwa, braku świadomości z zakresu cyberzagrożeń oraz niewystarczającego potencjału ludzkiego. Problemy stwarza również: brak prawnych i organizacyjnych ram ochrony infrastruktury krytycznej, brak aktualnych standardów cyberbezpieczeństwa oraz słabe ustawodawstwo krajowe dotyczące cyberprzestępczości[24].

Na uwagę zasługują działania podejmowane w Estonii, które mogą być wzorem dla innych państw. Estonię należy uznać za pioniera cyfryzacji w Europie, co potwierdza wprowadzenie już w 2008 r. strategii cyberbezpieczeństwa[25]. Był to pierwszy tego typu dokument na świecie. Estonia nieustannie pracuje nad zwiększeniem poziomu cyberbezpieczeństwa. Wynika to przede wszystkim z wysoce rozwiniętych e-usług, a działania prewencyjne mają przeciwdziałać przestępczości w sieci. Estonia jest zwolennikiem jednolitego rynku cyfrowego na obszarze Unii Europejskiej, co ma przełożyć się na wymierne zyski w perspektywie

[23] J. Semeniy, S. Glushchenko, O. Makarevich, *Ukraine*, w: *Cybersecurity 2018*, B.A. Powell, J.C. Chipman (red.), Law Business Research, London, s. 99.

[24] V. Boiko, *Comparison of the Polish and Ukrainian cybersecurity system*, „Teka of Political Science and International Relations" 2019, t. 14, nr 2, s. 119–137.

[25] Narodowa Strategia Cyberprzestrzeni Estonii, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Estonia [dostęp: 28 XI 2021].

rozwoju e-gospodarki. Ponadto usilnie mobilizuje państwa członkowskie do wspólnych działań na rzecz cyfryzacji i bezpieczeństwa w cyberprzestrzeni. Przedmiotem zainteresowania są m.in.: ochrona danych osobowych w sieciach komórkowych i na stronach internetowych, swobodny przepływ danych nieosobowych, a także opodatkowanie usług internetowych. Estonia realizując politykę cyberbezpieczeństwa, stara się przede wszystkim uporządkować istniejące regulacje, a także adaptować je do dynamicznie zmieniających się uwarunkowań. W dalszym ciągu dąży też do doskonalenia technologii wspomagającej reagowanie na incydenty w cyberprzestrzeni poprzez m.in. poprawę infrastruktury sieci, skoordynowanie administrowania systemami informatycznymi oraz wzmocnienie działu IT w administracji[26].

Wymiernym działaniem na terenie Unii Europejskiej w zakresie cyberbezpieczeństwa było przyjęcie *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*[27], tzw. RODO, wiążącego wszystkich przetwarzających dane osobowe w związku z prowadzoną działalnością gospodarczą. Za pomocą powyższego rozporządzenia wprowadzono wiele zmian oraz zwiększono zakres obowiązków administratorów i podmiotów przetwarzających dane.

W związku z tym, że cyberbezpieczeństwo stanowi obecnie jedno z największych wyzwań, jakie stoją przed administratorami i użytkownikami sieci teleinformatycznych, unijną odpowiedzią na nie jest również *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 roku w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii*[28]. Na terenie Polski dyrektywa ta została zaimplementowana *Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*[29]. Ustawa nałożyła nowe obowiązki na podmioty mające wpływ na bezpieczeństwo państwa. Między innymi wymogiem stały się audyty wewnętrzne systemów

[26] K. Raś, *Estonia jako lider w zwiększeniu cyberbezpieczeństwa*, „Biuletyn – Polski Instytut Spraw Międzynarodowych" 2018, nr 68, s. 20–22.

[27] Dz. Urz. UE L 119/1 z 27 IV 2016 r.

[28] Dz. Urz. UE L 194/1 z 6 VII 2016 r.

[29] Tekst jednolity: DzU z 2020 r. poz. 1369, ze zm.

teleinformatycznych, opracowywanie stosownej dokumentacji, wdrażanie systemów zarządzania bezpieczeństwem, a także przeprowadzanie czynności pozwalających na wykrywanie, rejestrowanie, analizowanie oraz klasyfikowanie incydentów. W Polsce została też uchwalona *Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*[30]. Na mocy tego dokumentu do zadań Agencji Bezpieczeństwa Wewnętrznego włączono m.in.: rozpoznawanie 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, oraz zapobieganie tym zagrożeniom. Szef ABW jest odpowiedzialny za prowadzenie centralnego rejestru zdarzeń o charakterze terrorystycznym naruszających bezpieczeństwo systemów teleinformatycznych o szczególnym znaczeniu dla bezpieczeństwa państwa albo sieci teleinformatycznych. Ponadto w celu zapobiegania i przeciwdziałania zdarzeniom o charakterze terrorystycznym w cyberprzestrzeni oraz ich zwalczania ABW może dokonywać oceny bezpieczeństwa systemów teleinformatycznych polegającej na przeprowadzeniu testów bezpieczeństwa w celu identyfikacji podatności. Przez podatność rozumie się słabość zasobu lub zabezpieczenia systemu teleinformatycznego, która może zostać wykorzystana i zagrozić integralności, poufności, rozliczalności i dostępności tego systemu.

Przedstawione przykłady pokazują, jak istotna jest ochrona zasobów informacyjnych na arenie międzynarodowej oraz jakie środki bezpieczeństwa pozwolą przeciwdziałać wszelkim zagrożeniom związanym z przepływem informacji.

Warto również zaznaczyć, że działania cyberprzestępców wywierają duży wpływ na obiekty należące do infrastruktury krytycznej. Ich celem jest przede wszystkim podważenie zaufania publicznego wobec społeczeństwa obywatelskiego i fundamentów demokracji. Jest to także zagrożenie suwerenności, które daje organizacjom terrorystycznym i kryminalistom możliwość anonimowego działania przy wykorzystaniu technik oraz skutecznych metod wpływania na politykę i strategię

[30] Tekst jednolity: DzU z 2021 r. poz. 2234.

innych państw. Przykładem mogą być działania Rosji, która jest jednym z najaktywniejszych sprawców cyberataków, podczas bezprawnej aneksji Krymu w 2014 r. Kolejnym przykładem są Chiny, które aktywnie zaangażowały się w przeprowadzanie cyberataków i kampanie dezinformacyjne skierowane przeciwko członkom sojuszu NATO i stanowią bardzo poważne zagrożenie krytycznych elementów infrastruktury energetycznej, co zostało podkreślone w ekspertyzie NATO 2030[31].

Cyberataki przeprowadzone w ciągu ostatnich 15 lat są dowodem na to, że mają one wpływ zarówno na tych, którzy je przeprowadzają – cyberprzestępców, jak i na środowiska, które próbują bronić sieci. Obecnie środowisko związane z cyberbezpieczeństwem wymaga wielu narzędzi i rozwiązań, które zazwyczaj są bardzo kosztowne. Ataki prowadzone naźmniejszą skalę to jedynie przyczółek do większych ataków, a idąc dalej – do rozwoju cyberbroni. Rozwój cyberataków sprawił, że specjaliści w dziedzinie bezpieczeństwa cybernetycznego zaczęli uważać je za nagminne zjawisko i skoncentrowali swoje działania na obronie sieci. Metody zapewnienia cyberbezpieczeństwa, jak i sposób reakcji na ataki muszą ewoluować adekwatnie do sposobów działania cyberprzestępców. W związku z tym, że za środowisko internetowe w większości odpowiada sektor komercyjny, organizacje państwowe i podmioty prywatne powinny rozważyć współpracę w zakresie bezpieczeństwa sieci. Wymaga to jednak szerokich zmian legislacyjnych dotyczących działań proaktywnych i reaktywnych podejmowanych w odpowiedzi na zagrożenia cybernetyczne.

Zasadny wydaje się rozwój doktryny operacyjnej realizowanej przez krajowe siły cybernetyczne, które powinny być rozwijane, testowane oraz modyfikowane w zależności od zagrożeń. Organizacja ćwiczeń bilateralnych wydaje się dobrym wstępem do dalszej kooperacji. W dłuższej perspektywie w ćwiczeniach powinni brać udział również przedstawiciele sektora komercyjnego odpowiedzialni za działania ochronne. Przedstawiciele organów i instytucji państwowych nie powinni obawiać się współpracy z ekspertami do spraw cybernetyki reprezentującymi ten sektor, gdyż przejęli oni już inicjatywę i prowadzą działania wyprzedzające. Ponadto globalny charakter Internetu wymaga współpracy międzynarodowej. Indywidualne rozwiązania stosowane w poszczególnych państwach nie będą efektywne w obliczu zagrożeń cybernetycznych, gdyż walka z tymi zagrożeniami wymaga spójnego

[31] https://nato.int [dostęp: 29 XI 2021].

i elastycznego podejścia. NATO jako organizacja międzynarodowa ma wieloletnie doświadczenie w kreowaniu polityki i przeprowadzaniu operacji skierowanych przeciwko zagrożeniom o charakterze konwencjonalnym. Jednak teraz nastąpił czas, aby zdobyte doświadczenie i wiedzę specjalistyczną wykorzystać w celu zapewnienia i utrzymania cyberbezpieczeństwa[32].

Reasumując, należy stwierdzić, że założona hipoteza została zweryfikowana. W ciągu ostatnich kilkudziesięciu lat nastąpił ogromny postęp technologiczny związany z rozwojem nowoczesnych technologii, a przede wszystkim powstaniem zaawansowanego społeczeństwa informacyjnego. Obecnie nikt już nie wyobraża sobie życia bez dostępu do Internetu, a tym samym do informacji pochodzących ze źródeł otwartych. Ich powszechność, dostępność, niski koszt pozyskania sprawiają, że są one pierwszym źródłem, z którego się korzysta. Jednakże wraz z ich rozwojem powstały także nowe zagrożenia, często o charakterze cyberterrorystycznym, które stanowią ogromne niebezpieczeństwo dla człowieka jako jednostki, jak również organizacji oraz struktur państwowych. Bezpieczeństwo informacyjne to obszar, który wymaga podjęcia radykalnych i natychmiastowych działań, gdyż cyberprzestępcy w sposób utajniony są w stanie dotrzeć do wszelkich systemów, aby zrealizować zaplanowany cel. Sytuacji nie sprzyja dynamicznie zmieniające się środowisko, pandemia koronawirusa i przeniesienie życia do świata Internetu, a także konflikty między państwami mające na celu zdobycie przewagi na arenie międzynarodowej. Implementowane regulacje prawne wydają się niewystarczające do ochrony informacji. Trzeba stworzyć efekt synergii poprzez połączenie działań międzynarodowych, a także działań na poziomie poszczególnych państw, aby na stałe zapewnić bezpieczeństwo sieci, na poziomie zarówno krajowym, jak i międzynarodowym. Należy mieć świadomość, że ataki cyberterrorystyczne będą występować, a nawet się nasilać. Ich skala może być bardzo różna, od manipulacji informacjami i szerzenia dezinformacji po ataki na systemy teleinformatyczne infrastruktury krytycznej. Pomimo że całkowite wyeliminowanie cyberterroryzmu nie jest realne, należy podejmować działania prewencyjne, a także mające na celu jak najszybsze wykrywanie ataków o charakterze cyberterrorystycznym i minimalizowanie powodowanych przez nie strat.

[32] W.E. Leigher, *Cyber conflict in a hybrid threat environment: Death by a thousand cuts*, Helsinki 2021.

Bibliografia

Aleksandrowicz T.R., *Zagrożenia dla bezpieczeństwa informacyjnego państwa w ujęciu systemowym. Budowanie zdolności defensywnych i ofensywnych w infosferze,* Warszawa 2021.

Boiko V., *Comparison of the polish and Ukrainian cybersecurity system,* „Teka of Political Science and International Relations" 2019, t. 14, nr 2, s. 119–137.

Elliott A., *Castells M.: Społeczeństwo sieci,* w: Elliott A., *Współczesna teoria społeczna. Wprowadzenie,* Warszawa 2011.

Grzelak M., *Szpiegostwo i inwigilacja w Internecie,* w: *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji,* K. Liedel, P. Piasecka, T. Aleksandrowicz (red.), Warszawa 2014, s. 164–181.

Hall R., Fox C., *Ponownie przemyśleć bezpieczeństwo,* „Przegląd NATO" zima 2001/2002.

Kissinger H., *Dyplomacja,* Warszawa 2016.

Leigher W.E., *Cyber conflict in a hybrid threat environment: Death by a thousand cuts,* Helsinki 2021.

Measuring the Information Society Report, t. 1, Geneva 2018.

Nowak J.S., *Społeczeństwo informacyjne – geneza i definicje,* w: *Społeczeństwo informacyjne. Krok naprzód, dwa kroki wstecz,* P. Sienkiewicz, J.S. Nowak (red.), Katowice 2008.

Oleński J., *Ekonomika informacji,* Warszawa 2001.

Raś K., *Estonia jako lider w zwiększeniu cyberbezpieczeństwa,* „Biuletyn – Polski Instytut Spraw Międzynarodowych" 2018, nr 68, s. 20–22.

Saramak B., *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy,* Warszawa 2015.

Sienkiewicz P., *Społeczeństwo informacyjne jako system cybernetyczny,* w: *Społeczeństwo informacyjne. Wizja czy rzeczywistość?,* t. 1, L.H. Haber (red.), Kraków 2004.

Semeniy J., Glushchenko S., Makarevich O., *Ukraine,* w: *Cybersecurity* 2018, B.A. Powell, J.C. Chipman (red.), Law Business Research, London.

Sosińska-Kalata B., *Obszary badań współczesnej informatologii (nauki o informacji)*, „Zagadnienia Informacji Naukowej" 2013, nr 2, s. 9–41.

Sun Tzu, *Sztuka wojny*, Gliwice 2004.

West Ch., *Competitive intelligence*, New York 2001.

Zalewski S., *Bezpieczeństwo polityczne. Zarys problematyki*, Siedlce 2013.

Źródła internetowe

https://datareportal.com/reports/digital-2021-global-overview-report [dostęp: 26 XI 2021].

https://epic.org/wp-content/uploads/privacy/cloud-act/cloud-act-text.pdf [dostęp: 28 XI 2021].

https://freedomhouse.org/article/new-report-freedom-net-2017-manipulating-social-media-undermine-democracy [dostęp: 28 XI 2021].

https://gdpr.pl/panstwa-spoza-ue-a-rodo-czesc-i-rosja [dostęp: 28 XI 2021].

https://nato.int [dostęp: 29 XI 2021].

http://unicjin.org/documents/congr10/10e.pdf [dostęp: 27 XI 2021].

http://www.bbc.uw.edu.pl/Content/20/08.pdf [dostęp: 25 XI 2021].

https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Estonia [dostęp: 28 XI 2021].

Akty prawne

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119/1 z 27 IV 2016 r.).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 roku w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194/1 z 6 VII 2016 r.).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (DzU z 2020 r. poz. 1369, ze zm.).

Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych (DzU z 2021 r. poz. 2234.).