Marcelina Pietras*

Wojna informacyjna jako współczesne narzędzie działań nieregularnych

Streszczenie

Trwająca obecnie na całym świecie rewolucja naukowo-informacyjna zmienia całkowicie najistotniejsze cele toczących się konfliktów, a wraz z nimi ustala globalny charakter oraz cel gry we współczesnych konfliktach. Czynniki walki zostały przewartościowane, rywalizacja o zasoby materialne zamieniona na zmagania o zasoby duchowe i intelektualne, a ludzka świadomość została głównym przedmiotem walki, umysł człowieka zaś polem bitwy.

Aktualnie informację uważa się za trzeci, fundamentalny komponent otaczającej nas rzeczywistości. Rozwój technologiczny sektora urządzeń komunikacyjnych spowodował, że współcześnie ludność cywilna nie jest już tylko biernym obserwatorem sytuacji, ale staje się uczestnikiem i podmiotem wydarzeń, np. poprzez swoją aktywność w mediach społecznościowych. Z punktu widzenia operacji sił specjalnych dostarczenie rzetelnej informacji lokalnej społeczności jest niezwykle istotne, ponadto często decyduje zarówno o pomyślności misji, jak i o potencjalnej śmierci.

Celem niniejszego artykułu jest zidentyfikowanie wpływu rozwoju technik informacyjnych na zmiany w obrębie prowadzenia i stosowania współczesnych form działań nieregularnych. Dokonano analizy pojęć, płaszczyzn oraz koncepcji walki w sferze informacji oraz wpływu na społeczeństwo. W artykule autorka wykazała rolę mediów społecznościowych w nowym podejściu do stosowania działań nieregularnych oraz zbadała zmiany, które zaszły w operacjach dezinformujących wykorzystujących nowoczesne technologie.

Słowa kluczowe: działania nieregularne, walka informacyjna, media społecznościowe, dezinformacja, sztuczna inteligencja

* Marcelina Pietras, Akademia Sztuki Wojennej w Warszawie, e-mail: marcelinapietras99@gmail.com.

Wstęp

Obserwując otaczającą rzeczywistość, można zauważyć dynamiczne zmiany zachodzące w sferach informacyjnych. Mają one wpływ na każdy aspekt życia również w zakresie prowadzenia działań zbrojnych, w tym nieregularnych. O istocie dzisiejszej nieregularności działań świadczą takie jej znane cechy, jak: zaskoczenie, asymetryczność czy wielowymiarowość, ale też w dużej mierze współcześnie wykorzystanie działań informacyjnych czy wręcz stosowanie dywersji psychologicznej. Zatem za przedmiot badań przyjęto – w kontekście współczesnym – działania nieregularne i wykorzystanie do ich prowadzenia technologii informacyjnych, oraz prognostycznym – działania mające na celu zwalczanie nowoczesnych form nieregularności. Tematyka artykułu jest unikalna i epizodyczna, zważywszy, że problematyka ta nie została dotychczas dobrze poznana naukowo oraz opisana w literaturze przedmiotu. Ciągły rozwój technologii dostarcza stale nowych, twórczych rozwiązań stosowanych we wspomnianych działaniach.

Za cel niniejszego artykułu uznano zidentyfikowanie wpływu rozwoju technik informacyjnych na zmiany w obrębie prowadzenia i stosowania współczesnych form działań nieregularnych.

Tak sformułowany cel pracy można osiągnąć, rozwiązując główny problem badawczy sformułowany w postaci następującego pytania: Jak rozwój nowych technologii informacyjnych wpływa na współczesny kształt działań nieregularnych? Ze względu na scharakteryzowaną problematykę badań i określony złożony problem główny za zasadne uznano podzielenie go na problemy szczegółowe: Jak nowoczesne techniki w sferze informacyjnej wpływają na współczesne formy działań nieregularnych? Jak z wykorzystaniem sztucznej inteligencji możemy zwalczać współczesne formy działań nieregularnych?

Przy opracowaniu tematu pracy posłużono się analizą i syntezą dostępnych materiałów źródłowych, materiałów i opracowań naukowych, literatury obcojęzycznej oraz informacji zamieszczonych na stronach internetowych. Dokonano analizy pojęć, płaszczyzn oraz koncepcji walki w sferze informacji oraz jej wpływu na społeczeństwo. W artykule autorka wykazała rolę mediów społecznościowych w nowym podejściu do stosowania działań nieregularnych oraz zbadała zmiany, które zaszły w operacjach dezinformujących wykorzystujących nowoczesne technologie.

Teoria informacji

Trwająca obecnie na całym świecie rewolucja naukowo-informacyjna zmienia całkowicie najistotniejsze cele toczących się konfliktów. Rewolucja naukowo-informacyjna oznacza zdolność społeczeństw do produkcji, przetwarzania oraz rozpowszechniania i wdrażania informacji. Przełom ten ustala globalny charakter oraz cel gry we współczesnych konfliktach. Najważniejsze czynniki walki zostały zmienione z rywalizacji o zasoby materialne na zmagania o zasoby duchowe i intelektualne. Ludzka świadomość jest głównym przedmiotem walki. Obecnie wojny nie mają linii frontów, umysł człowieka stał się polem bitwy[1].

Określenie „informacja" zostało zaczerpnięte z łacińskiego „informatio" i oznacza ono wyjaśnienie, wyobrażenie, zawiadomienie. Istnieje wiele definicji informacji. Leopold Ciborowski uważa, że „informacja to bodziec oddziałujący na układ recepcyjny człowieka, powodujący wytwarzanie w jego wyobraźni przedmiotu myślowego. Odzwierciedlającego obraz rzeczy materialnej lub abstrakcyjnej, który w jego przekonaniu kojarzy się jakoś z tym bodźcem"[2]. Według Piotra Sienkiewicza informacja to „zbiór faktów, zdarzeń, cech, obiektów ujętych w takiej formie, że pozwala odbiorcy ustosunkować się do zaistniałej sytuacji i podjąć odpowiednie działania umysłowe lub fizyczne"[3]. Podmiot, który nawet w niewielkim stopniu nie jest w stanie operować informacją, analizować jej i na tej podstawie wyciągać wniosków, jest łatwym celem do wszelkiego rodzaju manipulacji, ale przede wszystkim staje się naturalnym celem dezinformacji ze strony infoagresorów[4].

Aktualnie informację uważa się za trzeci, fundamentalny element otaczającej nas realnej rzeczywistości zaraz obok energii i materii. Zarówno pojęcie, jak i powstała na jego skutek teoria informacji stały się ważnymi elementami współczesnej teorii poznania, urozmaiciły i wzbogaciły metody i sposoby badań naukowych[5]. Ryszard Czechowski oraz Piotr Sienkiewicz, naukowcy zajmujący się wpływem informacji na życie dzisiejszego społeczeństwa, w swojej książce stwierdzają, że „żyć i działać we współczesnym świecie to znaczy korzystać z informacji"[6].

1 T. Formicki, *Wywiad i kontrwywiad jako kluczowe komponenty walki informacyjnej*, Warszawa 2020, s. 11.
2 L. Ciborowski, *Walka informacyjna*, Toruń 1999, s. 50.
3 P. Sienkiewicz, *Systemy kierowania*, Warszawa 1989, s. 128.
4 T. Formicki, op. cit., s. 23–36.
5 Ibidem, s. 18.
6 R. Czechowski, P. Sienkiewicz, *Przestępcze oblicza komputerów*, Warszawa 1993, s. 120.

Współczesne poprzemysłowe społeczeństwo weszło w nowy etap – rewolucji naukowo-informacyjnej. Parafrazując Carla von Clausewitza, można stwierdzić, że obecnie to informacja jest „środkiem ciężkości”[7]. Informacja napędza rozwój każdej dziedziny życia, bez niej rozwój stanąłby w miejscu. Informacje dotyczące konkurencji, sytuacji w innym państwie dają organizacji terrorystycznej czy grupie przestępczej ogromną przewagę w podejmowaniu decyzji. Tego typu wiedza ma istotne znaczenie nie tylko w wymiarze cywilnym, lecz także w aspekcie bezpieczeństwa, to informacja wyznacza kierunek intensyfikacji stosunków międzynarodowych. O tym, kto dysponuje pierwszorzędnymi narzędziami wywierania wpływu na innych decydują: jakość, technika pozyskania oraz sposób ochrony informacji. Podmiot posiadający informacje staje na pozycji dominanta, przewagę nad resztą zyskuje podmiot, który szybciej ją zdobędzie[8].

Koncepcje oraz metody walki informacyjnej

Walkę informacyjną możemy nazwać charakterystycznym przypadkiem procesu sterowania społecznego. Celem takich działań jest niszczenie oponenta za pomocą informacji. Trzema głównymi obszarami walki informacyjnej są: cyberprzestrzeń, infosfera, czyli obszar szerszy od cyberprzestrzeni obejmujący systemy informacyjne, które nie wchodzą w skład sieci, oraz noosfera – obszar mentalności nie tylko pojedynczego człowieka, lecz także narodów i grup społecznych, i to właśnie noosfera społeczeństwa jest celem walki informacyjnej[9].

Do walki informacyjnej wykorzystuje się wiele narzędzi oraz metod w obszarze odziaływania ideologicznego ukierunkowanego na obszar kognitywny oponenta. Działania te są często określane mianem dywersji ideologicznej lub politycznej. Celem dywersji ideologicznej, politycznej jest zmniejszenie morale społeczeństwa, elity politycznej danego kraju lub służb mundurowych. W klasycznym ujęciu dywersja polega na skrytych działaniach za linią frontu, obiera za cel infrastrukturę krytyczną przeciwnika. W dywersji ideologicznej nie wykorzystuje się aktów terroru, wysadzania obiektów czy zabójstw, prowadzi

7 Termin ten został użyty do wyróżnienia składowych dających w danym czasie narodowi zasadniczą siłę. Według Clausewitza (*O wojnie. Podręcznik stratega*, Gliwice 2013) są to: armia, stolica, sojusznicy, jedność interesów, opinia publiczna, osobowość dowódców.
8 T. Formicki, op. cit., s. 12–13.
9 Ibidem, s. 101–102.

się długoletnie „zatruwanie" wrogiego społeczeństwa. Istotnym elementem prowadzenia działań informacyjnych o charakterze dywersji ideologicznej jest dezintegracja społeczeństwa, opinii publicznej, w czego wyniku możliwe jest kontrolowanie większości poprzez dobrze zdyscyplinowaną, zorganizowaną, a także zdeterminowaną mniejszość[10]. Skuteczna strategia walki informacyjnej jest oparta na analizie, która jest poprzedzona zgłębieniem historii oraz kultury pozwalającej na określenie mocnych i słabych stron podmiotu informacyjnego wpływu. Ważnym elementem jest długookresowa analiza schematu edukacji oraz wychowania danego społeczeństwa, przyswajania wzorów postępowania w wymiarze państwowym. Walka informacyjna może stanowić element przygotowań do prowadzenia klasycznej operacji wojskowej, a nawet klasycznej wojny. Może być również składnikiem działań nieregularnych, łączyć konwencjonalne działania zbrojne z operacjami nieregularnymi przeprowadzanymi przez cywilów. Przede wszystkim walka informacyjna może stanowić samoistny element polityki państwowej ukierunkowanej na osiąganie politycznego lub gospodarczego punktu docelowego bez użycia bezpośredniej siły fizycznej[11].

Jurij Bezmienow, współpracownik radzieckich służb specjalnych, po dezercji do Ameryki Północnej w liście do Amerykanów[12] opisał m.in. etapy działalności wywrotowej. Jest to tak długotrwały proces, że przeciętna jednostka, biorąc pod uwagę krótki przedział czasowy, który jest dostępny jej pamięci historycznej, nie jest zdolna do uważania działań dywersyjnych za wysiłki przemyślane i konsekwentne. Wyróżnił on cztery etapy działalności wywrotowej[13]. Demoralizacja – zajmuje od 15 do 20 lat, jest ukierunkowana na podważenie tradycyjnych wartości, przerwanie więzów społecznych, polaryzację społeczeństwa, ale również podważenie zaufania do państwa, jego autorytetu oraz symboli narodowych czy religijnych. Etap ten jest niezbędny do wprowadzenia drugiego okresu, czyli destabilizacji. Etap ten to czas powszechnych strajków, protestów, tworzenia alternatywnych rządów, instytucji państwowych. Destabilizacja trwa z reguły od 2 do 5 lat. Następny etap – kryzys – trwa od 2 do 6 miesięcy, jest kojarzony z przesileniem, wojną domową. Ostatni etap, normalizacja, np. interwencja zbrojna. Przykładem takiej operacji może być kryzys krymski, który bez

10 L. Sykulski, *Rosyjska geopolityka a wojna informacyjna*, Warszawa 2019, s. 86–87.
11 Ibidem, s. 88.
12 T. Schuman (J. Bezmienow), *Love Letter to America*, Los Angeles 1984.
13 Idem, *Agentura wpływu. Tajniki działalności wywrotowej KGB*, Kraków 2020, s. 50–51.

okresu demoralizacji i destabilizacji, dokładnie opisany przez Bezmienowa, nie miałby powodzenia[14].

Wszechobecne mobilne, elektroniczne urządzenia, a także Internet wywróciły metody działań dywersanta, co więcej dostarczyły nowych być może skuteczniejszych metod działania. Bez względu na to, czy nacisk i propaganda odbywają się w prasie czy z wykorzystaniem mediów społecznościowych, nie ma również znaczenia, czy materiały propagandowe rozpowszechniane są za pomocą skrzynek pocztowych czy e-maila, najważniejszy jest efekt, czyli przekazanie jak największej liczbie osób treści korzystnych z punktu widzenia dywersanta[15].

Płaszczyzny walki informacyjnej

Siergiej Modiestow, definiując wojnę informacyjną, wziął pod uwagę czynniki geopolityczne. Jego zdaniem celem wojny informacyjnej jest osiągnięcie oraz utrzymywanie przewagi informacyjnej przez wywieranie konkretnego informacyjno-psychologicznego oraz informacyjno-technicznego wpływu na państwowe systemy decyzyjne. Określił on dwie płaszczyzny działań informacyjnych – psychologiczną oraz cybernetyczną[16]. Dzięki rewolucji naukowo-technicznej doszło do połączenia komputerów i telekomunikacji, a wynikiem tego jest powstanie zintegrowanych sieci systemów. Nie tylko pojedyncze jednostki, lecz także organizacje społeczne tudzież środowiskowe zauważyły potencjał sieci, który polega na dynamicznej społecznej interakcji. Dostrzeżono siłę połączonej energii ludzkich działań, która za pośrednictwem sieci jest w stanie zakwestionować aktualny ład polityczny, a nawet doprowadzić do upadku panującą władzę. Naukowcy z RAND Corporation zjawisko to nazwali wojną sieciową (*netwar*), nadali mu miano modelu konfliktu społecznego charakterystycznego dla obecnej epoki[17].

Sfera psychologiczna to wcześniej wspomniana noosfera (od greckiego słowa *noos*, czyli umysł). Jest to płaszczyzna mentalna, kognitywna, która odpowiada za światy zarówno wewnętrzny, jak i zewnętrzny. Można tutaj mówić

14 L. Sykulski, *Recenzja #13: Jurij Bezmienow. Agentura wpływu|Odc. 160 – dr Leszek Sykulski*, https://www.youtube.com/watch?v=clH2hU7uKks [dostęp: 7.09.2021].
15 J. Bezmienow, *Agentura*..., s. 13.
16 L. Sykulski, *Rosyjska*..., s. 84.
17 T. Formicki, op. cit., s. 185.

o obrazie świata w umyśle pojedynczego człowieka, ale także szerzej, np. o grupie społecznej, narodzie czy państwie. Walka ukierunkowana na tę sferę może się odbywać z wykorzystaniem takich klasycznych narzędzi, jak wpływ na społeczeństwo liderów opinii tradycyjnymi kanałami, np. poprzez wykłady, audycje radiowe, artykuły w prasie, ale także z wykorzystaniem nowocześniejszych narzędzi oferowanych dzięki Web 2.0, za pomocą serwisów generujących treści przez samych ich użytkowników bądź wykorzystujących sztuczną inteligencje[18].

Przestrzenią łączącą noosferę i świat fizyczny jest cyberprzestrzeń, wirtualny świat, który został stworzony z wykorzystaniem teleinformatycznych narzędzi. Internet – globalna sieć, współcześnie jest głównym generatorem świata wirtualnego, cyberprzestrzeń zaś staje się coraz istotniejszą płaszczyzną informacyjnego oddziaływania niż przestrzeń fizyczna. Umożliwia ona nie tylko psychologiczne oddziaływanie na noosferę, lecz także fizyczne ataki, których celem jest infrastruktura krytyczna oponenta, doprowadzając w ten sposób do sparaliżowania systemu dowodzenia oraz kierowania. Walka w tej przestrzeni obejmuje nie tylko oddziaływanie na mentalność przeciwnika, lecz także fizyczne ataki w sieci i poza nią. Celuje w infrastrukturę pozwalającą na przesyłanie informacji oraz działanie sieci, np. serwery lub światłowody. Walka informacyjna to nie tylko sfera cywilna, lecz także różnego rodzaju wojskowe narzędzia walki elektronicznej umożliwiające zakłócenie działań technicznych przeciwnika z wykorzystaniem emisji elektromagnetycznej, to także obszar powiązany z kryptologią[19]. Sieć stała się instrumentem polityki wykorzystywanym do narzucenia woli, a nawet zaprowadzenia nowego porządku. Zdolność tkwiącą w sieci obecnie skutecznie wykorzystują w walce jednostki, ale i różne organizacje zarówno charytatywne, biznesowe, jak i ugrupowania przestępcze i terrorystyczne oraz ruchy ideologiczne i religijne oraz grupy narodowe i etniczne. W dobie globalizmu informacyjnego jakikolwiek podmiot może zostać uzbrojony w środki ogólnoświatowego oddziaływania. Po uzyskaniu dostępu do informacji i osiągnięciu zdolności rozpowszechniania ich wśród innych podmiotów może zostać aktywnym aktorem międzynarodowej areny politycznej, kiedyś zarezerwowanej wyłącznie dla państw. Biorąc pod uwagę taką możliwość, wojna sieciowa może stać się konfliktem między państwem a niepaństwowym podmiotem wykorzystującym teren państwa

18 L. Sykulski, *Rosyjska…*, s. 85.
19 Ibidem, s. 85–86.

do swoich działań bądź państwem, które uznało niepaństwowego aktora za swojego pomocnika. Modelowym przykładem takich działań może być wojna izraelsko-libańska, podczas której doszło do konfliktu Izraela z niepaństwowa strukturą, Hezbollahem, wspieraną przez Syrię oraz Iran na ziemiach należących do Libanu. Wysiłki wykorzystane do walki mogą być skoncentrowane np. na kształtowaniu opinii publicznej lub działaniach grup opiniotwórczych. Mogą być wykorzystywane prawne środki dyplomatyczne, a także propaganda, kampanie psychologiczne, oszustwa bądź różnego rodzaju działalność wywrotowa. Można stwarzać zakłócenia w lokalnych mediach, infiltrować bazy danych i sieci komputerowe oraz popierać ruch oporu[20].

Rozwój technologiczny sektora urządzeń komunikacyjnych spowodował, że współcześnie ludność cywilna nie jest już tylko biernym obserwatorem sytuacji, ale staje się uczestnikiem i podmiotem wydarzeń, np. poprzez swoją aktywność w mediach społecznościowych. Biorąc to pod uwagę, służby wywiadowcze państw, ale i grup przestępczych lub terrorystycznych interesują się kondycją moralno-psychiczną społeczeństwa kraju, który stał się celem. Współcześnie, gdy konflikty mają inny charakter, przekształcają się w działania hybrydowe. Bardzo ważnym elementem bezpieczeństwa narodowego jest ochrona własnych aktywów informacyjnych, w tym sfery psychologicznej[21].

Dezinformacja jako element walki informacyjnej

Integralnym elementem walki informacyjnej jest dezinformacja, która ma na celu ukazanie oponentowi zafałszowanego obrazu rzeczywistości. Działania dezinformacyjne są ukierunkowane na procesy decyzyjne adresata działań zgodnie z wolą strony atakującej. Za atrybut procesu dezinformującego można uznać jego realizację w sposób usystematyzowany oraz kompleksowy, w stosunku do obiektu oddziaływania w formie osobowej, ale i w technicznej przestrzeni informacyjnej. Niezwykle istotnym czynnikiem w dezinformacji jest posiadanie wiedzy o przeciwniku, zarówno o jego słabych, jak i silnych stronach, a także o narzędziach wykorzystywanych przez niego w walce informacyjnej. Najbardziej podatne na dezinformację są: ludzki umysł, źródła i zasoby informacyjne przeciwnika i własne oraz mentalność narodu. Wiedza pozyskana na

20 T. Formicki, op. cit., s. 186–187.
21 Ibidem, s. 1312.

te tematy pozwala precyzyjnie skierować działania dezinformacyjne zgodnie z oczekiwaniami atakującego. Najważniejszy w dezinformacji jest człowiek, ponieważ w jego umyśle kształtują się procesy odpowiedzialne za postrzeganie czy określanie zjawisk oraz wydarzeń, które nie mają potwierdzenia w rzeczywistości, gdy człowiek zostanie dotknięty dezinformacją w jego świadomości powstaje swego rodzaju iluzja. Demokratyzacja życia społecznego oraz powstanie prywatnych środków masowego przekazu, głównie mediów elektronicznych, umożliwiły realizację działań dezinformacyjnych na większą skalę[22].

Przykłady wykorzystania dezinformacji przez ISIS

Jedną z grup terrorystycznych, która posiada rozbudowaną i dobrze działającą komórkę propagandową, było i jest tzw. Państwo Islamskie. Jego działalność propagandowa nie funkcjonowała w próżni. Istnienie idei oraz narracji jest konieczne do skutecznego zwiększenia odbioru. Taki zbiór został określony przez Wintera jako prepropaganda. W przypadku tzw. Państwa Islamskiego są to informacje, które odbiorca przekazu propagandowego pragnie przyswoić w sposób świadomy bądź nieświadomy. Gdy zostaną dokonane zmiany w światopoglądzie odbiorcy, wówczas może on zostać w pełni zaabsorbowany, a nawet uzależniony[23]. Propaganda ISIS w takim ujęciu jest ukierunkowana na wzmocnienie, krystalizację istniejących idei, a nie zaszczepienie ich w adresatach[24]. Jedną z podstawowych różnic między strategią propagandowa ISIS a pozostałych grup dżihadystycznych jest „[...] aksjologiczna dysocjacja przekazu medialnego związana z dokumentowaniem działań godzących we wszelkie fundamentalne, także dla muzułmanów wartości”[25]. Zabójstwa cudzoziemców i innowierców oraz np. palenie żywcem muzułmanów za przejaw barbarzyństwa uznał m.in. Nasr ibn Ali-al-Ansi, rzecznik Al-Kaidy na Półwyspie Arabskim.

Działalność propagandowa ISIS była szczególnie mocno rozwinięta w wirtualnym świecie. Mimo że Internet był wykorzystywany przez bojowników różnych organizacji na długo przed powstaniem kalifatu, członkowie

22 Ibidem, s. 957–958.
23 Ch. Winter, *The Virtual „Caliphate: Understanding Islamic State's Propaganda Strategy*, Quilliam 2015, s. 12.
24 M. Dąbrowska, P. Rybiński, *Dezinformacja jako narzędzie kreowania wizerunku*, cz. 1, *Działalność medialna ISIS*, „Zeszyty Naukowe ASzWoj” 2017, nr 4, s. 27–28.
25 A. Wejkszner, *Państwo Islamskie: narodziny nowego kalifatu*, Warszawa 2016, s. 134.

organizacji swoje umiejętności propagandowe doskonalili przez około 10 lat. Najlepszym tego dowodem jest pojawienie się pojęcia „e-dżihad". Materiały zamieszczane przez ISIS wyróżniają się przede wszystkim wysokim poziomem jakości, atrakcyjnością, ale i wykorzystaniem zaawansowanej technologii. Organizacja ta stara się tworzyć swoje materiały na wzór zachodni. Jednym z głównych celów oficjalnych mediów tzw. Państwa Islamskiego jest zapewnianie treści na tyle atrakcyjnych, żeby zwerbować nowych członków, dlatego organizacja opublikowała kilka przewodników, m.in. kierowanych do „samotnych wilków". Poradniki te są niezwykle szczegółowe, opisują jak w bezpieczny sposób dostać się do kalifatu, z kim się kontaktować w tym celu, dołączona jest cała lista kont na Twitterze, co zabrać ze sobą, wybierając się do tzw. Państwa Islamskiego. Poradniki te wzbogacone są o dużą liczbę map oraz zdjęć, np. do wniosku o wizę do Turcji, ponieważ – według ich autorów – to przez Turcję można było się przedostać bezpiecznie. ISIS starało się również uatrakcyjnić przekaz, szczególnie ten w języku angielskim, który był skierowany do przyszłych zachodnich bojowników. Filmy propagandowe były tworzone w jakości HD, np. mini serial „Mujatweets" prezentujący realia życia w kalifacie. Często publikowane wideo przypomina wstęp do gry komputerowej, a potencjalnym członkom gwarantuje się „[...] niesamowitą, prawdziwą męską przygodę". Tak zwane Państwo Islamskie publikuje również pieśni – latem 2016 roku powstała ich spora liczba, które nawiązywały do ataków terrorystycznych mających miejsce w Europie. Charakterystyczne dla nowych mediów są memy, ISIS publikowało je w znacznej ilości. Znany był również hashtag #CatsOfIjhad, publikowane były tam urocze zdjęcia kotów w celu nie tylko zwrócenie uwagi nowych odbiorców na publikowane treści, ale także pokazanie zwyczajnego życia w kalifacie[26].

Media społecznościowe narzędziem w rękach terrorystów

Internet i serwisy społecznościowe umożliwiły na większą skalę realizację działań wyznaczonych przez terrorystów. Z jednej strony Internet ułatwił oraz przyspieszył komunikację wśród zwolenników, uprościł koordynację zadań między wybranymi członkami grupy często rozmieszczonymi po

26 A. Zielińska, *Rynek medialny ISIS*, „Refleksje. Pismo Naukowe Studentów i Doktorantów WNPID UAM" 2019, nr 19–20, s. 174–180.

całym świecie. Z drugiej strony, media społecznościowe oraz różnego rodzaju komunikatory internetowe dały grupom terrorystycznym możliwość relacjonowania w czasie rzeczywistym swoich działań, ale i prowadzenie długotrwałych kampanii oddziaływania w sferze informacji – działań propagandowych. Obserwując działania informacyjne tzw. Państwa Islamskiego lub Hezbollahu, można zauważyć, że organizacje te nie prowadzą działań, a to, co robią wręcz można nazwać wojną w cyberprzestrzeni. Jednocześnie nie koncentrują się tylko na kwestiach zastraszania społeczeństw, ale również na pozyskaniu zwolenników, „żołnierzy", którzy są gotowi przybyć na kontrolowane tereny lub podjąć działania w roli „samotnych wilków". Jednym z przykładów negatywnego wykorzystania mediów społecznościowych przez bojowników jest wcześniej wspomniana możliwość bezpośredniego emitowania swoich działań w czasie rzeczywistym. Zamach, który został przeprowadzony w marcu 2019 roku w Christchurch, drugim co do wielkości mieście w Nowej Zelandii, jest przykładem negatywnego wykorzystania serwisów społecznościowych. Za pośrednictwem portalu Facebook prawicowy ekstremista przez około 17 minut transmitował w czasie rzeczywistym przebieg ataku, w którym śmierć poniosło 51 osób. Pierwszy komunikat o szkodliwości nagrania portal otrzymał po 29 minutach od rozpoczęcia transmisji. Zanim zostało ono usunięte, widziano je już 4 tys. razy. Po usunięciu nagrania były podejmowane próby ponownego wgrania filmu. Przez pierwsze 24 godziny od zamachu podjęto 1,5 mln prób, 1,2 mln prób zablokowano w momencie wgrywania. Pomimo całkowitego usunięcia filmu jest on wciąż dostępny w sieci za pośrednictwem innych stron[27].

Wraz z rozwojem kryptowalut organizacje terrorystyczne zaczęły je wykorzystywać w swojej działalności. Ich przepływ jest trudniejszy do namierzenia niż tradycyjnych środków finansowych. Problemem wykorzystania kryptowalut zainteresował się m.in. RAND Corporation. Wskazał on możliwość pozyskania środków od darczyńców, ale i finansowania ataków terrorystycznych przez zakup niezbędnych materiałów. W 2019 roku została wykryta działalność mająca na celu pozyskiwanie środków finansowych z wykorzystaniem technologii blockchain przez podmiot zależny od Hamasu. Grupa ta, wykorzystując Telegram oraz Facebooka, zachęcała do przekazywania darowizn właśnie w kryptowalutach na działalność organizacji[28]. Hamas, wykorzystując ser-

27 A.K. Olech, A. Lis, *Technologia i terroryzm. Sztuczna inteligencja w dobie zagrożeń terrorystycznych*, Warszawa 2021, s. 113–115.

28 E. Azani, M. Barak, E. Landau, N. Liv, *Identifying Money Transfers and Terror Finance Infrastructure*, Herzliya 2020.

wisy społecznościowe, wchodził w interakcje z członkami izraelskiego wojska z pomocą fikcyjnych profili. Po zdobyciu zaufania przesyłano złośliwe oprogramowanie, które umożliwiało przejęcie urządzenia ofiary. Nie był to jedyny przykład takich działań. Próbowano także kontaktować się z żołnierzami za pomocom komunikatorów internetowych, żeby pozyskać informacje o działalności armii. Z przytoczonych przykładów wynika, że działania informacyjne przekładają się na bezpieczeństwo i porządek publiczny poprzez oddziaływanie na opinię publiczną lub nastroje społeczne[29].

Twitter ważnym narzędziem działań nieregularnych

Według badań przeprowadzonych przez trzech naukowców z Massachusetts Institute of Technology (MIT) fałszywe wiadomości rozprzestrzeniają się znacznie szybciej na platformie społecznościowej Twitter niż prawdziwe. W celu przeprowadzenia badania prześledzono około 126 tys. kaskad wiadomości rozpowszechnianych za pomocą tej strony, które to wiadomości zostały opublikowane ponad 4,5 mln razy przez około 3 mln użytkowników Twittera między 2006 a 2017 rokiem. Spośród wszystkich zbadanych wiadomości polityka stanowiła największą kategorię, okazało się, że to właśnie fake newsy polityczne są najczęściej powielane. Następnymi kategoriami były wszelkiego rodzaju miejskie legendy, biznes, terroryzm, nauka, rozrywka oraz katastrofy naturalne. Istotnym wynikiem badań jest to, że prawdopodobieństwo retweetowania fałszywej wiadomości jest o 70% większe niż tej prawdziwej, prawda potrzebuje przeciętnie 6 razy więcej czasu niż informacja fałszywa, żeby dotrzeć do 1500 użytkowników na Twitterze[30].

Bojownicy tzw. Państwa Islamskiego, rozpowszechniając propagandę, używali głównie mediów społecznościowych, w szczególności Twittera. W 2014 roku na Twitterze było szacunkowo 45 tys. kont działających w celach propagandowych, a w 2015 roku już około 90 tys. Największa ich liczba, aż około 69%, była zarejestrowana na Bliskim Wschodzie, głównie w Arabii Saudyjskiej, Iraku oraz Syrii, znaczna zaś część postów zamieszczanych przez tych użytkowników była w języku angielskim. Z danych Europolu wynika, że kont na

29 A.K. Olech, A. Lis, op. cit., s. 116–117.

30 P. Dizikes, *Study: On Twitter, false news travels faster than true stories*, MIT News Office, March 2018, https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308 [dostęp: 5.09.2021].

Twitterze zaangażowanych w propagandę na rzecz ISIS było od około 45 do 50 tys., a każde z nich śledziło przeciętnie więcej niż tysiąc osób. Nie bez przyczyny ISIS zostało nazwane przez administracje Obamy „publicity machine", zwolennicy bowiem tzw. Państwa Islamskiego publikowali około 90 tys. postów dziennie. Taka częstotliwość sprawiła, że Twitter i inne media społecznościowe stale próbują wykrywać oraz blokować kampanie propagandowe szerzące się przez ich platformy, mimo to sprzyjają one grupom terrorystycznym, które używają mediów społecznościowych do rekrutacji nowych członków z zachodnich społeczeństw. Gdy Twitter zablokuje jedno konto, automatycznie pojawiają się kolejne[31]. W 2014 roku bojownicy tzw. Państwa Islamskiego wdarli się do północnego Iraku. Nie ukrywali tej operacji, wręcz przeciwnie, rozpowszechniali wydarzenie z wykorzystaniem Twittera. Wysyłali ogromną liczbę postów z dołączonymi zdjęciami bojowników bądź konwojów. W celu zwiększenia szansy na upowszechnienie wydarzenia z wykorzystaniem algorytmów strony stworzono hashtag #AllEyesOnISIS. Osiągnął on swój cel i po niedługim czasie stał się przodującym hasztagiem na arabskim Twitterze, docierał także do obrońców oraz mieszkańców miast będących celem ISIS. Żądania stawiane przez terrorystów bardzo szybko się rozprzestrzeniały, a filmy wideo przez nich nakręcone, które pokazywały tortury i egzekucje na przeciwnikach grupy terrorystycznej, były dostępne bez ograniczeń na portalu społecznościowym. Z chwilą opublikowania filmów #AllEyesOnISIS osiągnął zaplanowany cel, tj. wywołanie i spotęgowanie przerażenia i woli ucieczki społeczności miast wybranych za cel przez ISIS. Ważnym celem dla tzw. Państwa Islamskiego był Mosul, wielokulturowa metropolia, która liczy 3 tys. lat, zamieszkana przez 1,8 mln ludzi. Gdy zbliżała się inwazja ISIS na Mosul, #AllEyesOnISIS był już powszechnie znany, dlatego mieszkańców ogarnął strach. Armia iracka była gotowa bronić miasta, lecz z liczącego 25 tys. żołnierzy garnizonu spora liczba albo zdezerterował, albo została wymyślona przez skorumpowanych oficerów. Dziesięciotysięczna armia, która pozostała, mogła obserwować na swoich telefonach poczynania wrogów. Podczas śledzenia hashtagu pojawiało się pytanie: walczyć czy uciekać. Wcześniej, przed przybyciem najeźdźców, pojawił się strach. Wśród mieszkańców także panował strach, z miasta uciekło około 500 tys. cywili. Gdy w mieści pojawili się bojownicy w sile 1500 osób, na miejscu była nieliczna grupa żołnierzy i policjantów. Bez trudu zostali oni pokonani, a masakra, która miała tam miejsce, została dokładnie sfilmowana,

31 A. Zielińska, op. cit., s. 171.

a następnie rozpowszechniona w sieci. Tak zwane Państwo Islamski przyczyniło się do zapoczątkowania nowego rodzaju wojny błyskawicznej wykorzystującej Internet jako broń. Nagły upadek Mosulu pokazał jeszcze jedno oblicze skomputeryzowanej wojny. Bojownicy ISIS nie posiadają rzeczywistych zdolności do prowadzenia cyberwojny, poprowadzili militarną ofensywę na wzór powszechnej kampanii marketingowej i odnieśli niemal niemożliwe zwycięstwo. Nie włamywali się oni do sieci w celu wykorzystania dostępnych tam danych, ale zamieszczali posty w serwisach społecznościowych. W kolejnych miesiącach bojownicy zwerbowali ponad 30 tys. obcokrajowców z prawie 100 krajów. Odbudowana armia iracka, gdy ponownie wkroczyła do Mosulu, dysponowała już przenośnymi nadajnikami umożliwiającymi wymianę własnych informacji, ale przede wszystkim wojsko irackie uruchomiło kanały informacji na Facebooku, YouTube oraz Twitterze, przekazywali tam informacje dotyczące stanu operacji i różnego rodzaju zdjęcia, np. swoich żołnierzy wysadzających ciężarówki pułapki pozostawione przez tzw. Państwo Islamskie. Iracka operacja również miała własny hashtag, pod którym zamieszczane były posty, nazywał się on #FreeMosul. Niektórzy z użytkowników Internetu angażowali się w konflikt w sposób pozytywny. Przeglądali Internet w poszukiwaniu informacji o rannych cywilach, a następnie starali się tam wysłać ratowników medycznych z miejscowych szpitali. Jedno z takich kont – @MosulEye – było kierowane przez mieszkańca Iraku, który działał za liniami ISIS na rzecz pokoju oraz starał się odwrócić technikę, dzięki której tzw. Państwo Islamskie za pierwszym razem zdobyło miasto. Powstała ogromna sieć ochotników wykorzystujących media społecznościowe do ratowania ludzkich istnień[32].

Pewne elementy działań informacyjnych można było wyraźnie zaobserwować także podczas arabskiej wiosny w 2011 roku. Uczestnicy protestów w Kairze porozumiewali się ze sobą z wykorzystaniem mediów społecznościowych nie tylko w Internecie. Gdy władze zablokowały dostęp do sieci, korzystali z narzędzia „Speak to Tweet". Umożliwia ono połączenie poprzez telefon komórkowy z pocztą głosową oraz pozostawienie na niej wiadomości, która następnie jest automatycznie zamieszczana na Twitterze i oznaczona tagiem kraju, z którego pochodzi. Aplikacja umożliwia również odsłuchanie postów zamieszczanych na Twitterze[33]. Serwisy społecznościowe zmieniły zarówno

32 P.W. Singer, E.T. Brooking, *Nowy rodzaj wojny. Media społecznościowe jako broń*, Kraków 2019, s. 12–21.

33 K. Liedel, P. Piasecka, T.R. Aleksandrowicz, *Analiza informacji. Teoria i praktyka*, Warszawa 2012, s. 23–24.

przesłanie, jak i dynamikę konfliktu. Nowy wymiar zyskał również sposób rozpowszechniania i docierania do informacji. Przekształceniu uległo niemal wszystko – kto uczestniczył w walkach, gdzie się znajdował, a nawet to, w jaki sposób odniósł zwycięstwo[34].

Sztuczna inteligencja w walce z dezinformacją

Z punktu widzenia operacji sił specjalnych dostarczenie rzetelnej informacji lokalnej społeczności jest niezwykle istotne, ponadto często decyduje zarówno o pomyślności misji, jak i potencjalnej śmierci. Z tego powodu walka w sferze informacyjnej jest niezwykle ważna, a wojsko musi być dobrze do niej przygotowane[35].

Special Operations Command (SOCOM) wraz z Air Force podpisały kontrakt z firmą Primer, która zajmuje się tworzeniem rozwiązań wykorzystujących sztuczną inteligencję i uczenie maszynowe. Wynikiem tej współpracy będzie pierwsza platforma stosująca uczenie maszynowe do identyfikacji i oceny treści pod względem dezinformacji. Nowe podejście, które ma na celu rozwijanie naturalnego języka przez pracowników Primera, ma przynieść oczekiwane rezultaty. Firma w komunikacie prasowym podkreślała, jakim wyzwaniem dla wojska jest przeciążenie informacją. Każdego dnia jest tworzone 2,5 kwintyliona bajtów nowych danych. Dodatkowym utrudnieniem jest to, że analitycy muszą zmierzyć się z coraz większą liczbą zmanipulowanych oraz fałszywych informacji. Rozwiązanie firmy Primer ma pisać i czytać w kilku językach: angielskim, rosyjskim, chińskim, oraz być zdolne do automatycznego zidentyfikowania głównych trendów oraz najważniejszych elementów przetwarzanych wolumenów danych, bazując na popularności oraz częstotliwości ukazywania się danych słów i fraz. Takie rozwiązanie może być niezwykle przydatne w razie wystąpienia szybkiej konieczności syntezy długiego tekstu, ta nowa technologia sprawi, że będzie możliwe czytanie oraz wynajdywanie informacji automatycznie, tak, żeby zwiększyć szybkość oraz jakość podejmowanej decyzji w czasie rzeczywistym. Twórcy tego projektu są świadomi, że nauczenie platformy odróżniać prawdę od fikcji będzie długim procesem. Napisanie

34 P.W. Singer, E.T. Brooking, op. cit., s. 21.

35 A. Kozłowski, *US Special Forces vs dezinformacja. Czy sztuczna inteligencja przechyli szalę zwycięstwa?*, https://cyberdefence24.pl/us-special-forces-vs-dezinformacja-czy-sztuczna-inteligencja-przechyli-szale-zwyciestwa [dostęp: 12.09.2021].

nagłówków czy streszczenie artykułu jest stosunkowo proste, inaczej jest ze stwierdzeniem, co jest treścią dezinformującą. Autorzy oprogramowania jego trening porównują do procesu uczenia się dziecka. Oprogramowanie ma rozpoznawać wiadomości z zaufanych źródeł oraz identyfikować te pochodzące od podmiotów mało wiarygodnych. Proces ten wymaga czasu, niesamowitej ilości danych, ćwiczeń i stałej kontroli. Trudno jest również jednoznacznie zdefiniować wiarygodne źródła, często nawet oficjalne komunikaty rządów czy informacje podawane przez renomowane media zawierają dezinformacyjne treści. W tej sytuacji producenci platformy liczą na SOCOM i Air Force, które będą podawać te najbardziej wiarygodne źródła informacji wykorzystywane w codziennej pracy. Wkład żołnierzy pozwoli platformie stwierdzić, czy dane informacje są wiarygodne czy też nie bazują w szczególności na źródle pochodzenia informacji[36].

Prezentacja dotychczasowych możliwości platformy odbyła się z wykorzystaniem konfliktu pomiędzy Armenią i Azerbejdżanem. Ta nowoczesna technologia była w stanie znaleźć posty, źródła oraz wiadomości w mediach społecznościowych dotyczące konfliktu, pogrupować je, a następnie wskazać m.in. co konkretna strona mówi o danym wydarzeniu, np. o nalocie. Dzięki temu można było zorientować się jaka jest opinia danej grupy lub strony zaangażowanej w konflikt. W obecnej fazie platforma nie była w stanie poradzić sobie z wykryciem prawdy bądź treści fałszywej, funkcja ta pojawi się wraz z rozwojem tej technologii[37].

Program Semantic Forensics (SemaFor) ma na celu opracowanie technologii, które sprawią, że automatyczne wykrywanie, przypisywanie i charakteryzowanie sfałszowanych zasobów medialnych stanie się rzeczywistością. Celem tego programu jest opracowanie zestawu algorytmów analizy semantycznej, które radykalnie zwiększą obciążenie twórców sfałszowanych mediów, utrudnią im tworzenie atrakcyjnych, zmanipulowanych treści, które pozostaną niewykryte. Program SemaFor stworzy narzędzia, które używane razem mogą pomóc w identyfikacji, powstrzymaniu i zrozumieniu sfałszowanych medialnych wiadomości. SemaFor skupi się na trzech konkretnych typach algorytmów: semantycznego wykrywania, przypisywania i charakteryzacji. Algorytmy semantyczne określą, czy multimodalne zasoby medialne zostały wygenerowane lub zmanipulowane, podczas gdy algorytmy przypisywania wywnioskują,

36 Ibidem.
37 Ibidem.

czy media pochodzą od rzekomej organizacji lub osoby. Określenie, w jaki sposób i przez kogo zostały stworzone media, może pomóc w określeniu większych motywacji lub przesłanek ich stworzenia, a także zestawu umiejętności, którymi dysponuje fałszerz. Algorytmy charakteryzujące będą wnioskować, czy media wielomodalne zostały wygenerowane lub zmanipulowane w złych celach. Algorytmy opracowane przez SemaFor pomogą analitykom automatycznie zidentyfikować i zrozumieć media, które zostały sfałszowane w złych celach. Opracuje on także technologie, które pozwolą analitykom na bardziej efektywne przeglądanie i ustalanie priorytetów zmanipulowanych zasobów medialnych. Obejmuje to metody integracji ocen ilościowych dostarczanych przez algorytmy wykrywania, przypisywania i charakterystyki w celu nadania priorytetu mediom automatycznym do przeglądu i reakcji. W celu zapewnienia analitykom zrozumiałych wyjaśnień SemaFor opracuje również technologie automatycznego gromadzenia i przechowywania dowodów dostarczonych przez algorytmy wykrywania, przypisywania i charakteryzacji. Przez cały okres trwania programu technologie SemaFor będą oceniane w odniesieniu do coraz trudniejszych problemów, które są reprezentatywne dla nowych lub pojawiających się scenariuszy zagrożeń[38].

DARPA ogłosiła zespoły badawcze, które zostały wybrane do realizacji celów programu SemaFor. Zespoły zarówno z firm komercyjnych, jak i ośrodków akademickich będą pracować nad stworzeniem algorytmów wykorzystywanych do analizy zdolnych do zautomatyzowanej identyfikacji fałszywych przekazów. Cztery zespoły badawcze skoncentrują się na opracowaniu wyżej wymienionych algorytmów. Kierowane będą przez Kitware Inc, Purdue University, SRI International oraz University of California, Berkeley. Naukowcy pracują również nad scharakteryzowaniem środowiska zagrożeń oraz opracowaniem problemów na podstawie przypuszczalnych działań przeciwnika. Współpracują oni z Accenture Federal Services (AFS), Google/Carahsoft, New York University (NYU), NVIDIA, and Systems & Technology Research. Google, wykorzystując duże platformy internetowe, przedstawi możliwe zagrożenia związane z dezinformacją, NVIDIA dostarczy algorytmy generowania mediów oraz koncepcję dotyczącą potencjalnego wpływu nadchodzących technologii sprzętowych na jakość przekazywanych informacji, NYU – zapewnia współpracę z NYC Media Lab i szerokim ekosystemem medialnym, który zagwarantuje

38 *Uncovering the Who, Why, and How Behind Manipulated Media*, https://www.darpa.mil/news-events/2019-09 [dostęp: 15.09.2021].

wgląd w ewoluujące środowisko medialne oraz zaprezentuje sposób wykorzystania ich przez złośliwych manipulatorów. Ponadto AFS zapewnia ocenę operacyjności SemaFor w zastosowaniu do Globalnego Centrum Zaangażowania Departamentu Stanu, który przejął inicjatywę w zwalczaniu zamorskiej dezinformacji. Żeby upewnić się, że opracowywane narzędzia i algorytmy mają wystarczającą ilość odpowiednich danych szkoleniowych, naukowcy z PAR Government Systems zostali wybrani do kierowania działaniami w zakresie gromadzenia danych i oceny programu. Zespół PAR będzie odpowiedzialny za przeprowadzanie regularnych, zakrojonych na szeroką skalę testów, które będą mierzyć wydajność oraz możliwości rozwijanej platformy[39].

Zakończenie

W wyniku postępu technologicznego, który dokonał się w ostatnich latach, zmieniły się diametralnie formy działań nieregularnych. Przede wszystkim stały się bardziej powszechne ze względu na wykorzystanie mediów społecznościowych. Z badań, których wyniki zamieszczono w artykule, wynika, że fałszywe informacje rozprzestrzeniają się znacznie szybciej niż prawdziwe, co znacznie ułatwia prowadzenie operacji dezinformacyjnych w cyberprzestrzeni.

Trwające oraz minione konflikty zbrojne pokazały, że dla wszystkich służb odpowiedzialnych za bezpieczeństwo kwestią najważniejszą jest jakość i odpowiednio duża przewaga w zdobywaniu informacji wywiadowczych, a jeszcze ważniejsze jest odpowiednie przygotowanie przy ich wykorzystaniu neutralizacji występujących zagrożeń. Krzywdzące dla sił specjalnych jest postrzeganie przez opinię publiczną nieefektywności w identyfikacji przez te służby zagrożeń, jest to wynikiem ograniczeń społeczeństwa w dostępie do informacji o sukcesach w zneutralizowaniu ataków terrorystycznych. W takim przypadku organizacje takie jak ISIS uzyskują przewagę w przestrzeni publicznej. Niestety, nie jest to jedyna sfera, w której siły bezpieczeństwa są ograniczane przez systemy. Siły zbrojne w dalszym ciągu są przygotowywane do tradycyjnych operacji wojskowych, często pomijane jest to, że w ciągu ostatnich 200 lat aż 80% wojen było prowadzone w sposób nieregularny. Skutecznym sposobem na ich neutralizowanie było opracowanie nowych, innowacyjnych sposobów

39 *DARPA Announces Research Teams Selected to Semantic Forensics Program*, https://www.darpa.mil/news-events/2021-03-02 [dostęp: 15.09.2021].

pozyskiwania informacji oraz ich badania. Bazują one głównie na analizie danych z istniejących już systemów, koncentrują się na informacjach pochodzących z sieci społecznościowych oraz ze zmian w sferze geografii ludzkiej aktywności[40].

Dowódcy oraz personel prowadzący działania wywiadowcze muszą rozumieć obszar działań w czasie kontrataku. Powstanie w Peru potwierdza, że zdolności wywiadowcze można zintegrować z operacjami informacyjnymi oraz zintegrowanymi operacjami kształtowania polityki pieniężnej w celu skutecznego osłabienia powstania. W ostateczności rząd peruwiański zdołał wykorzystać rozwój gospodarczy oraz kampanię informacyjną do osłabienia rebelii Świetlistego Szlaku (Shining Path). Stopniowy rozwój skutecznej armii przyczynił się do kontynuowania sukcesu. Wywiad doprowadzał do schwytania przywódcy rebelii, dlatego zmienił charakter powstania i znacznie zmniejszył zagrożenie dla Peru ze strony organizacji terrorystycznej[41].

Pierwszą wojnę w Zatoce Perskiej nazwano wojną CNN, a kolejne działania sił terrorystycznych wykorzystujące tzw. efekt CNN[42]. Z badań Piers'a Robinsona wynika, że efekt CNN jest wpływem przekazu medialnego, czyli telewizji informacyjnych oraz gazet, omawianego kryzysu humanitarnego na politykę zachodnich państw właśnie względem tego kryzysu[43]. Wielkie stacje telewizyjne dostarczają istotne informacje w doskonały sposób, ale konkurencyjne z nimi są informacje pochodzące z Facebooka, YouTube oraz Twittera zarówno z powodu szybkości przekazu, jak i dlatego, że tworzy je społeczeństwo. Można wymienić wiele przykładów wykorzystania sieci społecznościowych i nowoczesnych sieci telekomunikacyjnych w trakcie działań militarnych. Należy wyróżnić tutaj przypadek wolontariuszy-wywiadowców działających podczas konfliktu w Libii. Komunikowali się oni z siłami NATO za pomocą portali społecznościowych i z wykorzystaniem Google Map podawali pozycje do bombardowań. Syryjscy rebelianci używali iPadów oraz telefonów z systemem Android do wzrostu skuteczności ognia, konsole do gier video i telewizory LED służyły do kontrolowania domowej produkcji czołgów, a snajperzy korzystali z aplikacji na iPhone oraz wbudowanych kamer do kalkulowania i późniejszego nagrywania swoich działań. Gwałtowny rozwój mobilnego Internetu oraz sieci komunikacyjnych

40 M. Pawlak, *Przewidzieć nieprzewidywalne*, „Polska Zbrojna" 2016, nr 1.
41 *FM 3-24 MCWP 3-33.5*, *Insurgencies and countering insurgencies*, Washington 2014, s. 8–1.
42 M. Pawlak, op. cit.
43 P. Robinson, *The CNN Effect: the myth of news, foreign policy and intervention*, Abingdon-on-Thames 2003, s. 2.

przyczynił się do pojawienia takich możliwości, szczególnie zauważalne było to w rejonach o wysokim natężeniu konfliktów zbrojnych. W 2000 roku około 10% społeczeństwa Iraku miało dostęp do telefonii komórkowej, w Syrii było to 30 tys., w Libii około 40 tys. Po dekadzie Irak miał już 10 mln użytkowników telefonów komórkowych, a Syria 13 mln. Nastąpił również gwałtowny wzrost dostępu do telewizji i Internetu. W tym czasie w Nigerii liczba telefonów komórkowych zwiększyła się z 30 tys. do 113 mln. Rozwój technik telekomunikacyjnych uwypuklił czynnik *Human Geography*, który jest powiązany z przemieszczaniem się ludności oraz możliwościami komunikacji w ramach np. sieci daspory. Daje ona możliwość stworzenia dokładnych i jednocześnie dynamicznych map zagrożeń w połączeniu z sieciami społecznymi, w ich lokalizacji oraz komunikacji. W Libii sporządzono mapę zagrożeń, która pokazywała przemieszczanie się reżimowych sił, obrazy z miejsc dotkniętych walkami oraz zagrożeń ludności cywilnej[44].

Bibliografia

Azani E., Barak M., Landau E., Liv N., *Identifying Money Transfers and Terror Finance Infrastructure*, Herzliya 2020.
Ciborowski L., *Walka informacyjna*, Toruń 1999.
Clausewitz C. von, *O wojnie. Podręcznik stratega*, Gliwice 2013.
Czechowski R., Sienkiewicz P., *Przestępcze oblicza komputerów*, Warszawa 1993.
Dąbrowska M., Rybiński P., *Dezinformacja jako narzędzie kreowania wizerunku*, cz. 1, *Działalność medialna ISIS*, „Zeszyty Naukowe AszWoj" 2017, nr 4.
Formicki T., *Wywiad i kontrwywiad jako kluczowe komponenty walki informacyjnej*, Warszawa 2020.
Liedel K.C., Piasecka P., Aleksandrowicz T.R., *Analiza informacji. Teoria i praktyka*, Warszawa 2012.
Olech A.K., Lis A., *Technologia i terroryzm. Sztuczna inteligencja w dobie zagrożeń terrorystycznych*, Warszawa 2021.
Pawlak M., *Przewidzieć nieprzewidywalne*, „Polska Zbrojna" 2016, nr 1.
Robinson P, *The CNN Effect: the myth of news, foreign policy and intervention*, Abingdon-on-Thames 2003.
Schuman T. (Bezmienow J.), *Agentura wpływu. Tajniki działalności wywrotowej KGB*, Kraków 2020.
Schuman T. (Bezmienow J.), *Love Letter to America*, Los Angeles 1984.
Sienkiewicz P., *Systemy kierowania*, Warszawa 1989.
Singer P.W., Brooking E.T., *Nowy rodzaj wojny. Media społecznościowe jako broń*, Kraków 2019.
Sykulski L., *Rosyjska geopolityka a wojna informacyjna*, Warszawa 2019.
Wejkszner A., *Państwo Islamskie: narodziny nowego kalifatu*, Warszawa 2016.
Winter Ch., *The Virtual „Caliphate": Understanding Islamic State's Propaganda Strategy*, Quilliam 2015
Zielińska A., *Rynek medialny ISIS*, „Refleksje. Pismo Naukowe Studentów i Doktorantów WNPID UAM" 2019.

44 M. Pawlak, *Przewidzieć nieprzewidywalne*, „Polska Zbrojna" 2016, nr 1.

Combat in the information sphere as a modern tool of irregular warfare

Abstract

The scientific-information revolution currently underway around the world is completely changing the most essential objectives of ongoing conflicts, and with it is establishing the global character and the purpose of the game in modern conflicts. The factors of struggle have been reevaluated, the competition for material resources has been replaced by the struggle for spiritual and intellectual resources, while human consciousness has become the main object of struggle, the human mind has become the battlefield.

Currently, information is considered to be the third fundamental component of the reality around us. Technological development of the sector of communication equipment has caused that nowadays the civilian population is no longer just a passive observer of the situation, but becomes a participant and subject of events, for example, through its activity in social media. From the point of view of special forces operations, providing reliable information to the local community is extremely important, moreover, it often determines both the success of the mission and potential death.

The aim of this article was to identify the impact of the development of information techniques on changes within the conduct and application of contemporary forms of irregular operations. An analysis was made of the concepts, planes and concepts of warfare in the sphere of information and the impact it has on society. In the article, the author demonstrated the role of social media in new approaches to the application of irregular operations and examined the changes that have occurred in disinformation operations using modern technologies.

Key words: irregular warfare, information warfare, artificial intelligence, social media, disinformation