doi 10.26343/0585556X11605 STUDIA SOCJOLOGICZNO-POLITYCZNE. SERIA NOWA
NR 1(16)/2022 ■ ISSN 0585-556X

Piotr Śledź
Uniwersytet Warszawski
Wydział Nauk Politycznych i Studiów Międzynarodowych
Katedra Studiów Strategicznych i Bezpieczeństwa Międzynarodowego[1]
ORCID: 0000-0003-4562-7491

DEZINFORMACJA W STOSUNKACH MIĘDZYNARODOWYCH W WARUNKACH CZWARTEJ REWOLUCJI PRZEMYSŁOWEJ

■ WSTĘP

Druga połowa XX wieku, w szczególności zaś jego ostatnie dekady, to okres niezwykle intensywnego rozwoju technologii informacyjnych, którego efektem było zwłaszcza upowszechnienie się komputerów i sieci Internet. Zasięg ich oddziaływania obejmował z czasem coraz więcej obszarów ludzkiej aktywności, co spowodowało ukształtowanie się nowego modelu stosunków społecznych w ramach tzw. społeczeństwa informacyjnego, w którym informacja jest już nie tylko nośnikiem treści, ale też towarem samym w sobie, umożliwiającym tworzenie i powiększanie wartości w gospodarce (Goban-Klas, Sienkiewicz 1999: 43). Zmiany te zaczęto jeszcze w latach osiemdziesiątych określać mianem trzeciej rewolucji przemysłowej (zob. np. Finkelstein, Newman 1984: 53–58; Helfgott 1986: 43). W XXI wieku tempo tych przemian nie ustało – przeciwnie, zdobycze trzeciej rewolucji przemysłowej zdynamizowały wręcz jeszcze rozwój technologiczny. Skala procesu oraz zasięg wywołanych w ten sposób wieloaspektowych przewartościowań sprawiły, że zaczęto go traktować jako zupełnie nowy etap rozwoju, określając mianem „drugiej ery maszyn" (Brynjolfsson, McAfee 2014: 7–11) czy „przemysłu 4.0" (Lasi i in. 2014: 239–242). Na bazie tego drugiego określenia ukuto termin „czwartej rewolucji przemysłowej".

Jego głównym propagatorem jest niemiecki ekonomista, koordynator Światowego Forum Ekonomicznego w Davos (którego edycja w 2016 roku odbyła się właśnie pod takim hasłem), Klaus Schwab. Dowodzi on, że o wyjątkowości współczesnych przemian stanowią trzy czynniki: ich szybkość (rozwój wykładniczy, nie linearny jak wcześniej), zasięg i głębokość (rozpościerających się ze sfery

[1] E-mail: piotr.sledz@uw.edu.pl

technologicznej na całokształt procesów gospodarczych, biznesowych, społecznych i na poziomie jednostki) oraz ich wpływ na funkcjonowanie różnorakich systemów (Schwab 2016: 8 i 9). Stwierdza, że granicę między trzecią a czwartą rewolucją przemysłową wyznacza przejście „od prostej cyfryzacji […] do dużo bardziej złożonych form innowacji wynikających z coraz to nowych połączeń między rozmaitymi technologiami" (ibidem: 53, tłum. własne). Chodzi przede wszystkim o systemy zdolne integrować wymiar cyfrowy z fizycznym i biologicznym, do których zaliczyć można m.in. platformy wielostronne wykorzystujące chmurę obliczeniową, technologie sztucznej inteligencji (AI) i uczenia maszynowego (*machine learning*), tzw. Internet Rzeczy, mikroukłady elektromechaniczne, bioczujniki, roboty, technologie wirtualnej i rozszerzonej rzeczywistości, druk trójwymiarowy i tzw. produkcję przyrostową, komputery kwantowe, nanotechnologie, biochipy oraz technologię *blockchain* (Skilton, Hovsepian 2018: 32–55). Ich zastosowanie już spowodowało bądź posiada istotny potencjał, by stało się tak w przyszłości, istotne przeobrażenia w sferze gospodarczej (m.in. nowe formy wytwarzania dochodu, zmiany w strukturze rynku pracy i naturze jej świadczenia), biznesie (w tym organizacji i współpracy przedsiębiorstw czy oczekiwań konsumentów), na poziomie państw (sprawowania władzy i realizacji usług publicznych), w stosunkach międzynarodowych (nowe wyzwania i zagrożenia bezpieczeństwa międzynarodowego), jak również dla funkcjonowania społeczeństw i jednostek (ich życia prywatnego i zawodowego).

Pośród wielu przemian Klaus Schwab (2016: 66 i 67, 88–90) dostrzega również te na poziomie relacji państwo–obywatel. Zakłada, że nowe środowisko informacyjne może przyczynić się do poprawy jakości rządzenia, gdyż lepiej poinformowana i bardziej świadoma (a przez to wymagająca) opinia publiczna wymusi większą transparentność władz, możliwości ich rozliczenia oraz angażowanie obywateli w procesy decyzyjne. Zagrożeń w tym zakresie – szerokich możliwości wykorzystania nowych mediów do wrogiej propagandy, promowania ekstremistycznego przekazu czy rekrutowania nowych zwolenników – upatruje raczej po stronie aktorów pozapaństwowych, w szczególności organizacji terrorystycznych. O zasadności tych argumentów świadczyły m.in. rola mediów społecznościowych w mobilizowaniu uczestników protestów w trakcie wydarzeń „arabskiej wiosny" (zob. Sawicka 2017: 130–135, 157–160) czy działalność tzw. Państwa Islamskiego, wykorzystującego je do rekrutacji nowych członków i sympatyków, a także obniżania poczucia bezpieczeństwa i wywoływania chaosu w uważanych za wrogie państwach, np. poprzez dezinformację, w tym zapowiedzi umieszczania bojowników tej organizacji pośród migrantów i uchodźców próbujących dostać się do Europy w trakcie kryzysu migracyjnego w 2015 roku (Szakács, Bognár 2021: 11; McDonald-Gibson 2015). Długofalowe skutki tego procesu okazały się jednak skrajnie odmienne. Część państw nauczyła się wykorzystywać te narzędzia do realizacji własnych interesów, również na arenie międzynarodowej – szczególnie przez różne formy dezinformowania.

Mówiąc o dezinformacji, stwierdzić należy, że jej istota sprowadza się do świadomego i zamierzonego wprowadzenia odbiorców w błąd, aby dzięki zmanipulowaniu ich percepcji ułatwić sobie realizację określonego celu. W przypadku wykorzystywania tego typu technik przez państwo na użytek zewnętrzny chodzi przede wszystkim o cele polityki zagranicznej. Możliwe jest wyróżnienie dwóch podstawowych typów dezinformacji w stosunkach międzynarodowych – bezpośredniego i pośredniego. Odrębną kategorią pozostaje dezinformacja prowadzona w warunkach wojennych, jako jedna z przestrzeni konfliktu, będąca jego immanentną właściwością. Dezinformacja bezpośrednia obejmuje rozpowszechnianie sfałszowanego lub zniekształconego, często propagandowego przekazu dotyczącego spraw związanych z realizacją polityki państwa będącego „nadawcą". Dezinformacja pośrednia (określana też mianem „psychicznej intoksykacji" – zob. Nord 1999: 63–67)[2] odnosi się zaś do propagowania treści obliczonych na wywołanie pośród opinii publicznej – w państwie lub państwach będących celem – określonych postaw i odczuć (najczęściej dezorientacji), które mogą przyczynić się do podjęcia działań korzystnych z punktu widzenia podmiotu inicjującego, na zasadzie *cui bono*. Podział ten pozostaje stosowny także w odniesieniu do współczesnego środowiska informacyjnego.

Wykorzystanie dezinformacji do realizacji celów polityki ma niezwykle długą historię, sięgającą starożytności – by przywołać choćby opowieść o koniu trojańskim w *Odysei* (Homer 2014: 83) czy dyrektywy formułowane przez Sun Tzu (2007: 24–27). Choć niniejsze opracowanie nie jest studium historycznym i szczegółowa rekonstrukcja genezy stosowania dezinformacji nie należy do jego celów, podkreślić trzeba jej szerokie wykorzystywanie w XX wieku, zwłaszcza przez Rosję/ZSRR, nazistowskie Niemcy i USA (zob. Posetti, Matthews 2018: 3 i 4). Jednak dopiero współcześnie pośród obywateli i decydentów politycznych upowszechniło się jej postrzeganie jako żywotnego zagrożenia bezpieczeństwa narodowego i międzynarodowego. Przełomową cezurą pozostaje w tym zakresie rok 2016 w związku z rosyjskimi próbami wywierania wpływu na wyniki referendum o członkostwie Wielkiej Brytanii w Unii Europejskiej oraz wyborów prezydenta Stanów Zjednoczonych przez wykorzystanie specyficznych środków tego rodzaju.

Sprawiło to również, że tematyka ta stała się przedmiotem licznych studiów. Choć można wskazać na wcześniejsze opracowania tego rodzaju (np. Debord 1990: 44–62; Volkoff 1999: 5–17), druga połowa drugiej dekady XXI wieku przyniosła znaczące wzmożenie badań w obszarze dezinformacji jako narzędzia konfrontacji w stosunkach międzynarodowych. Dotyczyły one m.in. konceptualizacji samego zjawiska (np. Gerrits 2018: 4–8; Lanoszka 2019: 229-240; O'Shaughnessy 2020: 57–67; Neo 2021: 215–221), umiejscowienia tego zagadnienia w obrębie teorii stosunków międzynarodowych (la Cour 2020: 708–711), jego znaczenia

[2] Pierre Nord tłumaczy jej istotę jako „informowanie nieprzyjaciela przez nas samych w taki sposób, w jaki powinien on być poinformowany, żeby działać na własną zgubę".

w kontekście działań hybrydowych (np. Wigell 2019: 266–268), zwalczania tego rodzaju zagrożeń (np. Haigh M., Haigh T. 2020: 313–318; Humprecht, Esser, Van Aelst 2020: 499–502) czy statusu prawnomiędzynarodowego (Baade 2018: 1362–1375; Rotondo, Salvati 2019: 210–217). Uwzględnić należy też liczne opracowania eksperckie o nieco bardziej praktycznym zabarwieniu (np. autorstwa analityków RAND oraz ryskiego Centrum Doskonałości NATO w zakresie komunikacji strategicznej czy helsińskiego na rzecz zwalczania zagrożeń hybrydowych) i studia przypadków. W polskiej literaturze przedmiotu rzeczony wątek pojawia się z kolei głównie w kontekście rosyjskiej dezinformacji (np. Darczewska 2014: 9–36, 2019: 8–14; Wojnowski 2015: 11–36; Pogorzelski 2017: 10–28; Marek 2020: 56–134; Legucka 2020: 162–182), informacyjnego wymiaru wojny hybrydowej Rosji przeciw Ukrainie (np. Wasiuta O., Wasiuta S. 2017: 162–253; Pacek 2017: 199–215; Banasik 2018: 88–99, 2021: 49–65; Wrzosek, Markiewicz, Modrzejewski 2018: 87–127) czy bezpieczeństwa informacyjnego *par excellence* (Grabowski 2018: 9–32; Modrzejewski 2018: 91–117; Aleksandrowicz 2021: 15–81).

Zadaniem niniejszego artykułu jest ukazanie wpływu zachodzących współcześnie przemian technologicznych i ich społecznych implikacji na możliwości stosowania dezinformacji w stosunkach międzynarodowych i jej skuteczność – wskazanie najważniejszych związków przyczynowo-skutkowych pomiędzy rozwojem technologii a skalą tego zjawiska. Robocza teza zakłada, że czwarta rewolucja przemysłowa stworzyła instrumentarium i okoliczności umożliwiające państwom wykorzystanie narzędzi dezinformacji na nieznaną wcześniej skalę, z uwagi na właściwości współczesnego środowiska informacyjnego opartego o jej zdobycze. Odpowiedzi na pytanie o te cechy posłuży pierwsza część niniejszego tekstu. W dalszej kolejności zaprezentowane zostaną taktyki dezinformacyjne, których zastosowanie na szeroką skalę umożliwiają rzeczone okoliczności. Kolejne pytanie badawcze, do którego odnosi się niniejszy artykuł, dotyczy państw wykorzystujących nowe instrumentarium dezinformacji do realizacji swoich celów. Dokonana zostanie ich identyfikacja, podobnie jak kluczowych towarzyszących temu motywacji oraz czynników sprzyjających. Ostatnia część artykułu poświęcona będzie odpowiedzi na pytanie o istniejące oraz potencjalne mechanizmy obronne w tym zakresie, a także związane z nimi ograniczenia.

CECHY WSPÓŁCZESNEGO ŚRODOWISKA INFORMACYJNEGO SPRZYJAJĄCE DEZINFORMACJI

Manuel Castells (2007: 20, 336 i 337) w swojej fundamentalnej publikacji *Społeczeństwo sieci* pisał o ukształtowaniu się pod koniec XX wieku nowego modelu komunikacyjnego o zasięgu ogólnoświatowym – a dzięki Internetowi zintegrowanego z mediami innego rodzaju, wykorzystującego możliwości stworzone przez rewolucję cyfrową – który przyczynił się do powstania nowego typu stosunków

zarówno w wymiarze gospodarczym, jak i społeczno-kulturowym. Proces ten stanowił swoiste uwieńczenie trwającej od lat osiemdziesiątych „customizacji" (personalizacji) przestrzeni informacyjnej – dostosowywania jej treści do oczekiwań odbiorcy dysponującego niezliczenie wieloma opcjami do wyboru, z jednoczesnym ograniczeniem znaczenia mediów *stricte* masowych. Z czasem to sam konsument stał się producentem treści – masowy dostęp do Internetu znacząco osłabił znaczenie tzw. gatekeeperów. Chodzi o, jak wyjaśnia Ian Greenleigh (2014: 10 i 11), wszelkie osoby władne spowolnić, zatrzymać lub przyspieszyć komuś dostęp do czegoś – w tym wypadku chodzi o informacje. Z reguły są to redakcje i wszelkie instytucje kontrolujące przestrzeń medialną.

O ile już upowszechnienie globalnej sieci internetowej samo w sobie znacząco ograniczyło wpływ gatekeeperów na środowisko informacyjne, to rozwój technologiczny w pierwszych dwóch dekadach XXI wieku – zwłaszcza zaś powstanie i umasowienie mediów społecznościowych – niemalże unieważnił ich dotychczasową rolę. Obecnie wspomniana „customizacja" przestrzeni medialnej ma charakter całościowy. Odbiorca posiada pełną moc decyzyjną w zakresie selekcji treści dostarczanej mu przez tego rodzaju portale internetowe czy platformy multimedialne (YouTube, Netflix, Amazon Prime, Spotify i wiele innych – często działające w modelu subskrypcyjnym, gdzie klient płaci za możliwość dostępu do treści „na żądanie"), a współcześni gatekeeperzy (inne osoby lub stosowne algorytmy sugerujące) mogą tylko zachęcać go do zapoznania się z jakąś konkretną treścią, rywalizując o jego uwagę, co stwarza przestrzeń do innych nadużyć.

W zasadzie wszystkie media internetowe, poza renomowanymi i rzetelnymi portalami, mogą zostać wykorzystane jako platforma dezinformacji, skoro zabezpieczenie w postaci gatekeeperów w tym wypadku znika, a gdy adresat treści może być jednocześnie ich twórcą, dochodzi do skrajnej dezagregacji przekazu (nieskończenie wielu zarówno autorów, jak i odbiorców), który w dodatku staje się niczym niezapośredniczony. Mowa w szczególności o mediach społecznościowych, ale również forach, blogosferach czy wszelkiego rodzaju portalach internetowych o niskiej wiarygodności, wykorzystujących tzw. *junk news*, czyli sprymitywizowany, niezweryfikowany (często bazujący na plotkach i półprawdach) i *stricte* sensacyjny przekaz, obliczony wyłącznie na wzbudzenie zainteresowania odbiorcy oraz generowanie ruchu sieciowego (zob. Venturini 2019: 126–137). Zjawisko to tłumaczy w kontekście rosyjskiej dezinformacji czołowy jej tropiciel w polskiej przestrzeni informacyjnej, Marcin Rey:

> […] każdy z nas stara się pisać takie rzeczy, by inni się zainteresowali i szerowali [udostępniali, upowszechniali daną treść – przyp. P.Ś.]. Rosjanie w działalności dezinformacyjnej wymierzonej w Zachód wykorzystują zasady rynkowe. Produkują treści i starają się nimi zainteresować ludzi na Zachodzie […]. Idea jest taka, aby rosyjski przekaz był rozpowszechniany spontanicznie (za: Gądek 2022).

Możliwości technologiczne, a więc funkcjonowanie tego rodzaju platform, umożliwiły niemalże nieograniczoną „produkcję" informacji. Ich ogrom przyczynia się do zaistnienia zjawiska „szumu informacyjnego" (Goban-Klas, Sienkiewicz 1999: 112 i 113) czy „przeciążenia informacjami" (*information overload*, zob. Mandel 2019: 5–8, 15–21) – nadmiaru treści docierających do odbiorcy, uniemożliwiającego właściwe zrozumienie i zinterpretowanie rzeczywistości. Wielu aktorów (od jednostek, przez liczne podmioty subpaństwowe i transnarodowe, po państwa) nauczyło się wykorzystywać tę okoliczność do realizacji własnych celów. W tym sensie możemy zaobserwować swego rodzaju powrót do clausewitzowskiej „mgły", choć tym razem *à rebours* – wynikającej nie z braku informacji (temu odpór dał rozwój stosownych technologii), ale z ich nadmiaru. Okoliczność ta sama w sobie ułatwia stosowanie dezinformacji, zwłaszcza narracji obliczonych na dalsze pogłębianie chaosu i zasiewanie wątpliwości u odbiorców. Jest też praprzyczyną wielu z opisywanych poniżej zjawisk związanych z zabieganiem o uwagę użytkownika, kryteriami selekcji przez niego informacji oraz działalności stworzonych do tego algorytmów (Tessier 2020: 27 i 28).

Media społecznościowe stanowią szczególną kategorię kanałów dystrybucji, umożliwiając prowadzenie działań dezinformacyjnych na nieporównywalnie szerszą niż kiedykolwiek skalę – dość powiedzieć, że liczbę ich użytkowników szacuje się na 4,5 mld osób (najwięcej Facebook – ponad 2,9 mld), co równałoby się ok. 57% całej populacji świata (Ang 2021)[3] – oraz skierowanie tego przekazu bezpośrednio do odbiorców (a często, dzięki *big data* i stosownym algorytmom służącym microtargetingowi, czyli dostosowywaniu przekazu na podstawie metadanych do indywidualnego użytkownika sieci, bardzo dokładnie wyprofilowanych i „namierzonych"). Oprócz skali ważnymi czynnikami sprawczymi są pewne specyficzne cechy mediów społecznościowych. Przede wszystkim zupełnie inna niż dotychczas jest rola odbiorcy, który dzięki ich interaktywnemu charakterowi staje się podmiotem przestrzeni informacyjnej (co implikuje jego o wiele większe zaangażowanie w porównaniu do mediów tradycyjnych, także z uwagi na element wartościujący, jakim są wszelkiego rodzaju polubienia czy też „lajki" bądź udostępnienia danej treści) – nie tylko adresatem, ale także twórcą, na którym spoczywa też niemal pełna odpowiedzialność za selekcję przyswajanych treści. Ostatnia z wymienionych okoliczności sprzyja, co ważne, wystąpieniu zjawiska „komory echo" (*echo chamber*) czy też „bańki informacyjnej" (*filter buble*) – powstania na podstawie wcześniejszych poglądów uczestniczących osób zamkniętego, jednolitego ideowo obiegu informacji (Dooley, Moore, Averin 2018: 39 i 40). Inne ważne w tym kontekście cechy mediów społecznościowych to m.in. 1) łatwa dostępność (co się tyczy urządzeń mobilnych z dostępem do Internetu – zawsze, wszędzie i wręcz od ręki), 2) szybkość obiegu informacji, 3) ogromna liczba treści

[3] Liczbę wszystkich użytkowników Internetu szacuje się na ponad 5,2 mld osób (stan na kwiecień 2022 roku), a więc ok. 2/3 populacji świata (Internet Live Stats 2022).

przekazywanych każdego dnia (sprzyjająca „szumowi informacyjnemu"), 4) możliwość zachowania anonimowości przez użytkowników, 5) brak jakichkolwiek ograniczeń przestrzennych oraz dotyczących treści przekazu (np. ekstremistycznej) (NATO StratCom CoE 2016: 5 i 6).

Bardzo istotną okoliczność w przypadku dezinformacji z wykorzystaniem przedmiotowego instrumentarium, gdy przekaz ten nie jest dystrybuowany oficjalnymi kanałami państwowymi, stanowi ponadto trudność w przypisaniu winy sprawcy, a zarazem – możliwość odcięcia się od prowadzonych w ten sposób działań ze strony ich faktycznych inicjatorów (*plausible deniability*), zwłaszcza gdy są nimi państwa. Jest to właściwość konfrontacji w cyberprzestrzeni *par excellence* (zob. Madej 2007: 333 i 334), ale w przypadku dezinformacji efekt ten jest bodaj jeszcze silniejszy. Przekaz może wpisywać się w narracje krajowych stronnictw politycznych i mediów lub być pochodną działalności obcych służb specjalnych w zakresie dezinformacji pośredniej. Niemożność rozróżnienia pomiędzy działaniami tego rodzaju inicjowanymi bezpośrednio przez rządy, powiązane z nimi pośrednio grupy, podmioty zewnętrzne czy też działające z „inspiracji" lub niezależnie różnorakie ugrupowania funkcjonujące w państwie będącym przedmiotem takiej presji pogłębia dodatkowo wspomniany chaos informacyjny i w ogromnym stopniu utrudnia zwalczanie dezinformacji.

Mimo dostrzegalnego trendu automatyzacji praktyk dezinformacyjnych – zwłaszcza w kontekście stosowania botów, a więc oprogramowania komputerowego umożliwiającego udostępnianie określonych treści i zautomatyzowane interakcje z użytkownikami sieci, w sposób imitujący ich zachowania, w oparciu o stosowny algorytm; oraz zbiorów *big data* i programów służących ich wykorzystaniu w celach dezinformacji, w tym selekcji potencjalnie „chłonnych" odbiorców i dostosowaniu przekazu na bazie tych informacji w ramach microtargetingu – kluczowy we wszystkich ich wymiarach pozostaje czynnik ludzki. W przestrzeni internetowej szczególną rolę odgrywają trolle, a więc użytkownicy odpowiedzialni za powielanie określonego przekazu na różnorakich portalach (zwłaszcza społecznościowych). Jessikka Aro (2020: 17 i 18) w swoim reportażu opisującym wykorzystanie powiązanych z rosyjskimi służbami specjalnymi trolli do „zabezpieczenia interesów Federacji Rosyjskiej w przestrzeni informacyjnej" wskazuje, że „trolle […] udawały prawdziwe osoby o wyrobionych poglądach, prowadziły fałszywe profile, uaktualniały je i zapełniały Internet pochwałami prezydenta Władimira Putina oraz krytyką rosyjskiej opozycji i Stanów Zjednoczonych". Osoby takie mogą być opłacone bądź działać z przyczyn ideologicznych lub antyspołecznych[4].

Do powyższych wyzwań wynikających z właściwości współczesnego środowiska informacyjnego dodać należy także te dotyczące roli podmiotów prywatnych

[4] Warto dodać, że zanim pojęcia „trolli" i „trollingu" zaczęto odnosić do działalności zorganizowanych grup wpływu, oznaczały przede wszystkim zachowania w przestrzeni internetowej o charakterze zwodniczym, destrukcyjnym lub zakłócającym różnego rodzaju aktywności innych użytkowników (zob. Kurowska, Reshetnikov 2018: 348).

– kierujących się logiką zysków, co dotyczy zwłaszcza największych korporacji sektora IT. Czyni to ich relację z podmiotami zainteresowanymi rozpowszechnianiem dezinformacji na swój sposób symbiotyczną. Sprzyja temu natura współczesnego rynku medialnego, a zwłaszcza ciągłe dążenie do poszerzania kręgu odbiorców (użytkowników), m.in. poprzez promowanie uproszczonego i sensacyjnego, a nierzadko radykalnego i polaryzującego przekazu przez te media, co niezwykle ułatwia dezinformowanie. Trudno w tych okolicznościach uznać portale społecznościowe jedynie za instrument, a nie aktywnych uczestników tych procesów – dość przypomnieć sprzedaż przez Facebooka prywatnych danych prawie 90 mln użytkowników firmie Cambridge Analytica zajmującej się prowadzeniem kampanii wyborczych z wykorzystaniem *big data* (m.in. na rzecz Donalda Trumpa czy zwolenników brexitu w 2016 roku), co Mark Zuckerberg przyznał, zeznając w 2018 roku przed Kongresem USA[5]. Platformom tym zależy na generowaniu jak największego ruchu sieciowego, czemu taki przekaz niewątpliwie sprzyja. Może być to pochodną polityki redakcyjnej (obliczonej na tzw. *clickbait*, a więc generowanie ruchu sieciowego w postaci „kliknięć", do których skłaniać mają krzykliwe czy wyzywająco brzmiące tytuły) lub działania zmechanizowanego algorytmu, co ma miejsce szczególnie w przypadku mediów społecznościowych (w taki sposób – domyślnie promujący sensacyjny i zazwyczaj negatywny przekaz w celu dotarcia do maksymalnie szerokiego audytorium – działa np. pozycjonowanie treści na Facebooku; zob. Merrill, Oremus 2021; Tiffany 2021). Polaryzacja i radykalizacja opłacają się więc nie tylko politykom, ale również właścicielom mediów internetowych. Przekaz służący dezinformowaniu znajduje tu zatem żyzne podłoże. Schemat ten przedstawia Marcin Rey:

> algorytmy sieci społecznościowych zauważają ruch wokół tematu, więc promują go […] treść rozklejają już prawdziwi internauci, którzy się zainteresowali, bo temat trafił w ich poglądy. Temat rozchodzi się w jakimś środowisku politycznym. Przenika do mediów z tego obozu, działacze partyjni przejmują go i dezinformacja może dotrzeć do decydentów politycznych (za: Gądek 2022).

Jeszcze inny zbiór wyzwań tworzą te wynikające z dynamicznego rozwoju technologii mogących być wykorzystanymi do manipulacji tego rodzaju. Wspomnieć należy tu w szczególności o algorytmach sztucznej inteligencji, posiłkujących się zwłaszcza zbiorami *big data*, których zastosowań w omawianym obszarze wskazać można co najmniej kilka. Oprócz botów wykorzystujących tego rodzaju mechanizmy, dużym wyzwaniem pozostaje intensywnie rozwijana technologia *deepfake*. Chodzi o generowane na podstawie technologii sztucznej inteligencji i machine learningu hiperrealistyczne materiały multimedialne (wykorzystujące obraz wideo i dźwięk) prezentujące sytuacje, które faktycznie się nie zdarzyły (także na żywo).

[5] Według zeznań jednego z byłych pracowników Cambridge Analytica firma mogła mieć dostęp do danych nawet ok. 230 mln użytkowników tego portalu (Cadwalladr 2018).

Szczególnie istotne jest w tym kontekście generowanie ruchu twarzy konkretnych osób poprzez ich stosowne mapowanie (Wasiuta O., Wasiuta S. 2019: 21). Także syntezowanie mowy osiągnęło już całkiem zaawansowany poziom, czego przykładem kanał „Vocal Synthesis" na Youtube, na którym czołowi współcześni politycy, celebryci i postacie historyczne „czytają" (nierzadko w absurdalnym kontekście) znane teksty kultury. Jednak doniosłości technologii *deepfake* dla dezinformacji międzynarodowej dowiodło wydarzenie z czerwca 2022 roku, gdy kilkoro burmistrzów/prezydentów europejskich miast (w tym Berlina, Madrytu, Wiednia czy Warszawy) odbyło wideorozmowę z deepfake'iem mera Kijowa – Witalija Kliczki (zob. Oltermann 2022). Zjawisko to jawi się jeszcze bardziej niepokojące, gdy uwzględnić rozwój zdolności sztucznej inteligencji do generowania określonej treści. Program Generative Pre-trained Transformer 3 (GPT-3) jest zdolny w szybkim tempie tworzyć teksty na zadany temat, utrzymane w określonym przez użytkownika tonie. Jego zastosowanie wykracza więc daleko poza obszar dezinformacji, niemniej w połączeniu z technologią *deepfake* ten kierunek rozwoju omawianej technologii nabiera dla niego szczególnego znaczenia.

Sztuczna inteligencja ma także nieco bardziej „przyziemne" zastosowania w kontekście internetowej dezinformacji. Posiłkuje się nią różnorakie oprogramowanie służące moderowaniu i pozycjonowaniu treści w Internecie czy formułowaniu rekomendacji w tym zakresie dla użytkownika. Wiele z tych algorytmów zaprogramowano tak, aby, podobnie jak w przypadku wspomnianych już portali społecznościowych, zwiększały one zaangażowanie internautów, przez wzbudzanie ich zainteresowania, stąd m.in. tendencja do powielania i promowania nieprawdziwych lub zmanipulowanych informacji (CFDD 2021: 4–19).

Spośród rozwiązań technologicznych utożsamianych z czwartą rewolucją przemysłową pewien potencjał w zakresie dezinformacji posiadają także technologie rzeczywistości wirtualnej (*virtual reality* – VR) lub rozszerzonej (*augmented reality* – AR). Zagadnienie to wymaga uwagi szczególnie w kontekście planów rozwijania przez korporację Meta (d. Facebook) tzw. metawersum – alternatywnej, cyfrowej rzeczywistości. Badania nad tą tematyką są póki co na bardzo wczesnym etapie – zespół badawczy z Japonii przeprowadził wstępny test podatności odbiorców na fake newsy rozpowszechniane przy użyciu wizji wygenerowanej przez okulary VR (Verhulst i in. 2020: 577 i 578).

GŁÓWNE TAKTYKI DEZINFORMACYJNE W ŚRODOWISKU NOWYCH MEDIÓW

Można byłoby w zasadzie stwierdzić, że w dużej mierze dezinformacja w internetowym środowisku informacyjnym czerpie pełnymi garściami z mechanizmów „klasycznej". Wiele choćby z rosyjskich utrwalonych wzorców znajduje tam zastosowanie, jak m.in. 1) wywołanie zagubienia, skonfundowania przez kreowanie – także

wyimaginowanych – zagrożeń (zarządzanie strachem), 2) przeciążenie przeciwnika ogromną liczbą sprzecznych informacji (wspomniane już zjawisko *information overload*), 3) zidentyfikowanie słabości drugiej strony i rozgrywanie tego faktu przez tworzenie przekonania, że mogą one zostać wykorzystane przeciwko niej, 4) wprowadzenie przeciwnika w błąd, tak aby podjął niekorzystną ze swojej perspektywy decyzję lub sprowokowanie realizacji przezeń polityki korzystnej z perspektywy państwa dezinformującego, 5) wywołanie podziałów przez generowanie i umacnianie antagonizmu państwa-adresata w stosunku do jego sojuszników, 6) rozpowszechnianie informacji, które są szkodliwe wobec adresata ze względów prawnych, moralnych lub ideologicznych bądź dyskredytują jego rząd w oczach społeczeństwa (za: Thomas 2004: 248–249). Specyfika internetowej przestrzeni informacyjnej wymusza jednak nieco inne od tradycyjnego podejście, stwarzając przy tym jednocześnie szanse bardziej efektywnego jej wykorzystania do realizacji promowanej w ten sposób agendy.

Przede wszystkim dezinformacja w sieci adresowana jest *a priori* do indywidualnego odbiorcy. Paradoksalnie, jak stanowią wyniki jednego z badań ilościowych, to ludzie, nie algorytmy, częściej wykazują tendencję do udostępniania fałszywych informacji (Vosoughi, Roy, Aral 2018: 1150). Wynika to z immanentnych ludzkich błędów poznawczych, takich jak np. efekt potwierdzenia (skłonność do przyjmowania za wiarygodne informacji bliskich przekonaniom danej osoby, stąd m.in. zjawisko „bańki informacyjnej"), dychotomia myślenia (podejście zero-jedynkowe, unikające wyważenia – ważne w kontekście polaryzacji), efekt pierwszeństwa (zależność polegająca na tym, że informacja na dany temat, która dotrze do odbiorców jako pierwsza, w największym stopniu determinuje ich percepcję w odniesieniu do tej kwestii; często łączy się również ze zjawiskiem „owczego pędu"), efekt izolacji (tendencja do skupiania uwagi na obiektach wyróżniających się – np. poglądach skrajnych), myślenie życzeniowe, utożsamianie zjawisk korelatywnych z przyczynowo-skutkowymi, efekt jednorodności grupy obcej (sprowadzenie do wspólnego mianownika wszystkich przedstawicieli grupy, np. narodu, której członkiem nie jest odbiorca), skłonność do przedwczesnej generalizacji (gdy liczba dowodów popierających takową jest jeszcze zbyt mała) czy efekt Dunninga-Krugera (inklinacja osób mających fragmentaryczną wiedzę na określony temat do jej przeszacowywania). Katalog możliwych do zastosowania manipulacji jest bardzo szeroki (zob. EUvsDisinfo 2021), a za najpowszechniejsze, co sugeruje, że także najskuteczniejsze i potencjalnie najgroźniejsze spośród nich, uznać można m.in. *cherry picking* (wybieranie i nagłaśnianie tych informacji, spośród wielu na dany temat, które są użyteczne bądź zgodne z czyimiś poglądami), efekt czystej ekspozycji (powtarzanie przekłamanych treści po wielokroć w celu ich utrwalenia w odbiorze społecznym), odwołanie do autorytetu (np. przez instrumentalne traktowanie wiedzy ekspertów czy wręcz ich sfabrykowanie), *whataboutism* (odwrócenie uwagi od meritum problemu przez komunikat stanowiący sofizmat lub fałszywy trop) czy wywołanie

fałszywej symetrii („symetryzm" lub „prawdopośrodkizm" – poszukiwanie nieuzasadnionej równowagi pomiędzy dwoma twierdzeniami, z których jedno jest przekłamane, zmanipulowane lub oparte na fałszywych przesłankach). Dochodzą do tego socjotechniki wykorzystujące m.in. odwołania do określonych emocji odbiorców, przekaz podprogowy czy niedopowiedzenia (zob. Shandra 2020).

W swoim eseju opublikowanym na łamach „The Atlantic" Jonathan Haidt zwraca uwagę na zależność pomiędzy rozwojem narzędzi cyfrowych (zwłaszcza mediów społecznościowych) a rosnącą skalą polaryzacji społecznej w USA, którą uznaje wręcz za postępującą dezintegrację społeczeństwa, zagrażającą przetrwaniu państwa w obecnej formie, z uwagi na coraz niższe zaufanie do jego instytucji i degradację kapitału społecznego, podkreślając przy tym, będącą efektem, podatność na oddziaływanie propagandowego przekazu, zdominowanego przez przedstawicieli skrajnych poglądów w przestrzeni informacyjnej (Haidt 2022). Za taki stan rzeczy odpowiadają przede wszystkim jednolitość obiegu informacji w Internecie (zjawiska „komory echo" i „bańki informacyjnej") oraz promowanie silnie nacechowanego emocjonalnie, sensacyjnego przekazu, skłaniającego odbiorcę do większego zaangażowania (z przyczyn polityczno-ideologicznych lub komercyjnych). Polaryzacja społeczna (w tym polityczna) może być wielowymiarowa i dotyczyć szerokiego zakresu zagadnień, wokół których ogniskują się i z czasem umacniają dwa przeciwstawne dominujące poglądy. Jej manichejska logika każe przyjmować w całości przekaz jednej ze stron konfliktu, argumenty drugiej w pełni odrzucając, także z uwagi na ich z czasem coraz bardziej skrajny, spowodowany konfliktem, charakter, co czyni dialog i poszukiwanie kompromisu nieskutecznymi. Polaryzacja jest okolicznością o tyle trudną do przezwyciężenia, że przynosi wymierne korzyści stronom, które decydują się na jej instrumentalne wykorzystanie, mobilizując zwolenników i eliminując niewpisujące się w jej logikę podmioty (stąd bywa nieraz stosowana w marketingu – nie tylko zresztą politycznym, by wspomnieć tzw. *Cola wars* z lat osiemdziesiątych i dziewięćdziesiątych, tj. napiętą rywalizację rynkową producentów Coca-Coli i Pepsi). Badacze z Uniwersytetu w Aarhus potwierdzili przy pomocy ilościowego studium korelację między silną identyfikacją partyjną a skłonnością do udostępniania fake newsów w mediach społecznościowych, tak aby wzmocnić przekaz preferowanej partii i zaatakować tę drugą (Osmundsen i in. 2021: 1012–1014).

Brak gatekeeperów (a w rezultacie – możliwość stworzenia wrażenia dostępu do wiedzy „niewygodnej" i z tego powodu „ukrywanej" przed opinią publiczną) oraz coraz bardziej skrajny przekaz przyczyniają się ponadto do wzrostu popularności teorii spiskowych. W przypadku dezinformacji kluczowa staje się sama podatność na nie, ponieważ, jak dowiodło studium ilościowe przeprowadzone przez badaczy The Royal Society w związku z teoriami spiskowymi o COVID-19, dotyczy to osób o niskim zaufaniu do instytucji publicznych, mediów i świata nauki, co do zasady skłonnych do wiary w sens spiskowego wyjaśniania świata, bardziej

niż będących zwolennikami jakichś konkretnych teorii (Roozenbeek i in. 2020). Promowanie teorii spiskowych na temat jednego zagadnienia pośrednio zwiększa zatem podatność na odwoływanie się do nich w innych kwestiach. To ważne, gdyż pozostają one istotnym elementem m.in. rosyjskiej propagandy, która próbuje uzasadniać posunięcia polityczne Kremla wobec Ukrainy od 2014 roku w ten sposób, tłumacząc je np. prowokacjami CIA czy reakcją na działania rzekomych ukraińskich neonazistów, przeprowadzających „ludobójstwo" na ludności rosyjskiego pochodzenia (Pomerantsev 2014: 205 i 206).

PAŃSTWA INICJUJĄCE

Choć dezinformację w Internecie wykorzystują również podmioty niepaństwowe, choćby transnarodowe organizacje terrorystyczne, jak tzw. Państwo Islamskie czy Al-Kaida, zasadniczą troską niniejszych rozważań pozostaje aktywność państw. Mimo że cyberprzestrzeń sama w sobie stanowi narzędzie pozwalające wyrównać siły państw i aktorów niepaństwowych, jako że nie ma do niej zastosowania większość czynników decydujących o przewadze państw w świecie materialnym (Madej 2007: 329), praktyka ostatnich lat dowodzi, że to ich działania tego rodzaju w największym stopniu negatywnie wpłynęły na bezpieczeństwo międzynarodowe.

Państwem, z uwagi na które dezinformacja w sieci zaczęła być powszechnie rozpatrywana jako problem o żywotnym znaczeniu dla bezpieczeństwa, jest Rosja. Katalog przykładów tego rodzaju operacji prowadzonych przez Kreml w ostatnich latach jest bardzo szeroki, a najbardziej znane z nich dotyczyły, oprócz związanych z rosyjskimi wojnami (zwłaszcza tej w Ukrainie), takich wydarzeń, jak wybory prezydenckie w USA (2016 i 2020) oraz we Francji (2017), referendum o członkostwie Wielkiej Brytanii w Unii Europejskiej (2016) czy pandemia COVID-19 (od 2020). W prowadzonej przez EastStratCom – jednostkę Europejskiej Służby Działań Zewnętrznych UE do walki z dezinformacją ze Wschodu rodem – bazie znajdowało się ponad 13,5 tys. przykładów treści tego rodzaju (stan na kwiecień 2022 roku), rozpowszechnianych od 2015 roku (EUvsDisinfo 2022).

Dezinformacja przy pomocy sieci społecznościowych stała się jednym z podstawowych sposobów wywierania presji informacyjnej przez Rosję, nad czym pieczę sprawują służby specjalne – FSB, GRU i SWR, ze szczególnym jednak uwzględnieniem wywiadu wojskowego. To z GRU powiązana jest tzw. Agencja Badań Internetu – uznawana za „centralę" rosyjskich trolli i botów zajmujących się politycznymi manipulacjami w sieci (Intelligence Community 2017). Jej właścicielem jest jeden z najbliższych Władimirowi Putinowi oligarchów, uznawany także za szefa Grupy Wagnera, Jewgenij Prigożyn, co dowodzi strategicznej rangi tych działań z punktu widzenia władz Rosji. Często akcje te skoordynowane są z cyberatakami – wykradzione dane publikowane są potem w Internecie (np. na portalu Wikileaks), gdzie ich treść może ponadto (jak stało się z e-mailami z serwerów wspierającego

kandydaturę Emmanuela Macrona w 2017 roku ruchu En Marche!) zostać zmanipulowana zgodnie z pożądanym przekazem politycznym (Hakala, Melnychuk 2021: 27 i 28). Rosja rozwinęła swoje zdolności w tym zakresie w stopniu pozwalającym na realizację szeroko zakrojonych, wielowymiarowych międzynarodowych kampanii dezinformacji. Należy tu wspomnieć przede wszystkim o uruchomionej w 2014 roku operacji „Secondary Infektion" wymierzonej w państwa Europy Zachodniej i Ameryki Północnej, polegającej na promowaniu określonego przekazu politycznego i pogłębianiu chaosu nie tylko wpisami w mediach społecznościowych i na różnorakich forach internetowych, ale także przez tworzenie fałszywych stron internetowych, „przecieki" i publikowanie sfałszowanych dokumentów czy włamania na konta osób publicznych i rozpowszechnianie za ich pomocą zmanipulowanych treści (zob. Nimmo i in. 2020: 43–82). O dość podobny *modus operandi* oparta jest akcja „Ghostwriter" przeciwko Polsce, Niemcom i Litwie, rozpoczęta prawdopodobnie w 2017 roku (Gielewska, Dauksza 2021).

Kolejnym państwem stosującym nowe narzędzia dezinformacyjne dla realizacji swoich strategicznych celów jest Chińska Republika Ludowa. Dotychczasowe tego rodzaju kampanie prowadzone były w szczególności jako wsparcie w konsolidowaniu chińskiej dominacji na obszarze Azji Wschodniej i Pacyfiku w tamtejszej przestrzeni informacyjnej, a ich główny cel stanowiła Republika Chińska na Tajwanie (Harold, Beauchamp-Mustafaga, Hornung 2021: 47–76), choć zdarzały się też takie wymierzone w Australię (Searight 2020) i Japonię (Stewart 2020). Pierwszy przypadek szerokiej skali zaangażowania Chin w działania dezinformacyjne o zasięgu globalnym stanowiły jednak dopiero te podjęte w związku z pandemią COVID-19 (zob. Dubow, Lucas, Morris 2021: 9–12; Matthews, Migacheva, Brown 2021: 27–39).

Gdy mowa o instrumentarium dezinformacji, to Chiny preferują póki co bardziej „tradycyjne" narzędzia, jako że nie osiągnęły jeszcze tak dalece idącej biegłości w tym zakresie, jak Rosja – zresztą i tak ich wpływ na sytuację polityczną w państwach będących celem uznaje się za niewielki, czego dowodem m.in. wyborcze sukcesy, wbrew chińskim staraniom, proniepodległościowych stronnictw na Tajwanie (Roberts 2020: 5). Pekin posiada jednak w tym obszarze istotny potencjał rozwojowy. Chińska Armia Ludowo-Wyzwoleńcza dostrzegła znaczenie adaptacji mediów społecznościowych do prowadzenia wojny informacyjnej (Harold, Beauchamp-Mustafaga, Hornung 2021: 16–20), co w połączeniu ze stosunkowo wysokimi zdolnościami technologicznymi rodzimego sektora IT może zmienić wskazany stan rzeczy. Pewne wysiłki już zresztą poczyniono. Chiny stworzyły „pięciocentową armię" trolli, w większości pracowników rządowych, którzy publikują w Internecie rocznie ok. 448 mln postów na różnych portalach, w dużej mierze jednak również na użytek wewnętrzny (King, Pan, Roberts 2017: 494–497). Czołowe serwisy społecznościowe usunęły lub zawiesiły wiele powielających chiński przekaz kont przy okazji protestów w Hongkongu latem

2019 roku (Paul 2019) i pandemii COVID-19 (BBC 2020). Oprócz tego władze ChRL wykorzystywały metadane i algorytmy sztucznej inteligencji w kampanii microtargetingu obliczonej na rozbudzanie prochińskich postaw pośród młodych Tajwańczyków (Roberts 2020: 50).

W przypadku Chin pewien potencjał, szczególnie w zakresie stosowania bardziej wysublimowanych form dezinformacji (np. wykorzystujących *big data*) na międzynarodową skalę, stwarza również ich dynamicznie rozwijający się przemysł wysokich technologii – zwłaszcza komputerów (Lenovo) oraz mikroelektroniki. Przykładowo, w 2022 roku ok. 1/3 globalnego rynku smartfonów i tabletów zagospodarowało pięć chińskich firm – Xiaomi, Huawei, OPPO, Vivo i RealMe (za: Statcounter 2022). To istotne w kontekście wymiany informacji między „inteligentnymi" urządzeniami tworzącymi sieci Internetu Rzeczy, zdolnymi zbierać informacje o użytkowniku bez jego wiedzy. Zgodnie z przyjętym w 2017 roku prawem wszystkie chińskie firmy mają obowiązek współpracy z państwowymi służbami wywiadowczymi i udostępniania im stosownych informacji (Kaska, Beckvard, Minárik 2019: 11 i 12 – autorzy wskazują w tym kontekście również na zagrożenia związane z rozbudową chińskiej infrastruktury sieci 5G za granicą). Pozostawia to wiele przestrzeni do pozyskiwania przez władze ChRL elektronicznych danych i ich późniejszego wykorzystania do celów własnej polityki. Oczywiście potencjalny zakres tego procederu jest o wiele szerszy niż dezinformacja, ale również i w tym kontekście dane te mogą okazać się cenne.

Określony potencjał krajowego sektora IT pozwala Chinom i Rosji na pewnego rodzaju „internalizację" Internetu. W przypadku rosyjskim wyraża się to w doktrynie „cyfrowej suwerenności" (Hakala, Melnychuk 2021: 12) i funkcjonowaniu tzw. RuNetu, a więc rosyjskojęzycznej internetowej przestrzeni informacyjnej zdominowanej przez rosyjskie portale społecznościowe VK (d. VKontakte), Yandex czy Odnoklassniki, oraz komunikator Telegram. Gdy mowa o Chinach, wspomnieć należy o portalach społecznościowych Sina Weibo, Kuaishou, Xiaohongshou czy Youku, oraz komunikatorach WeChat i QQ. Szczególnym przypadkiem jest zdobywająca globalną popularność, także w państwach Zachodu, platforma TikTok (w chińskiej wersji – Douyin). Jednocześnie obydwa państwa wprowadziły daleko idące ograniczenia wobec swoich obywateli co do korzystania z największych globalnych sieci społecznościowych, administrowanych przez podmioty zagraniczne – w przypadku Chin wręcz całkowicie je blokując (Rosja w marcu 2022 roku zablokowała Facebooka, Twittera i Instagram, ale był to raczej akt odwetu za ograniczenie możliwości rozpowszechniania na nich treści rosyjskiej propagandy). Opisany stan rzeczy służy głównie dwóm celom: 1) rozpowszechnianiu przekazu pośród ludności rosyjsko– bądź chińskojęzycznej, niezależnie od państwa jej zamieszkania, 2) niedopuszczaniu do krajowej opinii publicznej narracji z zewnątrz, podważających linię polityczną władz.

Inne państwa, których zaangażowanie w dezinformowanie zagranicznej opinii publicznej przez dużej skali kampanie prowadzone, przynajmniej częściowo, w Internecie zostało udowodnione, to Iran (operacja „Endless Mayfly" wymierzona w USA, Izrael i Arabię Saudyjską – zob. Lim 2020: 140–146) i Indie (długoletnia międzynarodowa operacja nazwana „Indian Chronicles", obliczona na dyskredytowanie Pakistanu – zob. Machado i in. 2020: 74–89). Dostrzegalna jest zatem pewna prawidłowość – wszystkie z wymienionych trudno uznać za liberalno-demokratyczne, czego dowodzi np. ranking Freedom House (2022: 18 i 19). Z drugiej strony próżno szukać podobnej skali kampanii prowadzonych np. przez państwa Zachodu. Choć takie próby rzecz jasna podejmowano – przykładem USA w okresie prezydentury Donalda Trumpa i liczne promowane przez niego (i sprzyjające mu media) narracje wymierzone zwłaszcza w Chiny (Hurst, Murphy 2020) – raczej nie okazały się skuteczne na skalę szerszą niż krajowa. Dowodzić może tego choćby brak zdecydowanej presji międzynarodowej na Pekin (w obliczu braku poparcia państw spoza Zachodu) w kierunku rzetelnego wyjaśnienia pochodzenia wirusa SARS-CoV-2, m.in. w świetle oskarżeń ze strony Trumpa – choćby przez skłonienie stawiających opór Chin do wpuszczenia niezależnej grupy badawczej (Maxmen 2022).

Dostrzegalna jest więc korelacja pomiędzy funkcjonowaniem mechanizmów państwa liberalno-demokratycznego a skłonnością i możliwościami stosowania dezinformacji w polityce zagranicznej *par excellence*. W największym stopniu wpływa na to polityczny i medialny pluralizm, w szczególności obecność stronnictw opozycyjnych oraz niezależnych redakcji, które mają możliwość bieżącego identyfikowania i demaskowania tego rodzaju przekazu. Jednocześnie wolność mediów i wypowiedzi sprawiają, że państwa takie pozostają znacznie bardziej narażone na stanie się ofiarą dezinformacji z zewnątrz, jako że kontrola instytucji państwowych nad przestrzenią medialną, w szczególności internetową, jest znacznie mniejsza, a jej egzekwowanie obarczone stosownymi procedurami prawnymi, w myśl których ograniczenia możliwe są do zastosowania jedynie w określonych okolicznościach. Państwom autokratycznym łatwiej dezinformować, ponieważ rządy mają znacznie większy wpływ na przekaz medialny, a same media częściej należą do państwa bądź są podporządkowane władzy.

Dotyczy to zarówno kształtowania owego przekazu, jak i możliwości zapobieżenia potencjalnym kontrakcjom z zewnątrz, np. w postaci fact-checkingu czy też swego rodzaju informacyjnej lub propagandowej „kontrofensywy" wobec własnego społeczeństwa. W odniesieniu do środowiska sieciowego, często próbują wręcz ograniczyć dostęp do Internetu lub mediów społecznościowych – systemowo lub *ad hoc* (na okoliczność konfliktów czy też kryzysów). W latach 2016–2021 doszło do 931 aktów ograniczenia dostępu do Internetu bądź jego szybkości w 74 państwach (w tym 177 razy łącznie 60 państw zastosowało tego typu środki na skalę ogólnokrajową) – aż ok. 60% spośród nich stanowiły regionalne restrykcje wprowadzone

przez władze Indii (łącznie 564), choć także 11 innych państw stosowało takie krajowe lub lokalne środki ponad dziesięciokrotnie[6] (AccessNow 2021). Jak szacuje Biuro Wysokiego Komisarza Narodów Zjednoczonych do spraw Praw Człowieka ok. połowa z tych 931 decyzji stanowiła reakcję na protesty i kryzysy polityczne (z czego 225 na demonstracje), a 52 na wybory – częstym oficjalnym uzasadnieniem władz (w 132 przypadkach) była chęć ograniczenia skali dezinformacji (OHCHR 2022: 5–9).

MECHANIZMY OBRONNE

André W.M. Gerrits (2018: 13 i 14) dzieli środki przeciwdziałania dezinformacji na cztery kategorie: 1) edukacyjne (czyniące odbiorców bardziej odpornymi na tego typu próby), 2) ochronne (wykorzystujące środki technologiczne do jej wykrywania i przeciwdziałania), 3) represyjne (blokowanie manipulacji przy pomocy stosownych technologii), 4) polityczne (środki instytucjonalne, np. służące budowie zaufania między państwami w oparciu o przekonanie, że dezinformacja zagraża bezpieczeństwu międzynarodowemu). Wydaje się, że można je odnieść także do jej zwalczania w środowisku internetowym.

Wymiar edukacyjny dotyczy przede wszystkim działania na zasadzie pracy u podstaw służącej kształtowaniu wśród odbiorców pożądanych nawyków i postaw, takich jak weryfikowanie prawdziwości informacji i krytyczna analiza tych treści, pozyskiwanie ich z różnych źródeł (wyjście poza własną „bańkę informacyjną"), a przede wszystkim świadomość takich zagrożeń i stosowanych w tym celu sposobów manipulacji. Póki co edukacja ta odbywa się raczej na poziomie *grassroots* – za pośrednictwem organizacji pozarządowych czy zainteresowanych podmiotów sektora prywatnego. Z przyczyn, o których nieco dalej, niewiele państw wprowadziło szeroko zakrojone szkolenie w tym zakresie – należą do nich Finlandia i Szwecja, które odpowiednio w 2016 i 2017 roku umieściły tę problematykę w programach nauczania szkół podstawowych (Roden 2017; Henley 2020). Z kolei działania o charakterze *stricte* politycznym dotyczą różnorakich form międzynarodowej współpracy na rzecz zwalczania dezinformacji (także w sieci), podejmowanych przez państwa i organizacje międzynarodowe. Oprócz prewencyjnych i interwencyjnych środków z zakresu komunikacji strategicznej, niektóre państwa przyjęły regulacje prawne dotyczące swoich uprawnień kontrolnych oraz obowiązków nakładanych na nadawców i właścicieli platform społecznościowych (*vide* kompleksowa ustawa francuska z 2018 roku).

Z perspektywy niniejszego opracowania szczególnie ważne są środki przeciwdziałania dezinformacji wykorzystujące rozwiązania technologiczne, których

[6] Były to: Pakistan (41), Jemen (27), Irak (24), Etiopia (23), Mjanma (19), Syria (14), Wenezuela (14), Bangladesz (12), Iran (12), Algieria (11), Sudan (11).

Gerrits (2018: 13 i 14) wyróżnia dwa rodzaje – ochronne (można je określić jako „miękkie") i represyjne („twarde"). Do tych pierwszych zaliczają się wszelkie formy zautomatyzowanego fact-checkingu, prezentowanie szerszego kontekstu tematycznego w odniesieniu do danej opublikowanej treści, czy też odpowiednie oznaczanie informacji o ograniczonej wiarygodności lub autorstwa instytucji państwowych bądź podmiotów finansowanych ze środków publicznych (jak czyni to choćby YouTube). Drugi rodzaj dotyczy częściowej lub całkowitej blokady dostępu do danej platformy dla podmiotu stosującego groźne manipulacje informacjami. Może więc obejmować bardzo szeroki zakres działań – od moderowania treści udostępnianych na forach czy w mediach społecznościowych (łącznie z ich usuwaniem) aż po tzw. *deplatforming*, czyli odebranie możliwości korzystania z danej platformy konkretnej osobie czy podmiotowi zbiorowemu. Na tę politykę coraz częściej decydują się największe portale społecznościowe (Twitter, Facebook, Instagram czy YouTube), czemu dały wyraz, usuwając po szturmie zwolenników Donalda Trumpa na Kapitol 6 stycznia 2021 roku konta 45. prezydenta USA oraz wielu przedstawicieli sympatyzującego z nim ruchu Alt-right, a później z kolei przedstawicieli birmańskiej junty po zamachu stanu z lutego 2021 roku czy rosyjskich władz i instytucji państwowych po inwazji na Ukrainę z lutego 2022 roku (w tym przypadku portale te wręcz ograniczyły całą swoją aktywność na terytorium Federacji Rosyjskiej). Kroki te wzbudziły pewne dyskusje zarówno z racji zakresu ingerencji podmiotów sektora prywatnego w sprawy publiczne, jak również nieprzejrzystości kryteriów stosowania tego rodzaju ograniczeń (zob. np. Bokat-Lindell 2021; Concha 2021).

Zwalczanie opisywanych w tekście zjawisk obarczone jest jednak dwoma zasadniczymi ograniczeniami. Po pierwsze, współczesne jej formy, wykorzystujące cyberprzestrzeń, aby możliwe było skuteczne im zapobieganie, wymagają specjalistycznej wiedzy eksperckiej, często z zakresu nauk ścisłych, którą decydenci polityczni i „tradycyjni" przedstawiciele nauk o bezpieczeństwie i o stosunkach międzynarodowych (nie wyłączając autora niniejszego artykułu) zwyczajnie nie dysponują. Utrudnia to selekcję i wdrożenie stosownych środków zaradczych, stąd niezwykle ważny staje się postulat tworzenia interdyscyplinarnych zespołów zajmujących się tą tematyką. Po drugie zaś, co wydaje się jeszcze poważniejszym problemem, dostrzec można nieraz pewne ciche przyzwolenie na dezinformację, skutkujące brakiem woli podjęcia dalej idących, skuteczniejszych działań – zarówno ze strony decydentów politycznych (wykorzystujących analogiczne mechanizmy marketingu politycznego oraz tego rodzaju instrumenty w polityce wewnętrznej i zagranicznej, m.in. do wzmocnienia tych punktów własnej agendy, które pokrywają się z „zasiewanymi" z zewnątrz), jak i sektora prywatnego (zwłaszcza mediów i platform społecznościowych, jako że generuje to ruch sieciowy, co przekłada się na wymierne zyski dla tychże podmiotów, m.in. z reklam).

Nieskuteczność dotychczas stosowanych środków ukazuje przykład Polski. Jest państwem o już i tak wysokiej percepcji zagrożenia ze strony Rosji i świadomości intencji Kremla (Szeptycki 2021: 141). Mimo to wzmożenie rosyjskiej dezinformacji w pierwszych dniach po agresji na Ukrainę 24 lutego 2022 roku, czego rezultatem były m.in. lawinowy wzrost (nawet do 130 tys. dziennie) prorosyjskich wzmianek w mediach społecznościowych (zob. Kowalski 2022), wywołało panikę skutkującą masowym wykupem paliwa i wypłatami pieniędzy z kont bankowych oraz wzbudziło strach przed ukraińskimi uchodźcami, który doprowadził do incydentów na ulicach Przemyśla (zob. Puto 2022).

WNIOSKI

Zgodnie z wynikami przeprowadzonego w 2022 roku w 46 krajach badania Internet (czyli portale i media społecznościowe – dla samych social mediów odsetek ten wyniósł średnio 56,8%) stał się on głównym źródłem informacji dla (w uśrednieniu) 82,1% ankietowanych, podczas gdy telewizję za takie uznało 61,3%, prasę zaś – jedynie 23,4% (obliczenia własne na podst. Newman i in. 2022: 62–159). W skali minionej dekady trend był rosnący dla źródeł internetowych oraz malejący dla mediów tradycyjnych. Masowość środowiska informacyjnego wykorzystującego cyberprzestrzeń oraz niemal nieograniczona dostępność do niego (pod względem czasu, miejsca i potrzebnych ku temu środków), a z drugiej strony jego maksymalnie zdezagregowany, zindywidualizowany, w pełni zależny od woli użytkownika (podatnego przy tym na liczne ludzkie błędy poznawcze) charakter są więc bodaj głównymi cechami tegoż, które sprawiają, że możliwości skutecznego stosowania dezinformacji są współcześnie bezprecedensowo duże. Dostrzegli to politycy, dla których bieżąca aktywność w mediach społecznościowych stała się niemal równie ważna jak pozostałe obszary działalności, czego najlepszym, choć nie jedynym, przykładem jest rzecz jasna Donald Trump.

Potęgują to ponadto zjawiska społeczne będące pochodną wszechobecności Internetu i mediów społecznościowych – zmiana charakteru relacji międzyludzkich, w tym większa atomizacja jednostek i tzw. syndrom FOMO (*fear of missing out* – poczucie strachu przed pominięciem czegoś ważnego, mające związek z dostarczaniem umysłowi niezliczonej liczby bodźców podczas korzystania z sieci), które sprzyjają tworzeniu się „baniek informacyjnych" i w konsekwencji – dalszej polaryzacji. Wielu użytkowników korzysta z Internetu z dużą dezynwolturą, przejawiającą się nie tylko w nieweryfikowaniu napotkanych informacji, lecz także udostępnianiu (często dobrowolnie) na masową skalę – nie tylko w cyberprzestrzeni, ale też w życiu codziennym, np. przy pomocy „inteligentnych" sprzętów (Internet Rzeczy) – danych zewnętrznym podmiotom, z których wiele (jak pokazał przypadek firmy Cambridge Analytica) może zrobić użytek także przez wykorzystanie pozyskanych zasobów do dezinformowania (np. przy użyciu microtargetingu).

Rozwój technologiczny stworzył więc nie tylko masowe fora dla dezinformacji, ale także zupełnie nowe możliwości techniczne jej służące, zwłaszcza w związku z algorytmami opartymi o sztuczną inteligencję i zbiory *big data*, tak by zwodniczy przekaz był jak najbardziej powszechny, stwarzał dalece idące pozory wiarygodności oraz odpowiadał potrzebom poszczególnych użytkowników (na podstawie śladów ich aktywności w sieci).

Choć na zjawisko nadmiaru bodźców docierających do jednostki, w tym „przeciążenia informacyjnego", zwracał uwagę już na przełomie lat sześćdziesiątych i siedemdziesiątych Alvin Toffler (1970: 343–355), wydaje się, że współcześnie, z uwagi na wzmiankowane wyżej procesy, przybrało ono nieznaną wcześniej skalę. Użytkownik Internetu styka się z ogromną liczbą komunikatów, z których tylko małą częścią jest w stanie, z uwagi na ograniczenia czasu i zdolności ludzkiej percepcji, się zapoznać. Stąd rozmaici nadawcy internetowi zmuszeni są zabiegać o uwagę internauty, o jego zaangażowanie. Sprzyja temu ponadto natura nastawionych na zysk podmiotów prywatnych – mediów oraz wszelkiego rodzaju platform świadczących rozmaite usługi w cyberprzestrzeni, szczególnie zaś „wielkiej czwórki" GAFA, największych światowych korporacji, tj. Google, Apple, Facebook (dziś Meta) i Amazon. W kontekście dezinformacji ma to dwojakie znaczenie: po pierwsze, przyzwyczaja użytkownika do mechanizmów wykorzystywanych w ramach tego rodzaju działań (manipulacji i socjotechnik), czyniąc go bardziej na nie podatnym; po drugie zaś, umożliwia rzeczywistym nadawcom zmanipulowanego przekazu ukrycie swojego faktycznego zaangażowania za tą swego rodzaju „mgłą informacyjną".

Patrząc na państwa, które wykorzystują instrumentarium ukształtowane w oparciu o zdobycze czwartej rewolucji przemysłowej na rzecz dezinformacji międzynarodowej, dostrzec należy, że są to te same, które i tak mają długą historią tego typu działań przy użyciu „tradycyjnych" sposobów. Internet stał się po prostu kolejną przestrzenią ich oddziaływania. Jako że dotyczy to przede wszystkim Rosji i Chin, także w kontekście „adresatów" tego rodzaju praktyk z ich strony, dostrzec można pewną wspólnotę celów. Ma to związek z przejawianą na wiele sposobów kontestacją liberalnego porządku międzynarodowego i pozycji Stanów Zjednoczonych w globalnym układzie sił (zob. szerzej: Kuźniar 2022: 117–129, 222–250, 293–299).

Pewien paradoks polega więc na tym, że to nie Zachód, który wciąż dysponuje największym potencjałem technologicznym i który stworzył warunki do zaistnienia czwartej rewolucji przemysłowej, jest w stanie wykorzystywać te kanały na swoją korzyść przeciwko Rosji i Chinom jako mocarstwom rewizjonistycznym, ale to one wyrządzają mu szkody, walcząc „jego własną bronią" (gdzie posiadanie określonego potencjału krajowego sektora IT stanowi jednak ważną okoliczność sprzyjającą). Decyduje o tym przede wszystkim natura systemu politycznego tych państw. Autokracje pozostają w dużej mierze odporne na tego

rodzaju oddziaływanie z zewnątrz, z uwagi na większe możliwości kształtowania obiegu informacji oraz ograniczania funkcjonowania niektórych mediów czy wręcz wprowadzenia całkowitej lub częściowej blokady Internetu. Państwa liberalno-demokratyczne z kolei pozostają na nie bardziej podatne, co wynika z funkcjonowania pluralizmu politycznego i medialnego oraz znacząco ograniczonych, zwłaszcza prawem krajowym, możliwości ingerencji w infosferę. Warto również zauważyć znamienny w omawianym kontekście fakt, że to właśnie w strefie euroatlantyckiej tradycyjne media cieszą się największym zainteresowaniem, podczas gdy obywatele państw Ameryki Łacińskiej, Azji Wschodniej czy Afryki znacznie częściej wybierają Internet i media społecznościowe (Newman i in. 2022: 114–159), co sugerowałoby ich większą podatność na rosyjską czy chińską dezinformację w sieci. Ta pozostaje więc dla USA i reszty państw Zachodu wyzwaniem nie tylko w kontekście zwalczania jej przejawów na poziomie krajowym, ale również w ich relacjach z innymi państwami.

Zakres mechanizmów służących zwalczaniu dezinformacji międzynarodowej w Internecie pozostaje ograniczony, w dodatku są one obarczone wieloma istotnymi zastrzeżeniami. Środki edukacyjne z założenia obliczone są na efekt długoterminowy, a prawno-polityczne często nie są w stanie nadążyć za tempem rozwoju tego instrumentarium i jego naturą (np. możliwością skorzystania z wirtualnej sieci prywatnej – VPN – i serwerów proxy, co umożliwia ominięcie nałożonych restrykcji, np. blokady określonych treści). Zwalczanie dezinformacji w sieci wymaga też od decydentów dostępu do eksperckiej wiedzy oraz zwykłej woli politycznej ku temu, których często brakuje.

Pewnym rozwiązaniem mogą być środki techniczne służące ograniczaniu skali dezinformacji w sieci. Wielu autorów dostrzega szanse związane z rozwojem narzędzi bazujących na sztucznej inteligencji, w szczególności mechanizmach machine learningu lub deep learningu, które mogą być wykorzystane do m.in. zautomatyzowanego fact-checkingu, wykrywania fake newsów (przez analizę tekstu), deepfake'ów oraz zmanipulowanych obrazów, materiałów audio i video, wykrywania i blokowania trolli, botów bądź „pacynek" (*sockpuppets* – chodzi o sieci złożone z co najmniej kilku kont używanych do pozorowania interakcji w Internecie, np. w celu propagowania zmanipulowanego przekazu) lub też skutecznego potwierdzania autentyczności określonych treści (zob. Kertysova 2018: 58–60; Juršėnas i in. 2022: 8–19). O ile jednak mechanizmy te mogą być niezwykle pomocne w zwalczaniu dezinformacji w sieci, nie rozwiążą tego problemu w całości. Wobec np. komunikatów podprogowych (wykorzystujących ironię, symbolikę lub innego rodzaju czynniki abstrakcyjne), manipulowania kontekstem bądź emocjami odbiorców czy innych treści możliwych do identyfikacji jedynie przez ludzki umysł, algorytmy pozostaną bezradne.

LITERATURA PRZYWOŁANA

AccessNow (2021), *#KeepItOn STOP Data 2016–2021*, https://docs.google.com/spreadsheets/d/1DvPAuHNLp5BXGb0nnZDGNoiIwEeu2ogdXEIDvT4Hyfk/edit (dostęp 17.07.2022).

Aleksandrowicz Tomasz R. (2021), *Zagrożenia dla bezpieczeństwa informacyjnego państwa w ujęciu systemowym. Budowanie zdolności defensywnych i ofensywnych w infosferze*, Warszawa: Wydawnictwo Difin.

Ang Carmen (2021), *Ranked: The World's Most Popular Social Networks, and Who Owns Them*, https://www.visualcapitalist.com/ranked-social-networks-worldwide-by-users/ (dostęp 17.07.2022).

Aro Jessikka (2020), *Trolle Putina. Prawdziwe historie z frontów rosyjskiej wojny informacyjnej*, tłum. Marta Laskowska, Kraków: Wydawnictwo SQN.

Baade Björnstjern (2018), *Fake News and International Law*, „The European Journal of International Law", t. 29, nr 4, s. 1357–1376.

Banasik Mirosław (2018), *Wojna hybrydowa i jej konsekwencje dla bezpieczeństwa euroatlantyckiego*, Warszawa: Wydawnictwo Difin.

Banasik Mirosław (2021), *Teoria i praktyka wojny informacyjnej stosowanej przez Federację Rosyjską*, w: Mirosław Banasik (red.), *Informacja czynnikiem warunkującym bezpieczeństwo. Kontekst rosyjski*, Warszawa: Wydawnictwo Difin, s. 49–65.

BBC (2020), *Coronavirus: Twitter removes more than 170,000 pro-China accounts, BBC News*, 12.06.2020, https://www.bbc.com/news/business-53018455 (dostęp 17.07.2022).

Bokat-Lindell Spencer (2021), *Deplatforming Trump Could Work. But at What Cost?* „The New York Times", 14.01.2021.

Brynjolfsson Erik, McAfee Andrew (2014), *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*, New York–London: W.W. Norton & Company.

Cadwalladr Caroline (2018), *'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower*, „The Guardian", 18.03.2018.

Castells Manuel (2007), *Społeczeństwo sieci*, tłum. Mirosława Marody, Kamila Pawluś, Janusz Stawiński, Sebastian Szymański, Warszawa: Wydawnictwo Naukowe PWN.

CFDD (2021), *Trained for Deception: How Artificial Intelligence Fuels Online Disinformation*, Coalition to Fight Digital Deception.

Concha Joe (2021), *'Strikingly sophisticated' Taliban thrive on Twitter while Trump still banned*, „The Hill", 20.08.2021.

Darczewska Jolanta (2014), *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku*, Warszawa: Ośrodek Studiów Wschodnich im. Marka Karpia.

Darczewska Jolanta (2019), *Między jawną dezinformacją a niejawną praktyką*, Warszawa: Ośrodek Studiów Wschodnich im. Marka Karpia.

Debord Guy (1990), *Comments on the Society of the Spectacle*, tłum. Malcolm Imrie, London–New York: Verso.

Dooley Sarah, Moore Emma, Averin Alexander (2018), *Change and 21st Century Media*, w: Leonie Haiden, Jente Althuis (red.), *Fake News. A Roadmap*, Riga: NATO Strategic Communications Centre of Excellence.

Dubow Ben, Lucas Edward, Morris Jake (2021), *Jabbed in the Back: Mapping Russian and Chinese Information Operations During COVID-19*, Washington, DC: Center for European Policy Analysis.

EUvsDisinfo (2021), *Modus trollerandi*, https://euvsdisinfo.eu/modus-trollerandi/(dostęp 17.07.2022).

EUvsDisinfo (2022), *Disinfo database*, https://euvsdisinfo.eu/disinformation-cases/ (dostęp 17.07.2022).

Fineklstein Joseph, Newman David (1984), *The Third Industrial Revolution: A Special Challenge to Managers*, „Organizational Dynamics", t. 13, nr 1, s. 53–65.

Freedom House (2022), *Freedom In the World 2022. The Global Expansion of Authoritarian Rule*, Washington, DC: Freedom House.

Gądek Jacek (2022), *Marcin Rey: W Polsce mamy wojnę informacyjną. „Nie kopać gówna"? To dziś nieaktualne*, https://wiadomosci.gazeta.pl/wiadomosci/7,114883,28259171,marcin-rey-w-polsce-mamy-wojne-informacyjna-nie-kopac-gowna.html (dostęp 17.07.2022).

Gerrits André W.M. (2018), *Disinformation in International Relations: How Important Is It?* „Security and Human Rights", t. 29, nr 1–4, s. 3–23.

Gielewska Anna, Dauksza Julia (2021), *The Ghostwriter Scenario*, VSquare, 13.08.2021, https://vsquare.org/the-ghostwriter-scenario/ (dostęp 17.07.2022).

Giles Keir, Hartmann Kim, Mustaffa Munira (2019), *The Role of Deepfakes in Malign Influence Campaigns*, Riga: NATO Strategic Communication Centre of Excellence.

Goban-Klas Tomasz, Sienkiewicz Piotr (1999), *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, Kraków: Wydawnictwo Fundacji Postępu Telekomunikacji.

Grabowski Tomasz W. (2018), *Postprawda a bezpieczeństwo. Wprowadzenie*, w: Tomasz W. Grabowski, Mirosław Lakomy, Konrad Oświecimski (red.), *Bezpieczeństwo informacyjne państwa w dobie postprawdy*, Kraków: Wydawnictwo Naukowe Akademii Ignatianum w Krakowie, s. 9–32.

Greenleigh Ian (2014), *The Social Media Side Door: How to Bypass the Gatekeepers to Gain Greater Access and Influence*, New York: McGraw-Hill Education,

Haidt Jonathan (2022), *Why the past 10 years of American life have been uniquely stupid*, „The Atlantic", nr 5.

Haigh Maria, Haigh Thomas (2020), *Fighting and Framing Fake News*, w: Paul Baines, Nicholas O'Shaghnessy, Nancy Snow (red.), *The SAGE Handbook of Propaganda*, London: SAGE Publications, s. 303–322.

Hakala Janne, Melnychuk Jazlyn (2021), *Russia's Strategy in Cyberspace*, Riga: NATO Strategic Communication Centre of Excellence.

Harold Scott W., Beauchamp-Mustafaga Nathan, Hornung Jeffrey W. (2021), *Chinese Disinformation Efforts on Social Media*, Santa Monica: RAND Corporation.

Helfgott Roy B. (1986), *America's Third Industrial Revolution*, „Challenge", t. 29, nr 5, s. 41–46.

Henley Jon (2020), *How Finland starts its fight against fake news in primary schools*, „The Guardian", 29.01.2020.

Homer (2014), *Odyseja*, tłum. z greki Lucjan Siemieński, https://wolnelektury.pl/media/book/pdf/homer-odyseja.pdf (dostęp 17.07.2022).

Humprecht Edda, Esser Frank, Van Aelst Peter (2020). *Resilience to online disinformation: A framework for cross-national comparative research*, „International Journal of Press/Politics", t. 25, nr 3, s. 493–516.

Hurst Daniel, Murphy Katharine (2020), *Trump's misleading information enables China to sow discord among allies, research finds*, „The Guardian", 22.06.2020.

Intelligence Community (2017), *Assessing Russian Activities and Intentions in Recent US Elections*, https://en.wikisource.org/wiki/Assessing_Russian_Activities_and_Intentions_in_Recent_US_Elections (dostęp 17.07.2022).

Internet Live Stats (2022), https://www.internetlivestats.com/ (dostęp 17.07.2022).

Juršėnas Alfonsas, Karlauskas Kasparas, Ledinauskas Eimantas , Maskeliūnas Gediminas, Rondomanskas Donatas, Ruseckas Julius (2022), *The Role of AI in the Battle against Disinformation*, Riga: NATO Strategic Communications Centre of Excellence.

Kaska Kadri, Beckvard Henrik, Minárik Tomáš (2019), *Huawei, 5G and China as a Security Threat*, Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Kertysova Katarina (2018), *Artificial Intelligence and Disinformation. How AI Changes the Way Disinformation is Produced, Disseminated, and Can Be Countered*, „Security and Human Rights", t. 29, nr 1–4, s. 55–81.

King Gary, Pan Jennifer, Roberts Margaret E. (2017), *How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument*, „American Political Science Review", t. 111, nr 3, s. 484–501.

Kowalski Jacek (2022), *Nagły wzrost dezinformacji w polskim internecie. Prorosyjskie konta trollowały też w sprawie szczepionek*, https://www.wirtualnemedia.pl/artykul/wzrost-dezinformacja-polski-internet-atak-rosja-na-co-uwazac (dostęp 17.07.2022).

Kurowska Xymena, Reshetnikov Anatoly (2018), *Neutrollization: Industrialized trolling as a pro-Kremlin strategy of desecuritization*, „Security Dialogue", t. 49, nr 5, s. 345–363.

Kuźniar Roman (2022), *Zmierzch liberalnego porządku międzynarodowego 2011–2021*, Warszawa: Wydawnictwo Naukowe Scholar.

la Cour Christina (2020), *Theorising digital disinformation in international relations*, „International Politics", t. 57, nr 4, s. 704–723.

Lanoszka Alexander (2019), *Disinformation in international politics*, „European Journal of International Security", t. 4, nr 2, s. 227–248.

Lasi Heiner, Fettke Peter, Kemper Hans-Georg, Feld Thomas, Hoffmann Michael (2014), *Industry 4.0*, „Business & Information Systems Engineering", t. 6, nr 4, s. 239–242.

Legucka Agnieszka (2020), *Dezinformacja jako element wojny informacyjnej Federacji Rosyjskiej – założenia i efektywność*, „Sprawy Międzynarodowe", t. 73, nr 4, 159–186.

Lim Gabrielle (2020), *Case study: Attributing Endless Mayfly*, w: Craig Silverman (red.), *Verification Handbook For Disinformation And Media Manipulation*, Maastricht: European Journalism Centre.

Machado Gary, Alaphilippe Alexandre, Adamczyk Roman, Gregoire Antonie (2020), *Indian Chronicles. Subsequent Investigation: Deep Dive into a 15-year Operation Targeting the EU and UN to Serve Indian Interests*, Brussels: EU DisinfoLab.

Madej Marek (2007), *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*, Warszawa: Polski Instytut Spraw Międzynarodowych.

Mandel Robert (2019), *Global Data Shock. Strategic Ambiguity, Deception, and Surprise in an Age of Information Overload*, Stanford: Stanford University Press.

Marek Michał (2020), *Operacja Ukraina. Kampanie dezinformacyjne, narracje, sposoby działania rosyjskich ośrodków propagandowych przeciwko państwu ukraińskiemu w okresie 2013–2019*, Warszawa: Wydawnictwo Difin.

Matthews Miriam, Migacheva Katya, Brown Ryan Andrew (2021), *Superspreaders of Malign and Subversive Information on Covid 19. Russian and Chinese Efforts Targeting the United States*, Santa Monica: RAND Corporation.

Maxmen Amy (2022), *Scientists struggle to probe COVID's origins amid sparse data from China*, https://www.nature.com/articles/d41586-022-00732-0 (dostęp 17.07.2022).

McDonald-Gibson Charlotte (2015), *How ISIS Threatens Europe*, https://time.com/3720076/isis-europe-migrants/ (dostęp 17.07.2022).

Merrill Jeremy B., Oremus Will (2021), *Five points for anger, one for a 'like': How Facebook's formula fostered rage and misinformation*, „The Washington Post", 26.11.2021.

Modrzejewski Zbigniew (2018), *Dezinformacja w służbie walki informacyjnej*, w: Tomasz W. Grabowski, Mirosław Lakomy, Konrad Oświecimski (red.), *Bezpieczeństwo informacyjne państwa w dobie postprawdy*, Kraków: Wydawnictwo Naukowe Akademii Ignatianum w Krakowie, s. 91–117.

NATO StratCom CoE (2016), *Social Media as a Tool of Hybrid Warfare*, Riga: NATO Strategic Communications Centre of Excellence.

Newman Nic, Fletcher Richard, Robertson Craig T., Eddy Kirsten, Nielsen Rasmus Kleis (2022), *Reuters Institute Digital News Report 2022*, Oxford: Reuters Institute for the Study of Journalism.

Neo Ric (2021), *The International Discourses and Governance of Fake News*, „Global Policy", t. 12, nr 2, s. 214–228.

Nimmo Ben, François Camille, Eib C. Shawn, Ronzaud Lea, Ferrera Rodrigo, Hernon Chris, Kostelancik Tim (2020), *Secondary Infektion*, New York: Graphika Inc.

Nord Pierre (1999), *Intoksykacja widziana przez intoksykującego*, w: Vladimir Volkoff (oprac.), *Psychosocjotechnika, dezinformacja. Oręż wojny*, tłum. Anatol Arciuch, Komorów: Wydawnictwo ANTYK Marcin Dybowski.

OHCHR (2022), *Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights*, A/HRC/50/55, Geneva–New York: Office of the United Nations High Commissioner for Human Rights.

Oltermann Philip (2022), *European politicians duped into deepfake video calls with mayor of Kyiv*, „The Guardian", 25.06.2022.

O'Shaugnessy Nicholas (2020), *From Disinformation to Fake News: Forwards into the Past*, w: Paul Baines, Nicholas O'Shaghnessy, Nancy Snow (red.), *The SAGE Handbook of Propaganda*, London: SAGE Publications, s. 55–70.

Osmundsen Mathias, Bor Alexander, Bjerregaard Vahlstrup Peter, Bechmann Anja, Bang Petersen Michael (2021), *Partisan Polarization Is the Primary Psychological Motivation behind Political Fake News Sharing on Twitter*, „American Political Science Review", t. 115, nr 3, s. 999–1015.

Pacek Piotr (2017), *Wojna informacyjna jako istotny element zbrojnego konfliktu hybrydowego na Ukrainie*, w: Bogusław Pacek, Julia Anna Grochocka (red.), *Konflikt hybrydowy na Ukrainie. Aspekty teoretyczne i praktyczne*, Piotrków Trybunalski: Wydawnictwo Uniwersytetu Jana Kochanowskiego w Kielcach Filia w Piotrkowie Trybunalski, s. 199–215.

Paul Kari (2019), *Twitter and Facebook crack down on accounts linked to Chinese campaign against Hong Kong*, „The Guardian", 20.08.2019.

Pogorzelski Piotr (2017), *Zagrożenie rosyjską dezinformacją w Polsce i formy przeciwdziałania*, Wojnowice: Kolegium Europy Wschodniej im. Jana Nowaka-Jeziorańskiego we Wrocławiu.

Pomerantsev Peter (2014), *Nothing is true and everything is possible. The surreal heart of the new Russia*, New York: PublicAffairs, Perseus Books Group.

Posetti Julie, Matthews Alice (2018), *A short guide to the history of 'fake news' and disinformation*, Washington, DC: International Center for Journalists.

Puto Kaja (2022), *Wojna na fejki*, https://www.dwutygodnik.com/artykul/9987-wojna-na-fejki.html (dostęp 17.07.2022).

Roberts Dexter (2020), *China's Disinformation Strategy. Its Dimensions and Future*, Washington, DC: Atlantic Council.

Roden Lee (2017), *Swedish kids to learn computer coding and how to spot fake news in primary school*, https://www.thelocal.se/20170313/swedish-kids-to-learn-computer-coding-and-how-to-spot-fake-news-in-primary-school/ (dostęp 17.07.2022).

Roozenbeek Jon, Schneider Claudia R., Dryhurst Sarah, Kerr John, Freeman Alexandra L.J., Recchia Gabriel, van der Bles Anne Marthe, van der Linden Sander (2020), *Susceptibility to misinformation about COVID-19 around the world*, https://royalsocietypublishing.org/doi/10.1098/rsos.201199 (dostęp 17.07.2022).

Rotondo Annachiara, Salvati Pierluigi (2019), Fake News, *(Dis)information, and the Principle of Nonintervention. Scope, limits, and possible responses to cyber election interference in times of competition*, „The Cyber Defense Review", special edition, s. 209–223.

Sawicka Zofia (2017), *Wpływ nowych mediów na przemiany polityczne wybranych państw Bliskiego Wschodu na przykładzie Arabskiej Wiosny*, Warszawa: Wydawnictwa Uniwersytetu Warszawskiego.

Schwab Klaus (2016), *The Fourth Industrial Revolution*, Cologny: World Economic Forum.

Searight Amy (2020), *Countering China's Influence Operations: Lessons from Australia*, https://www.csis.org/analysis/countering-chinas-influence-operations-lessons-australia (dostęp 17.07.2022).

Shandra Alya (2020), *A guide to Russian propaganda. Part 6: Spetspropaganda, the secret Soviet art of brainwashing*, https://euromaidanpress.com/2020/07/07/a-guide-to-russian-propaganda-part-6-spetspropaganda-the-secret-soviet-art-of-brainwashing/ (dostęp 17.07.2022).

Skilton Mark, Hovsepian Felix (2018), *The 4th Industrial Revolution. Responding to the Impact of Artificial Intelligence on Business*, Cham: Palgrave Macmillan.

Statcounter (2022), *Mobile Vendor Market Share Worldwide*, June 2022, https://gs.statcounter.com/vendor-market-share/mobile/worldwide/ (dostęp 17.07.2022).

Stewart Devin (2020), *Risks to the Japan-China 'Tactical Detente'*, https://nationalinterest.org/feature/risks-japan-china-tactical-detente-113426 (dostęp 17.07.2022).

Sun Tzu (2007), *Sztuka wojny oraz 36 podstępów*, tłum. i oprac. Jarosław Zawadzki, e-book.

Szakács Judit, Bognár Eva (2021), *The impact of disinformation campaigns about migrants and minority groups in the EU*, Brussels: Directorate General for External Policies of the Union.

Szeptycki Andrzej (2021), *Polish Take on Realism: Poland's Policy Towards the Former Soviet Countries, 1991–2021*, „Journal of International Analytics", t. 12, nr 1, s. 132–145.

Tessier Dana (2020), *The Needle in the Haystack: How Information Overload Is Impacting Society and Our Search for Truth*, w: Kimiz Dalkir, Rebecca Katz (red.), *Navigating Fake News, Alternative Facts, and Misinformation in a Post-Truth World*, Hershey, PA: IGI Global, 18–35.

Thomas Timothy L. (2004), *Russia's Reflexive Control Theory and the Military*, „Journal of Slavic Military Studies", t. 17, nr 2, s. 237–256.

Tiffany Kaitlyn (2021), *I Made the World's Blandest Facebook Profile, Just to See What Happens*, „The Atlantic", 19.11.2021.

Toffler Alvin (1970), *Future Shock*, New York: Random House.

Venturini Tommaso (2019), *From fake to junk news, the data politics of online virality*, w: Didier Bigo, Engin Isin, Evelyn Ruppert (red.), *Data Politics. Worlds, Subjects, Rights*, London-New York: Routledge.

Verhulst Adrien, Zhao Wanqi, Nakamura Fumihiko, Fukuoka Masaaki, Sugimoto Maki, Inami Masahiko (2020), *Impact of Fake News in VR compared to Fake News on Social Media, a pilot study*, 2020 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), s. 577 i 578.

Volkoff Vladimir (1999), *Psychosocjotechnika, dezinformacja. Oręż wojny*, tłum. Anatol Arciuch, Komorów: Wydawnictwo ANTYK Marcin Dybowski.

Vosoughi Soroush, Roy Deb, Aral Sinan (2018), *The spread of true and false news online*, „Science", t. 359, nr 6380, s. 1146–1151.

Wasiuta Olga, Wasiuta Sergiusz (2017), *Wojna hybrydowa Rosji przeciwko Ukrainie*, Kraków: Wydawnictwo Arcana.

Wasiuta Olga, Wasiuta Sergiusz (2019), *Deepfake jako skomplikowana i głęboko fałszywa rzeczywistość*, „Annales Universitatis Paedagogicae Cracoviensis", t. 9, nr 3, s. 19–30.

Wigell Mikael (2019), *Hybrid interference as a wedge strategy: a theory of external interference in liberal democracy*, „International Affairs", t. 95, nr 2, s. 255–275.

Wojnowski Michał (2015), *„Zarządzanie refleksyjne" jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w.*, „Przegląd Bezpieczeństwa Wewnętrznego", t. 7, nr 12, s. 11–36.

Wrzosek Marek, Markiewicz Szymon, Modrzejewski Zbigniew (2018), *Informacyjny wymiar wojny hybrydowej*, Warszawa: Akademia Sztuki Wojennej.

Piotr Śledź

DISINFORMATION IN INTERNATIONAL RELATIONS UNDER THE CONDITIONS OF THE FOURTH INDUSTRIAL REVOLUTION

This paper examines the opportunities for international disinformation resulting from the technological development under the Fourth Industrial Revolution and from its social implications. It assumes these phenomena have brought new instruments and opportunities for states to make use of disinformation on an unprecedented scale which has been enabled by the features of the contemporary information environment based mostly on Internet and social media. As a result disinformation has become arguably easier, more efficient and, therefore, more threatening than ever before. At the beginning the paper explores the aforementioned features and outlines which disinformation strategies can be used on a large scale in such circumstances. It identifies subsequently states making use of the new disinformation toolkit in their foreign policies as well as their main motivations and enablers. The final section presents the countermeasures to disinformation that could be undertaken and assesses the limits of their application.

Słowa kluczowe: dezinformacja, czwarta rewolucja przemysłowa, Internet, media społecznościowe, sztuczna inteligencja

Keywords: disinformation, Fourth Industrial Revolution, Internet, social media, Artificial Intelligence