WSTĘP

Rozwój technologiczny postępuje tak szybko, że nasze społeczeństwo z trudem przystosowuje się do rzeczywistości, którą tworzy nowe środowisko informacyjne. Nowe relacje między państwami, organizacjami i osobami, a także nowe sposoby prowadzenia walki zacierają granicę między wojną a pokojem. Dziś łatwiej i potencjalnie taniej można przełamać opór wroga, stosując ukierunkowane ataki cybernetyczne i informacyjne, niż używając siły militarnej. Społeczeństwu i rządom zaś większą szkodę mogą przynieść zorganizowane trollingowanie w sieciach społecznościowych, manipulacyjne programy telewizyjne, zhackowana korespondencja e-mailowa i atak cybernetyczny na systemy bankowe niż konwencjonalny wojskowy atak na dużą skalę.

Wzrost znaczenia informacji na przełomie XX i XXI w. spowodował, że bezpieczeństwo informacyjne stało się priorytetową dziedziną bezpieczeństwa narodowego. Konkurencja w jej zdobywaniu i gromadzeniu wzmogła konieczność jej ochrony oraz doprowadziła do walki o zasoby. Co za tym idzie, wraz z rosnącym jej przepływem w cyberprzestrzeni problematyka bezpieczeństwa informacyjnego nabrała wymiaru globalnego. Obecnie w różnych aspektach zajmują się nią m.in. agencje Unii Europejskiej oraz poszczególne sektory organizacji międzynarodowych. Poszczególne państwa zaś prowadzą politykę bezpieczeństwa

informacyjnego ukierunkowaną na ochronę istniejących systemów informacyjnych, zapewnienie bezpieczeństwa infrastruktury krytycznej oraz podmiotów prywatnych, narażonych na zagrożenia m.in. cyberatakiem i rozprzestrzenianiem szkodliwego oprogramowania. Rosnące zagrożenie atakami hakerów we wszystkich obszarach funkcjonowania społeczeństwa jasno pokazuje, że tylko wspólna i ogólnoeuropejska, a może ogólnodemokratyczna, strategia może zagwarantować nasze cyberbezpieczeństwo. Istota operacji cybernetycznych polega bowiem na tym, że nie uznają one żadnych granic terytorialnych. Decyzje mogą zapadać w Moskwie, Pekinie czy Phenianie, natomiast same operacje czy działania cybernetyczne mogą wykorzystywać sieci informatyczne zlokalizowane w dowolnym miejscu na świecie.

XXI w. przyniósł nowe formy agresji międzynarodowej, powiązane z ewolucją i rozbudową światowej sieci elektronicznej – internetu. Nowa kategoria zagrożeń dla bezpieczeństwa państwa – związanych m.in. z rozwojem e-administracji, sterowanych komputerowo elektrowni, systemów obsługi lotów i lotnisk oraz ogromną popularnością bankowości internetowej – została zintegrowana z już istniejącą definicją wojny internetowej, traktowanej jako działania podjęte w celu zakłócania komunikacji przeciwnika i podania mu fałszywego obrazu rzeczywistości[1]. Początek drugiego tysiąclecia nadał jednak temu terminowi zupełnie nowe znaczenie, o znacznie szerszym i bardziej zróżnicowanym niż kiedykolwiek wcześniej zakresie[2].

Obecne stulecie to także czas pojawienia się nowego zjawiska – bałaganu informacyjnego. Wszechobecność technologii z dostępem do internetu przynosi znaczne korzyści, ale również niesie za sobą poważne zagrożenia – nie tylko dla naszej gospodarki i bezpieczeństwa, ale i dla naszego zaufania do systemów komputerowych. Cyberataki i zakłócanie dostępu do sieci podważają wiarę w rząd i zaufanie publiczne do instytucji

1 D. Delibasis, *The Right to National Self-defence: In Information Warfare Operations*, Bury St Edmunds, Arena 2007, s. 25.

2 J. Kulesza, J. Kulesza, *Odpowiedzialność państw za podejmowane w cyberprzestrzeni działania zagrażające międzynarodowemu pokojowi i bezpieczeństwu*, „Studia Prawno-Ekonomiczne" 2011, t. LXXXIII (83); C. Biancotti, R. Cristadoro, *Koszty cyber(nie)bezpieczeństwa*, 6.02.2018, ObserwatorFinansowy.pl (dostęp 15.04.2019).

demokratycznych. Corocznie coraz więcej wydarzeń wskazuje na to, że przestrzeń informacyjna jest wypełniona dezinformacją, propagandą i sygnałami manipulacyjnymi. Względnie nowe zjawisko, jakim jest fake news, rozprzestrzenia się w internecie z zawrotną prędkością, ale ma już swojego godnego następcę – wideo typu *deepfake*, które może stać się nową strategią wykorzystywaną w marketingu politycznym.

Dziś fake newsy to informacje i artykuły oparte na przeinaczeniach, nieprawdzie i nadinterpretacjach, a większość z nich dotyczy sceny politycznej – polityków, partii, a także postulatów i programów wyborczych. Informacje takie sprawiają wrażenie zweryfikowanych i rzetelnych, niejednokrotnie pojawia się w nich źródło wiadomości mające poświadczać ich autentyczność. W istocie jednak wprowadzają odbiorców w błąd i rozlewają się w sieci w nieustraszonym tempie. Powstaje chaos informacyjny, a polityk, który padł ofiarą fake newsa, traci w sondażach, podczas gdy zyskuje jego rywal ze sceny politycznej, który być może jest również autorem spreparowanej informacji.

Nie miałoby to żadnego wpływu na życie społeczne, gdyby fałszywe wiadomości były jedynie globalnym żartem. W rzeczywistości istnieje jednak strategia o wymiarze finansowym, mająca na celu pielęgnowanie wątpliwości, wyrabianie alternatywnych prawd, zmuszanie ludzi do myślenia, że to, co mówią politycy i media, zawsze jest w większym lub mniejszym stopniu kłamstwem. Ciężar dowodu został odwrócony: podczas gdy dziennikarze muszą nieustannie udowadniać, że to, co mówią lub piszą zgodnie z etyką zawodu, jest prawdą, ci, którzy szerzą fałszywe wiadomości, krzyczą: „To ty ponosisz odpowiedzialność za to, że się mylimy!".

O wiele większa swoboda informacji w erze cyfrowej może być celem arbitralnej władzy politycznej. Może być również instrumentem służącym do manipulacji przez różne podmioty, w tym mocarstwa. Wybory z ostatnich 2 lat w różnych państwach Zachodu dostrzegły szerzące się fałszywe wiadomości i hacking mające na celu zakłócenie porządku publicznego, zagrażające szczerości sondażu wyborczego, a tym samym tworzące zamieszanie, wątpliwości i niezgodę. Jest to atak na samą suwerenność wybranych państw, który wykorzystuje pasywne podejście platform do tego niedopuszczalnego zjawiska – bierności, która graniczy z nieodpowiedzialnością.

Powodowani cyniczną wizją przestrzeni cyfrowej, sprawcy tych manewrów starają się odwrócić zasady, na których opierają się te demokracje – otwartość, wolność informacji i komunikacji – aby uczynić je instrumentami interferencji i destabilizacji. To nowa era propagandy – dezinformacja nie jest oczywiście zjawiskiem nowym, ale cyfrowa rewolucja i jej wpływ na to, w jaki sposób społeczeństwo, a zwłaszcza młodzi ludzie, przekazuje swoje wiadomości, zapewnia jej niespotykany dotąd zakres oddziaływania. Ta ingerencja musi zostać powstrzymana poprzez połączenie działań władz publicznych, odpowiedzialności korporacyjnej i czujności ze strony społeczeństwa obywatelskiego i mediów.

Wraz z rozpowszechnieniem się komputerów liczba wyrafinowanych wirusów nieustannie rośnie, co stwarza nowe zagrożenia dla bezpieczeństwa. Jak podkreśla prof. W. Gogołek, „pojawiają się nowe kategorie wirusów. Są to m.in. wirusy polimorficzne, które potrafią samodzielnie zmieniać swój kod, a w rezultacie powstaje trudniejsza do wykrycia mutacja ich postaci, czy retrowirusy, które atakują programy antywirusowe”[3]. O ile agresję wojskową, presję ekonomiczną i przerwy w dostawie gazu można od razu zakwalifikować jako wrogie działania innego państwa, o tyle wykryć propagandę informacyjną jest znacznie trudniej. Broń informacyjna jest niewidzialna, podobna do promieniowania, a ludność nawet nie czuje, że pada ofiarą jej działania[4].

Przykładem wojny informacyjnej jest nasilająca się geopolityczna konfrontacja między Rosją i USA. Doprowadziła ona do tego, że w 2019 r. Kongres Stanów Zjednoczonych zaproponował wydzielenie 280 mld dol. na walkę z zagrożeniami hybrydowymi, w tym z dezinformacją. Działania wojskowe na terytorium Ukrainy, jak podkreślają O. i S. Wasiutowie, są jednym z jej etapów[5]. Jak twierdzi brytyjski dziennikarz P. Pomerantsev w swoim badaniu rosyjskiej przestrzeni medialnej dla „Guardiana”, Rosja, nie mogąc dogonić USA w uzbrojeniu wojskowym, postanowiła zwyciężyć

3 W. Gogołek, *Informatyka dla humanistów*, Wydawnictwo Kropki Trzy, Warszawa 2012, s. 206.

4 P. Pomerantsev, *Inside the Kremlin's Hall of Mirrors*, 9.04.2015, TheGuardian.com (dostęp 11.04.2019).

5 O. Wasiuta, S. Wasiuta, *Wojna hybrydowa Rosji przeciwko Ukrainie*, Wydawnictwo Arcana, Kraków 2017.

wroga „asymetrycznymi sposobami”[6], kontrolując świadomość społeczeństwa. Takie podejście jest charakterystyczne dla kierunku krytycznej geopolityki. Już J. Agnew i G.Ó. Tuathail pisali o tym, że w epoce globalizacji wróg nie znajduje się poza granicami państwa, lecz jest zintegrowany z jego społeczeństwem[7].

Wojna informacyjna zawsze działa dwukierunkowo. Z jednej strony odwołuje się do narodu, który ją prowadzi – potencjalnych bojowników – by podnosić morale, mobilizować i wzniecać nienawiść do wroga. Z drugiej jej celem jest demoralizacja oponenta. Choć już w starożytności specjalnie wykorzystywano do tego proroków i poetów – elementy wojny informacyjnej można znaleźć m.in. u Homera, który opisuje mobilizację Greków do wojny z Trają i rolę poetów w tej konfrontacji – długo nie osiągnęła ona współczesnego poziomu. Obecne konflikty mają zupełnie inne cechy – to wojny o świadomość, w których główny cios wymierzony jest w tożsamość ludzi, a wpływ informacji ma na celu podważenie ich przyzwyczajeń. W dzisiejszym społeczeństwie informacyjnym zarządzanie ludzką tożsamością staje się przedmiotem zainteresowania sztabów generalnych armii, służb specjalnych i największych sieci wywiadowczych.

Mimo że propaganda informacyjna zawsze zajmowała ważne miejsce w polityce wewnętrznej i zewnętrznej, w wieku informacyjnym nabiera ona nowego znaczenia. W wyniku rozwoju nowych technologii, które przyspieszyły rozprzestrzenianie się procesów globalizacyjnych i przyczyniły się do powstania jednej przestrzeni informacyjnej, wojny informacyjne stały się jedną z najbardziej skutecznych metod osiągnięcia celu. Wykorzystanie tych ostatnich jako środka konfrontacji geopolitycznej można śledzić na przykładzie wojen w Zatoce Perskiej, Czeczenii, na wschodzie Ukrainy, na Krymie i w Syrii. Badanie tego zjawiska w celu ochrony własnej przestrzeni informacyjnej i własnych pozycji w przestrzeni globalnej nabiera więc szczególnie istotnego znaczenia.

Bezpieczeństwo informacji polega na analizie zagrożeń, które mogą się pojawić w sferze informacyjnej, i stworzeniu warunków, które zapobiegną

6 P. Pomerantsev, *Inside the Kremlin's Hall of Mirrors*, dz. cyt.

7 J. Agnew, G.Ó. Tuathail, *Geopolitics and discourse: Practical Geopolitical Reasoning in American Foreign Policy*, „Political Geography”, March 1992, vol. 11, no. 2.

ich wystąpieniu. Dotyczy to przede wszystkim aspektów technicznych przekazywania i przetwarzania informacji. Dlatego też Unia Europejska przyjęła wiele dokumentów dotyczących tego zagadnienia, jak również współpracują w tej dziedzinie członkowie NATO. Istnieje także kilka światowych i europejskich centrów walki z dezinformacją, manipulowaniem wiadomościami i cyberbezpieczeństwem. Są to:

- Centrum Doskonalenia Obrony przed Cyberatakami (Cooperative Cyber Defense Center of Excellence, CCDCOE) z siedzibą w Tallinie pełni funkcję think tanku Paktu Północnoatlantyckiego, a jego główne zadanie stanowi prowadzenie interdyscyplinarnych badań nad cyberbezpieczeństwem oraz przeprowadzanie ćwiczeń oraz szkoleń edukacyjnych i doskonalących w tym obszarze. Jego misją jest rozwój zdolności obronnych, współpracy i wymiany informacji między członkami Sojuszu i jego partnerami w dziedzinie bezpieczeństwa cybernetycznego.
- Światowa Komisja ds. Stabilności w Cyberprzestrzeni (Global Commission on the Stability of Cyberspace) zajmuje się opracowywaniem pakietu propozycji norm i zaleceń zmierzających do zapewnienia międzynarodowego bezpieczeństwa, stabilności i przewidywalnych działań w cyberprzestrzeni, zarówno ze strony państw, jak i podmiotów komercyjnych. Jej zadaniem jest przygotowanie zestawu propozycji norm i polityk na rzecz wzmocnienia międzynarodowego bezpieczeństwa, stabilności i odpowiedzialnych zachowań w cyberprzestrzeni ze strony aktorów państwowych i niepaństwowych.
- Międzynarodowa Organizacja Atrybucji Cyberataków to nowy element cyberobrony, służący do poprawy transparentności działań w sieci ułatwiającej społeczności międzynarodowej podejmowanie właściwych działań wobec nieprzestrzegających zasad i prawa. Organizacja ta ma identyfikować pośredników, którzy są angażowani przez zainteresowane państwa do ataku na inne kraje.
- Europejska Agencja Bezpieczeństwa Sieci i Informacji (European Network and Information Security Agency) jest centrum eksperckim w dziedzinie bezpieczeństwa cybernetycznego w Europie z siedzibą w Grecji. Jej celem jest zapewnienie wysokiego poziomu

bezpieczeństwa sieci i informacji w UE, a także rozwijanie i promowanie kultury bezpieczeństwa sieci i informacji w społeczeństwie z korzyścią dla obywateli, konsumentów, przedsiębiorstw i organizacji społecznych w Europie.

- Centrum Eksperckie NATO ds. Komunikacji Strategicznej (NATO Strategic Communication Centre of Excellence, NATO StratCom COE) ma za zadanie nie tylko walkę z cyberatakami, działaniami propagandowymi i dezinformacją, ale również dbanie o komunikację strategiczną między członkami Sojuszu.
- Centrum Analiz Propagandy i Dezinformacji w Polsce ma za zadanie wzmacnianie struktur społeczeństwa obywatelskiego zarówno w Polsce, jak i w państwach sojuszniczych obszaru transatlantyckiego. Na szczególną uwagę zasługuje ogólnopolski projekt zainicjowany przez centrum w lutym 2019 r. dzięki wsparciu National Endowment for Democracy – „Zwiększanie zdolności polskiego społeczeństwa w zakresie przeciwdziałania dezinformacji".

Oprócz tego w różnych państwach UE powstają ruchy i grupy internetowych wolontariuszy na rzecz przeciwdziałania rosyjskim trollom, wypełniającym przestrzeń informacyjną teoriami spiskowymi. Bałtyckie elfy codziennie dążą do demaskowania rosyjskiej propagandy. Prowadzą dochodzenia, starają się dokładnie badać trolle, fałszywe konta i całe kampanie dezinformacyjne, inicjują też własne działania, wykorzystując dobre emocje i humor, dzięki którym starają się rozpowszechniać pozytywne historie. W Ukrainie, gdzie wojna informacyjna i cyberataki ze strony Federacji Rosyjskiej trwają już ponad 5 lat, opracowywana jest koncepcja polityki informacyjnej państwa, a także bezpieczeństwa informacji.

Na oddzielną uwagę zasługują w nowym społeczeństwie informacyjnym media. Początkowo dostępne jedynie dla elit, najbogatszych i najlepiej wykształconych, stanowiły one nieliczący się element systemu społecznego. Z czasem słusznie zaczęto mówić, że są czwartą władzą – obok ustawodawczej, wykonawczej i sądowniczej. Obecnie stały się one nie tyle władzą pierwszą, ile autonomiczną, niezależną od polityki, biznesu, a często nawet technologii, siłą, która w szerokim zakresie wpływa na nasze życie. Tę nową prawidłowość trafnie opisywała do niedawna koncepcja mediatyzacji – procesu intensyfikacji obecności mediów w naszym

życiu[8]. Wraz z pojawieniem się nowych mediów i wzrostem znaczenia internetu stopień złożoności tego procesu znacznie się jednak zwiększył. Stwierdzenie, że polityka – podobnie jak muchę – najłatwiej zabić gazetą, nabiera obecnie szerszego znaczenia. Dziś bowiem kampanię wyborczą można wygrać wpisem na Facebooku lub tweetem, a wojnę prowadzić za pomocą odpowiednio przygotowanej kampanii medialnej.

Nie można zapominać o znanych dotychczas próbach wyjaśniania i rozumienia mediów jako głównego źródła informacji, które wpływa na procesy polityczne, w tym wyborcze, a też na zjawiska w obszarze gospodarki, kultury i edukacji. Informacje, tak jak i przedtem, tworzą w umysłach odbiorców mapę świata, oddzielając to, co ważne, od tego, co mniej istotne, porządkują świat i go hierarchizują. Poza tworzeniem agendy naszej wiedzy o świecie pozwalają także odbiorcom zrozumieć rzeczywistość poprzez jej upraszczanie oraz nadawanie określonych ram wielowymiarowym zjawiskom i procesom. Wreszcie – mają ogromny wpływ na wybór treści, którymi będą oni zajmować swoją uwagę.

Uwarunkowania ekonomiczne, polityczne, gry interesów i wpływów od dziesięcioleci determinowały dobór problematyki, którą odbiorcy mieli się interesować za sprawą jej obecności w mediach, oraz tematyki pomijanej lub stanowiącej medialne tabu. Te opisane już prawidłowości nabrały specyficznego znaczenia i kolorytu w dobie nowych mediów[9]. Media nie tylko straciły swój dotychczasowy analogowy charakter, który wymagał obecności przed odbiornikiem czy dysponowania egzemplarzem gazety. Internet umożliwia również dostęp zawsze i wszędzie, a także daje możliwość interakcji na niespotykaną dotąd skalę. Obecnie podział na nadawców i odbiorców ma charakter czysto formalny, gdyż ich role da się w każdej chwili odwrócić – niemal każdy użytkownik mediów może raz odbierać, a raz nadawać informacje, co całkowicie zmieniło procesy weryfikacji wiadomości. Ich tworzenie i udostępnianie przestało

8 R. Klepka, *Analiza zawartości mediów: dlaczego i do czego można ją wykorzystać w nauce o bezpieczeństwie i politologii?*, „Annales Universitatis Paedagogicae Cracoviensis Studia de Securitate et Educatione Civili" 2016, t. VI, nr 224, s. 33–35.

9 H. Batorowska, O. Wasiuta, R. Klepka, *Media jako instrument wpływu informacyjnego i manipulacji społeczeństwem*, Wydawnictwo Libron, Kraków 2019, s. 129–137.

być domeną dziennikarzy, od których oczekiwano dotąd przestrzegania kodeksu etycznego. Obecnie każdy może być autorem treści medialnych, a ich zasięg zależny jest tylko od siły ich promowania w sieci oraz zainteresowania odbiorców.

Nowe media, których naturalnym centrum pozostaje internet, a w szczególności media społecznościowe, poza wieloma możliwościami niosą za sobą nowe zagrożenia dla bezpieczeństwa informacyjnego. Korzystanie z nich wiąże się z mniej czytelnymi mechanizmami dostępu do określonych treści. Odbiorcy niezwykle trudno poznać algorytmy, które sprawiły, że trafił na daną stronę internetową, zapoznał się z konkretnym tweetem czy wpisem na Facebooku. Bańki filtrujące, komory echa i brak pewności co do tego, kto i dlaczego chciał, abyśmy otrzymali określoną informację – gdyż coraz trudniej wierzyć w to, że została ona odnaleziona przez użytkownika przypadkowo, a nie w wyniku działania algorytmów… Nowe zagrożenia informacyjne związane z mediami to możliwości wykorzystania starych narzędzi, takich jak cenzura, propaganda czy manipulacja, na niespotykane dotąd sposoby i nieznaną skalę.

Mając na uwadze złożony, wielowymiarowy świat bezpieczeństwa informacyjnego, oddajemy do rąk Czytelników *Vademecum bezpieczeństwa informacyjnego* będące efektem pracy naukowców zatrudnionych w Instytucie Nauk o Bezpieczeństwie Uniwersytetu Pedagogicznego im. KEN w Krakowie oraz Współpracowników Instytutu. Naszym celem było stworzenie specjalistycznego opracowania, które spełniałoby funkcję praktycznego kompendium wiedzy z różnych zakresów współczesnego bezpieczeństwa informacyjnego i uwzględniającego najnowsze fakty i tendencje.

Vademecum bezpieczeństwa informacyjnego ma pomóc Czytelnikom i wszystkim zainteresowanym proponowaną problematyką zapoznać się z szeroko rozumianymi zagadnieniami z zakresu bezpieczeństwa informacyjnego. W pracy przeanalizowano specjalistyczną terminologię, która zarówno pojawia się w dyskursie naukowym, wśród specjalistów w dziedzinie bezpieczeństwa informacyjnego, jak i stanowi przedmiot dyskusji potocznych, nierzadko opartych jedynie na domysłach czy odczuciach. Głównym celem publikacji jest dokładne wyjaśnienie terminów i pojęć z zakresu bezpieczeństwa informacyjnego. Zawiera ona analizę ponad 250 terminów, które traktowane są jako najważniejsze w literaturze

naukowej i publikacjach edukacyjnych, a także tych wywołujących największe kontrowersje czy wątpliwości.

Mamy wielką nadzieję, że zaproponowane Czytelnikom vademecum zajmie swoje miejsce w dyskusji naukowej na temat sposobu określania i kluczowych problemów odnoszących się do wybranych kategorii ważnych z perspektywy nauk o bezpieczeństwie, będzie uzupełniać już znajdujące się w obiegu naukowym lub dotychczas nieopisane, nowe obszary bezpieczeństwa informacyjnego, odzwierciedlać odmienne wizje i tematy o różnym stopniu ważności, aktualności i zróżnicowanym zakresie. Autorzy mają nadzieję, że praca okaże się przydatna dla każdego, kto zechce opanować najnowszą wiedzę i terminologię naukową z zakresu bezpieczeństwa informacyjnego – zarówno dla tych, którzy na co dzień zajmują się nim edukacyjnie, praktycznie i zawodowo, jak i dla szerokiego grona Czytelników.

W podobnym gronie autorskim, związanym z Instytutem Nauk o Bezpieczeństwie Uniwersytetu Pedagogicznego w Krakowie, powstało rok wcześniej *Vademecum bezpieczeństwa*, które spotkało się z życzliwym przyjęciem i ze strony środowiska naukowego, i studentów. Mamy wielką nadzieję, że podobnie stanie się z niniejszą publikacją. Liczymy więc na konstruktywne wnioski od Czytelników, które pozwolą nam w przyszłości poszerzyć, uzupełnić i udoskonalić obecną wersję *Vademecum bezpieczeństwa informacyjnego*.

Olga Wasiuta, Rafał Klepka