Tom 14/2022, ss. 127-141
ISSN 0860-5637
e-ISSN 2657-7704
DOI: 10.19251/rtnp/2022.14(3)
www.rtnp.mazowiecka.edu.pl

Ewa Jóźwiak

Znaczenie informacji wobec stanu bezpieczeństwa polskiego społeczeństwa w obliczu wojny w Ukrainie

The importance of information for the security of the Polish community in the face of the war in Ukraine

Streszczenie: Artykuł poświęcono problematyce wpływu informacji na bezpieczeństwo osobiste człowieka jako jednostki społecznej. Zdefiniowano pojęcie bezpieczeństwa oraz wskazano na konkretne zachowania posiadające znamiona przemocy w cyberświecie. Poruszono także kwestię inwazji Rosji na Ukrainę, która obniżyła poczucie bezpieczeństwa również w krajach trzecich, w tym zwłaszcza w Polsce. W literaturze pojęcie informacji oraz społeczeństwa informacyjnego rozpatrywane jest w wielu aspektach. Propaganda oraz manipulacja są głównymi trendami dezinformacyjnymi, które należy minimalizować. Sieć wirtualna to medium komunikacyjne, które nieustannie rozszerza się o nowe zasoby co powoduje, że wszelkie procesy informacyjne mają charakter zbiorowy bądź indywidualny. Cyberprzestrzeń jest polem powstawania cybermanipulacji, propagandy oraz wywierania wpływów.
Słowa kluczowe: informacja, cyberprzestrzeń, Internet, media, cybermanipulacja, dezinformacja

Summary: The article deals with the issue of the impact of information on personal security of a person as a social unit. It defines the concept of security and identifies specific behaviours that have the hallmarks of violence in the cyber world. The issue of Russia's invasion of Ukraine, which definitely lowered the feeling of security also in third countries, especially in Poland, was also addressed. In the specialist literature, the concept of information and the information society is considered in many aspects. Propaganda and manipulation are the main disinformation trends to be minimised. The virtual web is a communication medium that is constantly expanding with new resources, which makes all information processes collective or individual. Cyberspace is a field of cyber-manipulation, propaganda and influence.
Keywords: information, cyberspace, internet, media, cyber-manipulation, disinformation

Wstęp

Stan poczucia bezpieczeństwa jest mocno powiązany z zaspokajaniem złożonych potrzeb człowieka od biologicznych po społeczne czy kulturowe. Istnieje pogląd wskazujący, iż bezpieczeństwem jest pewność istnienia, wynikająca głównie z braku zagrożeń oraz pewność przetrwania, egzystencji, stanu posiadania oraz rozwoju jednostki. Odczuwanie tej pewności jest utożsamiane z realiami społecznymi. Zagrożenie określane jest jako ewentualność wystąpienia negatywnie wartościowanego zdarzenia bądź stanu świadomości[1]. Definicja bezpieczeństwa wymaga rozważań na gruncie różnych dziedzin nauki ze względu na wieloaspektowość tego pojęcia. Najprościej ujmując bezpieczeństwo to „*stan gwarantujący pewność istnienia i przetrwania*"[2]. Systemy bezpieczeństwa mają swoje przedmioty ochrony i podkreślają je bardziej niż inne. Przyjmując kategorię jednostki oraz jej wartości, które mają być chronione, należy

[1] K. Szewior, *Bezpieczeństwo społeczne jednostki. Założenia i polska rzecz*ywistość, Wyd. UW, Warszawa 2016, s. 74.

[2] S. Jarmoszko, C. Kalita, J. Maciejewski, *Nauki społeczne wobec problemu bezpieczeństwa (wybrane zagadnienia)*, [w:] S. Jarmoszko, *Teoretyczne konceptualizacje i sensy bezpieczeństwa w naukach społecznych*, Uniwersytet Przyrodniczo-Humanistyczny, Siedlce 2016, s. 27.

wziąć pod uwagę możliwość ich utraty, co mogłoby wywołać niepożądane stany emocjonalne takie jak lęk czy niepokój[3]. Dlatego określając bezpieczeństwo człowieka jako pewność istnienia, przetrwania i funkcjonowania, należy rozpatrywać je zarówno w danej społeczności, jak i każdej przestrzeni życia[4]. Wraz z nieustannym unowocześnianiem technologii informacyjnych neutralizowana jest rola oddziaływań fizycznych w relacjach międzyludzkich. Na pierwszym miejscu stawiany jest wpływ na proces myślowy, a następnie zachowanie zewnętrzne lub stan fizyczny[5]. Wszelkie oddziaływania w cyberświecie mają wymiar emocjonalny i intelektualny. W świecie Internetu, a przede wszystkim w sferze informacji odnotowuje się coraz więcej działań mających znamiona cyberprzemocy. Nieadekwatne komunikaty informacyjne czy nieumiarkowane formy ich przekazu to oddziaływania prowadzące do podjęcia przez jednostkę niezamierzonych czynności, a w konsekwencji wywołania niechcianych rezultatów. Presję i nacisk prowokuje nieprawdziwa i naszpikowana fałszem informacja. Jest ona dobrem wielkiej wagi w otaczającej nas przestrzeni, zarówno realnej jak i wirtualnej. Rozwój nowych technologii w XX wieku spowodował powstanie społeczeństwa informacyjnego. Wyjaśniając ten termin, warto się odnieść do raportu Narodowej Akademii Nauk USA z 1979 roku, w którym zwrócono uwagę na powstającą cywilizację informacyjną opartą na postępie technologicznym[6]. Z roku na rok społeczeństwo informacyjne rozwija się razem ze wzrostem funkcjonalności systemu informacyjnego. Umysł oraz mentalność jednostki w dobie społeczeństwa informacyjnego nie posiadają bariery przed manipulacją, dezinfor-

[3] L. F. Korzeniowski, *Podstawy nauk o bezpieczeństwie*, Difin, Warszawa 2012, s. 76.

[4] R. Zięba, *Bezpieczeństwo międzynarodowe po zimnej wojnie*, WAiP, Warszawa 2008, s. 16.

[5] J. Janowski, *Cybermanipulacja jako samodzielna forma i stały składnik przemocy informacyjnej w cyberprzestrzeni* [w:] *Cyberprzemoc szczególnym zagrożeniem społeczeństwa informacyjnego*, M. Kowalewski, M. Jakubiak (red.), Oficyna Wyd. Politechniki Warszawskiej, Warszawa 2021, s. 28.

[6] A. M. Wilk, *Państwo w dobie społeczeństwa informacyjnego - perspektywa strategicznych zmian*, w: *Internet 2000. Prawo - ekonomia - kultura*, red. R. Skubisz, Lublin 2000, s. 194.

macją czy bezwzględną i zmasowaną propagandą[7]. Dlatego też zagrożenia w cyberprzestrzeni są i będą istotnymi problemami społecznymi.

Charakter cyberprzestrzeni

Infrastruktura cyberprzestrzeni sprzyja budowaniu dezinformacji. Przestrzeń, która zrzesza miliony ludzi, stwarza warunki do ataków na psychikę poszczególnych osób[8]. Korzystanie z wirtualnej sfery połączone jest z możliwością wystąpienia pewnych zagrożeń, które mogą mieć wpływ na funkcjonowanie zdrowotne oraz psychospołeczne jednostki. Umiejętne i świadome korzystanie z cyberprzestrzeni identyfikuje się częściowo z zagwarantowaniem stanu, który jest wolny od ryzyka utraty ważnych dla użytkownika informacji poprzez stosowanie instrumentów ochronnych, właściwych do skali zagrożenia[9]. Manfred Spitzer zauważył, że sieć wirtualna oraz elektroniczne urządzenia są nośnikami anonimowości[10]. Cyberprzestrzeń została też nazwana „*mekką*" wszystkich, którzy poszukują interakcji, przy zachowaniu pełnej anonimowości. Przeświadczenie o anonimowości w Internecie kształtuje nietolerowane aktywności, a indywidualni uczestnicy świata online zazwyczaj lekceważąco podchodzą do ochrony swoich danych w sieci. Wynika to głównie z niskiej świadomości dotyczącej potencjalnych zagrożeń mogących wystąpić w Internecie[11]. Organizacje pozarządowe realizują programy, mające na celu minimalizację zjawiska wykluczenia cyfrowego ludzi w średnim i starszym wieku. Osoby młode, spędzające wiele czasu w przestrzeni cyfrowej, bagatelizują skutki braku zabezpieczeń sieciowych, a osoby 50+, 60+ czy 70+, rozpoczynając przygodę ze światem

[7] O. Wasiuta, S. Wasiuta., *Wojna informacyjna zagrożeniem dla bezpieczeństwa ludzkości*, Kraków 2017, s.76.

[8] J. Janowski, *Cybermanipulacja…*, op. cit., s. 33.

[9] M. Fraczek, *Zagrożenia w cyberprzestrzeni dla Polski i krajów Unii Europejskiej, Materiał opracowany na II Ogólnopolski Kongres Politologii*, UAM Poznań 2012, s. 9.

[10] M. Spitzer, *Cyfrowa demencja*, Wyd. Dobra Literatura, Warszawa 2020, s. 9.

[11] M. Fraczek, *Zagrożenia…*, op.cit., s. 145.

wirtualnym są bezradne. Poznając zasady bezpiecznego korzystania z sieci, są w stanie uchronić się od niebezpieczeństw tam panujących. Dlatego zinstytucjonalizowana edukacja w zakresie informatyki stanowi istotny element strategii bezpieczeństwa w cyberprzestrzeni. Wnioskuje się, że problem patologii cyfrowej może się pogłębiać razem z dynamizacją społeczeństwa informacyjnego oraz rozszerzaniem dostępu do przestrzeni sieciowej. Analogicznie za barierami tworzenia coraz lepszych i skuteczniejszych zabezpieczeń powinno iść dążenie do edukowania się w zakresie niezagrożonego użytkowania Internetu[12].

Informacyjna wojna – techniki i działanie

Osoba przeprowadzająca atak często korzysta z socjotechnik, czyli takich mechanizmów psychologicznych, które za cel stawiają manipulowanie społeczeństwem w celu spełnienia założonej misji. Zmanipulowana osoba często udziela nieświadomie zbyt wielu informacji, które ułatwiają dalsze procesy w łańcuchu cyberprzemocy. Portale społecznościowe, komunikatory i pozostałe media są zazwyczaj zsynchronizowane z innymi serwisami zewnętrznymi, co sprzyja powstawaniu zalewu informacji na temat przedmiotu ostatniej frazy wpisanej do wyszukiwarki. Użytkownicy wirtualnego świata pragnący nieustannie być jego częścią są poddawani inwigilacji i manipulacji. Każdy uczestnik cyberprzestrzeni nie jest w stanie odpowiednio zabezpieczyć się przed cyberinwigilacją oraz cybermanipulacją, które są nieodłącznymi komponentami przemocy w sieci. Każda funkcjonująca w świecie jednostka chce być w ciągłym kontakcie ze światem. Człowiek, podążając za nowymi trendami, dąży do samodoskonalenia, rozwoju oraz do wyzwolenia z ograniczeń, jakie daje odcięcie od globalnego kontaktu. Pozorna, przyciągająca siła funkcjonalności Internetu

[12] A. Waligórska-Kotfas, Bezpieczeństwo w Internecie jako wyzwanie społeczeństwa informacyjnego [w:] Wybrane problemy i wyzwania bezpieczeństwa. Bezpieczeństwo jednostkowe – Bezpieczeństwo zbiorowe. Ujęcie interdyscyplinarne, K. Zawieja-Żurowska (red.), Wydawnictwo PWSZ w Koninie, Konin 2015, s. 173.

sprawia, że jednostka izoluje się. Badacze zauważają że rezultatem ewolucji technologicznej jest wyłączenie się użytkownika z realnego świata. Jednostka zdolna i racjonalna ulega manipulacji, staje się ofiarą w sieci, ulegając wpływom zewnętrznym, zmieniając istotę postrzeganej wcześniej rzeczywistości. Wyprofilowana świadomość na temat niebezpieczeństw w sieci degraduje się, przez co występujące tam zjawiska, również te niepożądane, stają się normalnością zyskując wymiar uniwersalny. Uznać można, że przemoc to oddziaływanie na umysł o charakterze bezpośrednim lub pośrednim pozbawione możliwości kontroli. Zjawisko cybermanipulacji same w sobie jest przemocą, ponieważ doprowadza zmanipulowaną ofiarę do dezaprobowanych przez nią rezultatów. Łącząc się z innymi elementami, tworzy daleko idące, innowacyjne formy przemocy w cyberprzestrzeni[13].

Sytuacje międzynarodowe są wykorzystywane do manipulowania ludźmi poszukującymi szczegółowych i aktualnych informacji. W relacjach na temat inwazji ujawnia się nie tylko koszmar wojny, ale także zjawisko *fake newsów.* Działania te skupiają się na atakach również w państwach, które nie są zaangażowane w konflikt[14]. Analitycy konkludują, że rozpoczęta wojna wcale nie zainicjowała dezinformacji, ponieważ ta trwała już od dawna, choć w różnym stopniu i sile można było ją dostrzec. Aktualnym okazało się powiedzenie polityka Hirama Johnsona – „*Pierwszą ofiarą wojny jest prawda*"[15]. Wraz z intensyfikacją inwazji Rosji na Ukrainę coraz częściej pojawiają się głosy o realnym zagrożeniu cyberwojną. Polska, która szczególnie włączyła się w pomoc zaatakowanym sąsiadom stała się punktem docelowym w cyberwojnie mocarstwa rosyjskiego z Zachodem. Tuż po wystąpieniu konfliktu zbrojnego rosyjscy

[13] R. Borkowski, Cywilizacja, technika, ekologia: wybrane problemy rozwoju cywilizacyjnego u progu XXI wieku, AGH, Kraków 2001, s. 13.

[14] Wojna w Ukrainie. SBU: rosyjski atak hakerski na ukraińskie portale informacyjne, https://www.polsa tnews.pl/wiadomosc/2022-03-17/wojna-w-ukrainie-sbu-rosyjski-atak-hakerski-na-ukrainskie-portaleinformacyjne/, (dostęp: 26.11.2022 r.).

[15] Wojna otwiera nam oczy na dezinformację, https://technologia.dziennik.pl/internet/artykuly/8393380,dezinformacja-wojna-ukraina-rosja.html (26.11.2022).

hakerzy dokonali wielu prób ataku na polskie serwery, na rządowe skrzynki mailowe trafiło przeszło 30 tysięcy fałszywych i złośliwych wiadomości[16]. Prezydent Stanów Zjednoczonych, Joe Biden poinformował wówczas, że kraje zachodnie są gotowe na natychmiastową reakcję w przypadku wystąpienia jakiegokolwiek z ataków na infrastrukturę krytyczną. Specjaliści szykowali się na wystąpienie prawdziwego Cyber Pearl Harbor, czyli ofensywy, która szczególnie może zagrażać amerykańskiej infrastrukturze cybernetycznej oraz powiązanym z nią usługom informatycznym[17]. Teoretycy, obserwując działania zbrojne, stwierdzili jednak, że cyberwojna nie przekracza granic i nie wymaga odpowiedzi. Państwa trzecie starają się jednak rozbudowywać wiedzę swoich obywateli w zakresie właściwości i autentyczności dostępnych informacji. Eksperci dostrzegli, iż agresor Ukrainy skupił się głównie na inwestowaniu zasobów w zaplanowane akcje dezinformacyjne aniżeli jawne hakerskie natarcia. Spadło poczucie bezpieczeństwa nie tylko w dotkniętym kraju wojną, ale również w innych państwach.

Oceny polskich internautów na temat bezpiecznego surfowania w sieci są podzielone. Pojawia się pytanie, czy w ogóle można mówić o braku zagrożeń w tej sferze. Biorąc pod uwagę całościowy proces wymiany informacji, przesyłania ich oraz udostępniania danych przeważa jednak przekonanie, że Internet nie jest bezpieczną płaszczyzną komunikowania się. Deliberując nad cechami dotyczącej aktualnej sytuacji w Polsce, która stała się krajem sąsiednim państwa, na terenie którego toczy się wojna, tj. Ukrainy, należy podkreślić, że polskie społeczeństwo doświadczyło dezinformacji, m.in. przy pomocy *fake news'ów*. Zjawisko dezinformacji to także wytwór nieuwagi. Jednostka ma niepohamowaną skłonność do udostępniania informacji wyrwanych z kontekstu. Zdarzało się również, że media powielały niesprawdzone treści, co mogło w pewnym stopniu fałszywie

[16] Zagrożenia w cyberprzestrzeni – czy Polsce grozi cyberwojna? https://nano.komputronik.pl/n/cyberwojna-cyberterroryzm-wojna-cybernetyczna/, (dostęp: 26.11.2022 r.).

[17] Stop waiting for a "cyber Pearl Harbor", https://qz.com/2044945/the-threat-of-a-cyber-pearl-harboris-a-red-herring/, (dostęp: 26.11.2022 r.).

autoryzować przekonania osób, które zapoznały się już z fragmentem komunikatu. Na ogół społeczność trafiała na przykłady dezinformacji w aspekcie agresji rosyjsko-ukraińskiej, którymi są: publikowanie treści nieprawdziwych, które sami zweryfikowali czy publikowanie informacji z wielu kont, bez podania swoich danych. Rzadziej jednak doświadczali incydentów, przejawiających się agresją wobec Polaków, którzy angażują się w pomoc swoim sąsiadom. To samo tyczy się też próby wywołania agresji wobec Ukraińców broniących swojej ojczyzny oraz uciekających przed wojną do Polski. Działania hakerów rosyjskich stały się realnym zagrożeniem nie tylko dla pokoju w Ukrainie, ale również dla polskiej cyberprzestrzeni.

Wiele mówi się o wolności słowa, która odnosi się do wolności wyrażanych poglądów, pozyskiwania i rozpowszechniania informacji[18]. Po wybuchu wojny, w Internecie wraz z informacjami zaczęły się pojawiać również grafiki z instrukcją jak nie dać oszukać się przy pomocy *fake news'ow*. Jednak aby z nimi walczyć, najpierw należy poznać ich specyfikę oraz kategoryzację. Nieprawdziwe informacje można rozpatrywać w kategoriach:

– Mal information, czyli wykorzystywaniu i upowszechnianiu informacji w celu wyrządzenia szkody. Taką szkodą może być szeroko i względnie rozumiana krzywda. Przykładem mogą być treści korespondencji ujawnione ze względu na konflikt między konkurentami z partii politycznych. Zazwyczaj ujawnia się fragment wiadomości, która bezsprzecznie stawia jedną stronę w złym świetle;
– Misinformation, czyli błędne informacje udostępniane w sieci nie mające w zamiarze złego przekazu. Bywa to często połączenie nieadekwatnej fotografii do treści[19];
– Bezsprzecznie nieprawdziwa informacja, stosowana w celu dokonania rozbudowanej manipulacji na jednostce;

[18] Europejska Konwencja Praw Człowieka, art. 9 i 10.

[19] How to identify misinformation, disinformation, and malinformation/ https://cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-it-sap00300 /, (dostęp: 26.11.2022 r.).

– Fałszywa informacja z elementem satyry. Komentarze na forach społecznościowych używane w celach humorystycznych;
– Sporna informacja, rozumiana jako nadająca innego znaczenia treść;
– Manipulacja cytatem, polegająca na użyciu czyjejś idei w komunikacie w celu przekształcenia pierwotnego przekazu;
– Clickbait, czyli złożone z kliknięcia (click) oraz tzw. przynęty (bait) pojęcie, mające za cel zdobycie jak największej liczby wyświetleń przez chwytliwe nagłówki, zdjęcia[20].

Wyróżnia się też trzy obszary, na których może wystąpić spór informacyjny. Pierwszy z nich to obszar osobisty, (z ang. *personal information warfare*), drugi stanowi obszar korporacyjny (*corporate information warfare*), a trzeci obszar to globalny (*global information warfare*)[21]. Wieloaspektowość walki informacyjnej złożona jest przede wszystkim z uniwersalności dostosowania się do różnorakich założeń oraz motywów. Przekracza ona standardowy obszar poczynań, a uczestnicy walki nie muszą być powiązani tylko ze zbrojnymi siłami. Wszelkie procesy takie jak zdobywanie informacji, zakłócanie ich udostępniania czy ewentualna ochrona tych danych odbywała się praktycznie zawsze, lecz jako powiązane nie nazywały się wojną informacyjną[22].

Mimo iż dezinformacyjne doniesienia powiązane z wojną ustały, to ostatnia sytuacja z 15 listopada 2022 roku, która miała miejsce w przygranicznym z Ukrainą Przewodowie stała się siłą sprawczą do tworzenia kolejnych teorii o charakterze spiskowym. Załączane zdjęcia budziły w ludziach strach i panikę, nie było oficjalnych informacji i przez wiele godzin sytuacja ta nie została potwierdzona. Przedstawiciele rządu apelowali

[20] Fake newsy w życiu codziennym – jak nie dać się oszukać? https://kulturalnemedia.pl/lifestyle/fake-newsy-w-zyciu-codziennym-jak-nie-dac-sie-oszukac/, (dostęp: 26.11.2022 r.).

[21] A. Mróz- Jagiełło, P. Majdan, Komunikowanie w cyberprzestrzeni, Ekonomiczne Problemy Usług nr 2/2018 (131), t. 2., s. 269.

[22] A. Mróz- Jagiełło, P. Majdan, Komunikowanie…op.cit., s.269.

o rozwagę w poszukiwaniu informacji na temat tragedii. Dopiero następnego dnia pojawiły się potwierdzone informacje. Społeczność przez ten czas była poddawana wielu już atakom dezinformacyjnym.

Przeciwdziałanie dezinformacji

W Polsce, jak i na świecie nieprzerwanie debatuje się nad wpływem technologii na życie każdego człowieka, zarówno młodego, w średnim wieku czy starszego. Wraz z rozwojem najnowszych środków i narzędzi komunikacyjnych rośnie również liczba negatywnych zjawisk. Wszelkie praktyki wykorzystywane w celu ochrony informacji nabierają nowego wymiaru, ponieważ progresyjna aktywność w sieci powoduje tym samym ryzyko przekształcenia udostępnianych danych bądź utraty kontroli nad nimi[23]. Jeszcze przed wybuchem wojny u naszych sąsiadów, specjaliści CERT Polska [24] w roku 2021 zarejestrowali gigantyczny wzrost cyberataków w kraju – w stosunku do roku 2020 różnica wynosi aż 182%[25]. Badania te odsłaniają niebezpieczeństwo i powagę problemu w digitalowym świecie. Kluczowa jest edukacja i wdrożenie odpowiednich programów mających na celu przeciwdziałanie zagrożeniu. Racjonalne zapobieganie, jak również skutecznie wdrażana bezpieczna działalność komunikacyjna to fundamentalne elementy w strategii cyberbezpieczeństwa. Osiągnięcie bezpieczeństwa w cyberprzestrzeni wymaga nieprzerwanego monitorowania wszystkich zmian, przekształceń oraz efektów w zakresie metod, form i technik użytkowanych przez wirtualnych przestępców. Niewątpliwie, wybuch wojny w Ukrainie przyczynił się do wzmożonej aktywności w sieci. Konflikt ten stał się punktem zainteresowań prasy, radia, telewizji, a zwłaszcza Internetu – razem

[23] Raport Polacy w Cyberprzestrzeni- czy jesteśmy świadomi cyberataków? – Procontent Communication- SW Research-, Warszawa 2022, s.2.

[24] CERT - Computer Emergency Response Team- zespół reagowania na incydenty bezpieczeństwa komputerowego, działa w strukturach NASK – Panstwowego Instytutu Badawczego.

[25] Ibidem, s.2.

z wieloma komunikatami pojawiały się również te dezinformacyjne. Jednak problem zjawiska dezinformacji był obecny dużo wcześniej, to właśnie po 24 lutym 2022 roku przeciwdziałanie stało się wyzwaniem zarówno dla Polski, jak i Europy, ale również dla organizacji i instytucji międzynarodowych. Równolegle z działaniami za naszą wschodnią granicą, NASK PIB, czyli Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy[26] mający na celu zapewnienie bezpieczeństwa Internetu, stworzył profile na portalach społecznościowych o nazwie #WłączWeryfikację. Celem tych profili oraz zamieszczanych tam informacji jest przede wszystkim dementowanie nieprawdziwych treści. Specjaliści odpowiedzialni za prowadzenie profilu stawiają również na edukację społeczeństwa. Wskazują przede wszystkim na przejawy działań dezinformacyjnych, szkodliwość *fake news'ów*, budowę nieprawdziwej informacji, generalizację stereotypów czy kulturę komunikacji w mediach społecznościowych. Aktualnie profil „Włącz Weryfikację – NASK" na portalu społecznościowym Facebook, ma ponad 10 tys. obserwujących[27]. To jedno z wielu podjętych działań przez NASK zasługujące na kluczową uwagę w zwalczaniu dezinformacji w social mediach. Na arenie międzynarodowej również podjęto kroki w celu zmniejszenia masowo pojawiających się *fake news'ów.* W czerwcu 2022 roku, Komisja Europejska przedstawiła zaktualizowaną i udoskonaloną wersję kodeksu postępowania w zakresie zwalczania dezinformacji. Pierwotna wersja weszła w życie w 2018 roku, a jej działalność skupiała się między innymi w identyfikacji fałszywych kont i botów na portalach społecznościowych czy kontroli algorytmów. Założeniem głównym było i dalej jest tworzenie odpowiednich zabezpieczeń przed dezinformacją. W 2020 roku Komisja Europejska przedstawiła ocenę, która zakładała, iż

[26] NASK PIB - Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy nad którym nadzór sprawuje Kancelaria Prezesa Rady Ministrów. Działalność skupia się na zwiększeniu efektywności i bezpieczeństwa Internetu, prowadzi rejestr domen internetowych.

[27] #STOPdezinformacji #WŁĄCZWeryfikację https://www.nask.pl/pl/wlaczweryfikacje/wlaczweryfikacje/4413,WlaczWeryfikacje.html (dostęp: 29.12.2022 r).

kodeks jest praktycznym narzędziem zwiększającym transparentność założeń platform internetowych w walce ze zjawiskiem dezinformacji. Jednak ukazano pewne nieprawidłowości w stosowaniu zobowiązań kodeksu przez serwisy internetowe, a także brak odpowiedniego mechanizmu kontroli i dostępu w stosunku do nich. Rewolucję przynosi nowy kodeks, który zniwelował słabości pierwotnej wersji oraz dodał zestaw zobowiązań i środków ograniczających platformy w sieci względem czerpania korzyści z emitowania reklam. W zaktualizowanym kodeksie w zakresie zwalczania dezinformacji zwrócono kluczową uwagę na ochronę użytkowników umożliwiając dostęp do sprawdzonych źródeł oraz do materiałów edukacyjnych na temat świadomego korzystania ze środków medialnych. Przeznaczono również środki oraz umożliwiono dostęp do danych kanałów dla naukowców w celu prowadzenia przez nich zintensyfikowanych badań w zakresie zjawiska dezinformacji[28]. W świetle zagrożenia przybywa coraz więcej projektów mających na celu zniwelowanie zjawiska, zarówno krajowych, jak i międzynarodowych. Priorytetem jest zapewnienie bezpieczeństwa Internetu – skupiska użytkowników całego świata, a także ich życia.

Podsumowanie

Doświadczenie cyberprzemocą, bo tak można nazwać wszelkie manipulacje, propagandę oraz działania dezinformacyjne, zdecydowanie wpływają na poczucie bezpieczeństwa osobistego człowieka. Ma ono wpływ nie tylko na postrzeganie zagrożeń cyberprzemocą w znaczeniu indywidualnym, zbiorowym, jak i globalnym. Stan bezpieczeństwa jest stanem wolności bez ryzyka pojawienia się negatywnych zagrożeń z zewnątrz. Niestety, nie ma stanu bezpieczeństwa, który byłby na tyle silny, by żadne niepożądane elementy nie przedostały się i go nie

[28] Nowy Kodeks Postępowania w zakresie zwalczania dezinformacji https://cyberpolicy.nask.pl/nowy-kodeks-postepowania-w-zakresie-zwalczania-dezinformacji/ (dostęp: 29.12.2022 r.).

zakłóciły. Wszelkie zagrożenia mogą występować w każdej sferze, zarówno rzeczywistej jak i online. Sytuacja pandemiczna sprawiła, że większość ludzi aktywnie spędzała czas w sieci, korzystając z niej w różnych miejscach. Doświadczenie dezinformujących działań spowodowało obniżenie poczucia bezpieczeństwa wśród społeczeństwa. Sieci wirtualne są sieciami społecznymi, co pozwala na pokonanie wszelkich dystansów. Internet pozwala na łączenie się zbiorowości i podtrzymywanie więzi. Świat online postrzegany jest również jako bardzo atrakcyjny obszar w którym symulowane są pewne czynności, zdarzenia czy reakcje. Postęp technologiczny, a wraz z nim postęp komunikacyjny to ogromna szansa rozwoju dla ludzkości. Warto wiedzieć, że proces komunikacji w cyberprzestrzeni, poza oczywistymi atutami, takimi jak permanentna dostępność czy łatwość nawiązywana kontaktu, wymiany poglądów czy pozyskiwania informacji i wiedzy, buduje również coraz więcej barier, które w konsekwencji pociągają za sobą wiele niepożądanych zjawisk o znamionach cyberprzemocy (np. manipulacja, propaganda). Podkreśla się jak istotne jest budowanie świadomości społecznej oraz nieustanna edukacja w zakresie korzystania z dobra jakim jest Internet oraz na temat zagrożeń, jakie za sobą te „dobro" niesie. W tym obszarze zagrożenia rozwijają się intensywnie i stanowią dla globalnego świata nie lada wyzwanie. Komunikacja w cyberprzestrzeni zdecydowanie wpływa na bezpieczeństwo państwa jako społeczeństwa, a wszelkie nieodpowiednie metody komunikowania się są zagrożeniem dla państw trzecich. W odniesieniu do wojny w Ukrainie zauważono jak szeroki jest przekrój wszelkich środków wywierania wpływu. Pole manewru do manipulowania społeczeństwem rośnie wraz z każdą udostępnioną informacją, a proces globalizacji umożliwił błyskawiczny obieg wszelkich treści.

Bibliografia

Literatura:

Borkowski R., Cywilizacja, technika, ekologia: wybrane problemy rozwoju cywilizacyjnego u progu XXI wieku, AGH, Kraków 2001.

Fraczek M., Zagrożenia w cyberprzestrzeni dla Polski i krajów Unii Europejskiej, Materiał opracowany na II Ogólnopolski Kongres Politologii, UAM Poznań 2012.

Janowski J., Cybermanipulacja jako samodzielna forma i stały składnik przemocy informacyjnej w cyberprzestrzeni [w:] Cyberprzemoc szczególnym zagrożeniem społeczeństwa informacyjnego, M. Kowalewski, M. Jakubiak (red.), Oficyna Wyd. Politechniki Warszawskiej, Warszawa 2021.

Jarmoszko S., Kalita C., Maciejewski J., Nauki społeczne wobec problemu bezpieczeństwa (wybrane zagadnienia), [w:] S. Jarmoszko, Teoretyczne konceptualizacje i sensy bezpieczeństwa w naukach społecznych, Uniwersytet Przyrodniczo-Humanistyczny, Siedlce 2016.

Korzeniowski L.F., Podstawy nauk o bezpieczeństwie, Difin, Warszawa 2012.

Mróz-Jagiełło A., Majdan P., Komunikowanie w cyberprzestrzeni, Ekonomiczne Problemy Usług nr 2/2018 (131), t. 2.

Spitzer M., Cyfrowa demencja, Wyd. Dobra Literatura, Warszawa 2020.

Szewior K., Bezpieczeństwo społeczne jednostki. Założenia i polska rzeczywistość, Wyd. UW, Warszawa 2016.

Wasiuta O., Wasiuta S., Wojna informacyjna zagrożeniem dla bezpieczeństwa ludzkości, Kraków 2017.

Waligórska-Kotfas A., Bezpieczeństwo w Internecie jako wyzwanie społeczeństwa informacyjnego [w:] Wybrane problemy i wyzwania bezpieczeństwa. Bezpieczeństwo jednostkowe – Bezpieczeństwo zbiorowe. Ujęcie interdyscyplinarne, K. Zawieja-Żurowska (red.), Wydawnictwo PWSZ w Koninie, Konin 2015.

Wilk A. M., , Państwo w dobie społeczeństwa informacyjnego - perspektywa strategicznych zmian, w: Internet 2000. Prawo - ekonomia - kultura, red. R. Skubisz, Lublin 2000.

Zięba R., Bezpieczeństwo międzynarodowe po zimnej wojnie, WAiP, Warszawa 2008.

Inne:

Wojna w Ukrainie. SBU: rosyjski atak hakerski na ukraińskie portale informacyjne, https://www.polsa tnews.pl/wiadomosc/2022-03-17/wojna-w-ukrainie-sbu-rosyjski-atak-hakerski-na-ukrainskie-portaleinformacyjne (dostęp: 26.11.2022).

Wojna otwiera nam oczy na dezinformację, https://technologia.dziennik.pl/internet/artykuly/8393380,dezinformacja-wojna-ukraina-rosja.html (dostęp: 26.11.2022).

Zagrożenia w cyberprzestrzeni – czy Polsce grozi cyberwojna? https://nano.komputronik.pl/n/cyberwojna-cyberterroryzm-wojna-cybernetyczna/ (dostęp: 26.11.2022).

Stop waiting for a "cyber Pearl Harbor", https://qz.com/2044945/the-threat-of-a-cyber-pearl-harboris-a-red-herring/ (dostęp: 26.11.2022).

How to identify misinformation, disinformation, and malinformation/ https://cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-itsap00300 / (dostęp: 26.11.2022).

Fake newsy w życiu codziennym – jak nie dać się oszukać? https://kulturalnemedia.pl/lifestyle/fake-newsy-w-zyciu-codziennym-jak-nie-dac-sie-oszukac/ (dostęp: 26.11.2022).

Raport Polacy w Cyberprzestrzeni- czy jesteśmy świadomi cyberataków? – Procontent Communication- SW Research.

STOPdezinformacji #WŁĄCZWeryfikację, https://www.nask.pl/pl/wlaczweryfikacje/wlaczweryfikacje/4413,WlaczWeryfikacje.html/ (dostęp: 29.12.2022).

Nowy Kodeks Postępowania w zakresie zwalczania dezinformacji https://cyberpolicy.nask.pl/nowy-kodeks-postepowania-w-zakresie-zwalczania-dezinformacji/ (dostęp: 29.12.2022).