WIEDZA OBRONNA
2021, Vol. 275 No. 2
ISSN: 2658-0829 (Online) 0209-0031 (Print)
Journal homepage: http://wiedzaobronna.edu.pl
DOI: https://doi.org/10.34752/2021-e275

ALEKSANDER KSAWERY OLECH *
Instytut Nowej Europy, Warszawa, Polska

ALAN LIS *
Instytut Nowej Europy, Warszawa, Polska

WYKORZYSTANIE NOWYCH TECHNOLOGII PRZEZ TERRORYSTÓW NA PRZYKŁADZIE DRONÓW I DEEP FAKE'ÓW

THE USE OF NEW TECHNOLOGIES BY TERRORISTS ON THE EXAMPLE OF UAV AND DEEP FAKE

ABSTRAKT: Organizacje terrorystyczne w coraz większym zakresie, w różnych aspektach swojej działalności, wykorzystują nowe rozwiązania technologiczne – od komunikacji wewnętrznej, poprzez procesy rekrutacyjne, aż po przeprowadzanie skumulowanych ataków. Technologiczny rozwój umożliwia im skuteczne funkcjonowanie i sprawniejsze realizowanie wyznaczonych celów, niejednokrotnie znacznie zwiększając obręb prowadzonych operacji o narzędzia i środki, które były niedostępne jeszcze kilka lub kilkanaście lat temu. Niniejszy artykuł odnosi się do aspektu wykorzystania przez organizacje terrorystyczne nowych technologii w postaci dronów — zarówno tych bardziej tradycyjnych (ale zaawansowanych technologicznie), jak również tych wyposażonych w sztuczną inteligencję – i deep fake'ów, czyli fałszywych zdjęć i materiałów audio i wideo. Głównym celem jest zasygnalizowanie niebezpieczeństw, jakie niesie za sobą wykorzystywanie przez terrorystów nowych technologii, również sztucznej inteligencji, oraz zrodzona naukowa potrzeba dokładnej analizy tego zagrożenia.

SŁOWA KLUCZOWE: terroryzm, drony, deep fake'i sztuczna inteligencja, technologia

* dr Aleksander Ksawery Olech, Institute of New Europe, Warsaw, Poland
https://orcid.org/0000-0002-3793-5913 akolech@wp.pl

* Alan Lis, Institute of New Europe, Warsaw, Poland,
https://orcid.org/0000-0002-9555-2689 alanlis95@gmail.com

ABSTRACT: Terrorist organisations are increasingly taking advantage of new technologies in various aspects of their activity – from internal communication, to recruitment processes, to carrying out their attacks. Technological development allows them to operate effectively and achieve their goals more efficiently, often significantly increasing the scope of operations with tools and resources that were unavailable for such organisations a few years ago. This article addresses the use of new technologies by terrorist organisations on the example of drones - both more traditional ones (but still technologically advanced), as well as those equipped with artificial intelligence — and deep fakes, that is fake photos, audio, and video materials. The main purpose is to signal the perils of terrorists' use of new technologies, including artificial intelligence, and the need for a thorough analysis of this threat.

KEYWORDS: terrorism, drones, deep fakes, artificial intelligence, technology

WPROWADZENIE

Organizacje terrorystyczne coraz częściej i w coraz większym stopniu wykorzystują zdobycze nowej technologii w różnych aspektach swojej działalności, począwszy od komunikacji wewnętrznej, przez przeprowadzanie procesów rekrutacyjnych, aż po przeprowadzanie ataków. W ostatnich latach został poczyniony ogromny postęp w dziedzinie rozwoju sztucznej inteligencji (SI), która bezsprzecznie jest jednym z najpotężniejszych mnożników siły XXI wieku i ma potencjał, by zmienić światowy układ sił militarnych, a tym samym globalny krajobraz polityczny.

Ewentualne wykorzystanie przez organizacje terrorystyczne sztucznej inteligencji może być tragiczne w skutkach. Chociaż w przypadku większości organizacji terrorystycznych ryzyko, że wejdą one w posiadanie SI jest znikome, taka możliwość istnieje i musi zostać gruntownie przeanalizowana. W tym artykule zostanie jednak poruszona kwestia wykorzystania przez terrorystów nie tylko sztucznej inteligencji w postaci dronów wyposażonych w algorytmy SI i deep fake'ów, lecz również innych zdobyczy technologii – bardziej tradycyjnych, jednak wciąż technologicznie zaawansowanych bezzałogowych statków powietrznych.

Autorzy egzemplifikują największe zagrożenia ze strony terrorystów, którzy uzyskali najnowsze narzędzia do prowadzenia swojej działalności. Z uwagi na dość szeroki charakter zagadnienia ograniczono liczbę przykładów oraz wskazano na najbardziej szkodliwe aktywności realizowane przez grupy ekstremistów. Jednocześnie podano wątpliwości, czy możliwym jest skuteczne realizowanie czynności na rzecz zatrzymania zagrożeń terrorystycznych przy

dynamicznie rozwijającym się na świecie sektorze militarnym. W rozważaniach wykorzystano opracowania naukowe oraz informacje udostępnione przez specjalistów w dziedzinie bezpieczeństwa i technologii.

Na początku artykułu przedstawiono definicję sztucznej inteligencji, wskazując, co kryje się pod tym terminem. Następnie opisano ryzyko zdobycia SI przez terrorystów, po czym poruszono kwestię wykorzystania dronów przez organizacje terrorystyczne (zarówno tych klasycznych, jak i potencjalnie wykorzystanych bezzałogowych statków powietrznych wyposażonych w algorytmy sztucznej inteligencji). Kolejnym elementem, który poddano analizie jest problematyka zastosowania deep fake'ów oraz wyjaśnienie, w jaki sposób mogą one zostać wykorzystane przez terrorystów. Całość rozważań zamyka się w rekomendacji, którą przedstawiono w zakończeniu.

OKREŚLENIE I WERYFIKACJA SZTUCZNEJ INTELIGENCJI

Obecnie nie ma jednej, powszechnie uznawanej definicji sztucznej inteligencji[1,2]. W dziedzinie tej zachodzą szybkie zmiany i jest ona nieustannie rozwijana, co skutkuje pojawianiem się coraz to nowych możliwości definiowania SI. W ciągu ostatnich kilkunastu lat nastąpiło znaczne ożywienie zainteresowania tą tematyką, a technologia SI przyciąga uwagę specjalistów z wielu różnych dziedzin[3]. Potwierdza to fakt, że od 2010 roku liczba publikacji akademickich na temat sztucznej inteligencji wzrosła 8-krotnie[4].

Z uwagi na powyższe można argumentować, że pod terminem „sztuczna inteligencja" kryje się szeroki zakres technologii odnoszących się do dziedziny informatyki, których celem jest „budowa inteligentnych maszyn zdolnych do wykonywania zadań zwykle wymagających ludzkiej inteligencji"[5], które w swej naturze byłyby w pełni lub częściowo autonomiczne. Sztuczna inteligencja jest w stanie naśladować lub wykazywać funkcje związane z ludzkimi

[1] McKinsey & Company, *Artificial Intelligence And Southeast Asia's Future*, https://www.mckinsey.com/~/media/mckinsey/featured%20insights/artificial%20intelligence/ai%20and%20se%20asia%20future/artificial-intelligence-and-southeast-asias-future.ashx, dostęp: 22.10.2020, s 4.
[2] K. Sayler, 2020. *Artificial Intelligence And National Security*, https://fas.org/sgp/crs/natsec/R45178.pdf, dostęp: 11.11.2020.
[3] K. Sayler, 2020. *Artificial Intelligence And National Security*, https://fas.org/sgp/crs/natsec/R45178.pdf, dostęp: 11.11.2020.
[4] G. Moy, S. Shekh, M. Oxenham and S. Ellis-Steinborner, *Recent Advances In Artificial Intelligence And Their Impact On Defence*, https://www.dst.defence.gov.au/sites/default/files/publications/documents/DST-Group-TR-3716_0.pdf, dostęp 16.10.2020.
[5] Builtin.com, *What Is Artificial Intelligence? How Does AI Work?*, https://builtin.com/artificial-intelligence, dostęp: 1.11.2020.

zachowaniami, takie jak zdolność do uczenia się, autokorekty lub rozumienia języka[6]. Systemy oparte na SI mogą być w oparciu na oprogramowaniu działać w świecie wirtualnym (przykładem są tutaj systemy rozpoznawania twarzy i mowy czy też oprogramowania przeznaczone do analizy obrazu), jak również być wbudowane w urządzenia sprzętowe (drony, autonomiczne pojazdy itp.)[7].

Istnieją różne rodzaje sztucznej inteligencji, spośród których szczególnie interesującym przykładem jest uczenie maszynowe. Jest to zdolność do uczenia się lub przystosowywania się do danego środowiska (w przypadku robotów) w taki sposób, aby urządzenia wyposażone w SI były w stanie wykonywać zadania, nie będąc do tego specjalnie zaprogramowanym. Urządzenia posiadające takie zdolności opierają się na algorytmach, które umożliwiają im uczenie się i doskonalenie poprzez doświadczenie. Chociaż istnieje wiele różnych metod edukacji maszynowej, dwie główne to tzw. uczenie się nadzorowane i tzw. uczenie się bez nadzoru[8]. Urządzenia zdolne do samodzielnego uczenia się, mogą prognozować przyszłe zachowania lub wyniki projektu bez potrzeby ingerencji człowieka. Chociaż sama edukacja maszynowa jest bardzo popularna, należy podkreślić, że wiele „bardzo rozwiniętych urządzeń wyposażonych w sztuczną inteligencję [...] nie korzysta z uczenia maszynowego”[9].

Zaawansowane metody uczenia maszynowego określane są jako „głębokie uczenie” i stanowią kolejny przykład technologii sztucznej inteligencji. Innymi rodzajami są m.in. przetwarzanie języka naturalnego i robotyka[10].

GROŹBA PRZEJĘCIA PRZEZ TERRORYSTÓW SZTUCZNEJ INTELIGENCJI

Panuje powszechne przekonanie, że organizacje terrorystyczne mogą wykorzystywać sztuczną inteligencję do przeprowadzanych przez siebie zamachów. Wśród organizacji, które dysponują wystarczającymi środkami finansowymi, by uzyskać dostęp do tak zaawansowanych

[6] Techjury.Net, *Infographic: How AI Is Being Deployed Across Industries*, Robotics Business Review, https://www.roboticsbusinessreview.com/ai/infographic-how-ai-is-being-deployed-across-industries/, dostęp: 28.10.2020.
[7] E. Bird, J. Fox-Skelly, N. Jenner, R. Larbey, E. Weitkamp and A. Winfield, *The Ethics Of Artificial Intelligence: Issues And Initiatives*. Brussels 2020.
[8] G. Moy, S. Shekh, M. Oxenham, and S. Ellis-Steinborner, *Recent Advances In Artificial Intelligence And Their Impact On Defence*, https://www.dst.defence.gov.au/sites/default/files/publications/documents/DST-Group-TR-3716_0.pdf, dostęp: 16.10.2020.
[9] E. Bird, J. Fox-Skelly, N. Jenner, R. Larbey, E. Weitkamp and A. Winfield, *The Ethics Of Artificial Intelligence: Issues And Initiatives*. Brussels 2020.
[10] Techjury.Net, *Infographic: How AI Is Being Deployed Across Industries*, Robotics Business Review, https://www.roboticsbusinessreview.com/ai/infographic-how-ai-is-being-deployed-across-industries/, dostęp: 28.10.2020.

technologii, na szczególną uwagę zasługują następujące: al-Kaida, ISIS, Hamas, Hezbollah, talibowie (Taliban), Partia Pracujących Kurdystanu (PKK), Palestyński Islamski Dżihad, Kata'ib Hezbollah, Lashkar-e-Tayyiba i Boko Haram. Poza finansowaniem z innych źródeł czynnikiem wpływającym na możliwość pozyskania takich technologii jest otrzymywanie pomocy finansowej od państwa-sponsora, czego przykładem może być Hezbollah[11]. Przekazanie takich technologii organizacjom terrorystycznym przez państwo-sponsora nie jest scenariuszem, który można kategorycznie wykluczyć, niemniej jednak warto podkreślić, że rządy wspierające konkretne organizacje terrorystyczne mogą mieć ograniczone zaufanie w tym względzie, obawiając się zbytniego usamodzielnienia się terrorystów i — przynajmniej częściowej — utraty kontroli nad nimi.

Można więc postawić tezę, że możliwość pozyskania sztucznej inteligencji przez organizacje terrorystyczne do przeprowadzenia śmiertelnego ataku jest realna, ale w przypadku większości wyżej wymienionych organizacji terrorystycznych raczej mało prawdopodobna, przynamniej na chwilę obecną. Niemniej jednak jest to zagrożenie — nawet jeśli obecnie nie w pełni ukształtowane — którego nie można bagatelizować.

Gdyby terroryści uzyskali dostęp do broni kontrolowanej przez sztuczną inteligencję lub wspomaganej jej algorytmami, znacznie zwiększyłoby to zagrożenie dla społeczności międzynarodowej. Po pierwsze, skutkowałoby to zwiększeniem skuteczności przeprowadzanych przez nich zamachów. Drugim efektem mogłoby być zmniejszenie „zapotrzebowania" na zamachowców-samobójców. Po trzecie, istnieje możliwość, że organizacjom terrorystycznym łatwiej byłoby uzyskać poufne informacje o siłach zbrojnych państw je zwalczających poprzez operacje hakerskie wspierane przez sztuczną inteligencję.

Sztuczna inteligencja pozbawiona jest kompasu moralnego. Użycie broni opartej na jej algorytmach oznacza ograniczony lub wręcz całkowity brak zahamowań wpływających na zachowania bojowe. Organizacje terrorystyczne są odpowiedzialne za tysiące ofiar śmiertelnych, cywilnych i wojskowych i z pewnością są zmotywowane, aby przy użyciu zaawansowanych technologii zwiększyć te liczby. Dla takich grup sztuczna inteligencja jest po prostu kolejnym środkiem walki z przeciwnikiem. Terrorystów nie ograniczają takie pojęcia, jak przyzwoitość, moralność czy proporcjonalność. W rezultacie sama sztuczna inteligencja jest niczym innym, jak środkiem do maksymalizacji szkód i minimalizacji strat. Ponadto sztuczna

[11] M. Hoenig, *Hezbollah and the Use of Drones as a Weapon of Terrorism,* https://fas.org/pir-pubs/hezbollah-use-drones-weapon-terrorism, dostęp: 14.10.2020.

inteligencja może być używana do celów propagandowych, aby pochwalić się możliwością zastosowania nowinek technologicznych, co może mieć pozytywny wpływ np. na procesy rekrutacyjne. Konkludując, można postawić tezę, że organizacje terrorystyczne będą dążyć do przeprowadzania ataków przy użyciu sztucznej inteligencji, nawet jeśli nie jest to kluczowe dla powodzenia ich operacji[12].

Również drony mogą być wyposażone w SI, taka broń także może trafić na wyposażenie terrorystów. Poniższa część tekstu dotyczy wykorzystania przez terrorystów zarówno bardziej „tradycyjnych", ale wciąż technologicznie zaawansowanych bezzałogowych statków powietrznych, jak i właśnie dronów wyposażonych w algorytmy sztucznej inteligencji.

TERRORYŚCI WYKORZYSTUJĄCY DRONY STEROWANE PRZEZ SZTUCZNĄ INTELIGENCJĘ

Bezzałogowe statki powietrzne, takie jak drony, mogą być jednym z pierwszych typów broni kontrolowanej przez sztuczną inteligencję bądź wspomaganej jej algorytmami i używanej w celach terrorystycznych. Ich prostota umożliwia terrorystom przeprowadzenie ataku bez angażowania dużej liczby osób i logistyki. W zależności od skali ataku niektóre uderzenia mogą być koordynowane nawet przez jedną osobę.

Aktorzy niepaństwowi, w tym organizacje terrorystyczne, od lat próbują używać dronów przeciwko walczącym z nimi państwom. Według pojawiających się w mediach informacji miała już miejsce znaczna liczba takich wydarzeń, lecz do końca 2016 roku żadne z nich nie było śmiertelne. Drony były zwykle używane do przelotu nad określoną częścią terytorium w celu zbierania informacji, np. na temat baz wojskowych, ich możliwego uzbrojenia i wyposażenia. Na początku XXI wieku bezzałogowe statki powietrzne były najczęściej używane w obszarach terytorialnych Izraela i Pakistanu, niemniej jednak w ciągu ostatnich 5 lat wykorzystanie dronów odnotowano również w innych krajach.

Dostosowując się do ulepszeń technologicznych, ekstremistom udało się osiągnąć swój cel i ostatecznie 2 października 2016 roku przeprowadzili śmiertelny atak z wykorzystaniem drona przeciwko aktorowi państwowemu. Był to pierwszy udany zamach przy użyciu tego rodzaju technologii, najprawdopodobniej dokonany przez Państwo Islamskie[13]. Do tego czasu, zgodnie

[12] R. van der Veer, *Terrorism in the age of technology*, https://www.clingendael.org/pub/2019/strategic-monitor-2019-2020/terrorism-in-the-age-of-technology, dostęp: 18.09.2020.
[13] J. Ware, *Terrorist groups, artificial intelligence, and killer drones*, https://warontherocks.com/2019/09/terrorist-groups-artificial-intelligence-and-killer-drones, dostęp: 21.09.2020.

z informacjami Pentagonu, terroryści używali tylko podstawowych wersji dronów, które byli w stanie łatwo zakupić i obsługiwać w celu prowadzenia obserwacji czy transportu materiałów wybuchowych. W ramach swojej odpowiedzi siły amerykańskie użyły specjalnego sprzętu do pokonania bezzałogowców — „karabinów" przeciwdronowych — aby zakłócić sygnał pomiędzy maszyną a pilotem[14].

Innym przykładem jest wysłanie przez ISIS bezzałogowego statku powietrznego wypełnionego materiałami wybuchowymi do ataku na pozycje francuskie i kurdyjskie w Erbilu w północnej części Iraku. Dwóch żołnierzy kurdyjskich zginęło, a dwóch francuskich żołnierzy sił specjalnych zostało ciężko rannych. Jest to jedna z najpopularniejszych metod użycia dronów przez ISIS[15]. Należy podkreślić, że atak ten był początkiem działań terrorystycznych wspomaganych wysoko rozwiniętymi technologiami, a także wskazówką, w jakim kierunku podążą ekstremiści. Co warte podkreślenia, w 2017 roku ISIS ogłosiło utworzenie dywizji o nazwie Bezzałogowe Statki Powietrzne Mudżahedinów, której głównym celem było wykorzystanie bezzałogowców w ramach długoterminowej strategii rozwoju technologii dronów i ich przystosowania do użycia jako broni. Grupa wykorzystuje technologię dronów do obserwacji, głównie w Iraku i Syrii. Ponadto organizacja była w stanie zaatakować dronem czołg bojowy w Mosulu w 2017 roku[16].

W tym samym roku zdalnie pilotowany przez jemeńskich rebeliantów Houthi statek zaatakował instalacje naftowe Arabii Saudyjskiej w Bukajku i Churajs. Rebelianci celowali w największy na świecie zakład przewarzania ropy, który ma kluczowe znaczenie dla globalnych dostaw energii[17]. Wysłali od 10 do 25 dronów, które przeprowadziły operację jako rój. Bezzałogowe statki powietrzne zaatakowały co najmniej dwiema falami i spowodowały tak duże szkody, że ugaszenie pożarów stanowiło spore wyzwanie. Kontrola zdjęć satelitarnych ujawniła, iż miało miejsce minimum 19 uderzeń, które uszkodziły 14 pojemników magazynowych.

[14] T. Gibbons-Neff, *ISIS used an armed drone to kill two Kurdish fighters and wound French troops, report says*, https://www.washingtonpost.com/news/checkpoint/wp/2016/10/11/isis-used-an-armed-drone-to-kill-two-kurdish-fighters-and-wound-french-troops-report-says, dostęp: 21.09.2020.
[15] N. Guibert, *Irak: Paris confirme qu'un drone piégé a blessé deux membres des forces spéciales françaises à Erbil*, https://www.lemonde.fr/proche-orient/article/2016/10/11/irak-deux-commandos-francais-gravement-blesses-a-erbil-par-un-drone-piege_5011751_3218.html, dostęp: 21.09.2020.
[16] T. Rogoway, *ISIS Drone Dropping Bomblet On Abrams Tank Is A Sign Of What's To Come*, https://www.thedrive.com/the-war-zone/7155/isis-drone-dropping-bomblet-on-abrams-tank-is-a-sign-of-whats-to-come, dostęp: 21.09.2020.
[17] N. Kumar, *Saudi Arabia Drone Attack: Sign of Changing Character of Hybrid War*, https://www.vifindia.org/article/2019/october/01/saudi-arabia-drone-attack-sign-of-changing-character-of-hybrid-war, dostęp: 22.09.2020.

Chociaż Arabia Saudyjska jest w posiadaniu systemów obrony przeciwrakietowej MIM-104 Patriot, nie była w stanie wykryć dronów z powodu ich zbyt niskiego i skierowanego z wielu kątów lotu — po raz kolejny obrona przeciwlotnicza okazała się nieskuteczna.

Aktorzy niepaństwowi już teraz wykorzystują podobny sprzęt do zdobywania informacji o lokalizacji sił zbrojnych, rodzaju uzbrojenia czy potencjalnych ruchach żołnierzy. W tym sensie terroryści działają podobnie jak siły państwowe, a posiadanie zaawansowanych technologii w coraz większym stopniu pozwala im na nawiązanie walki na równych warunkach poprzez znajdowanie nowych sposobów zwalczania wroga. W związku z tym wydaje się, że każdy aktor (państwowy czy niepaństwowy) musi zaakceptować rzeczywistość, w której bezzałogowe statki powietrzne, wyposażone lub nawet sterowane przez sztuczną inteligencję, stają się podstawowym narzędziem na polu bitwy, pomimo toczących się dyskusji i wysuwanych pytań o etykę rozmieszczania dronów na polu walki[18].

Czołowe organizacje opracowują obecnie sposoby elektronicznego wzmacniania swoich dronów i dostosowywania strategii, aby uczynić je mniej podatnymi na działania obronne. Aktorzy niepaństwowi również zwiększają swoje szanse na wykorzystanie roju dronów sterowanych przez sztuczną inteligencję. Nieliczne technologie są tak skuteczne w obniżaniu fizycznych, finansowych i psychologicznych kosztów wdrożenia do operacji, co jest powszechnie akceptowaną korzyścią sprzyjającą używaniu dronów.

Istnieje co najmniej kilka czynników, które prowadzą do częstego używania bezzałogowców nie tylko przez terrorystów, lecz również rebeliantów, grupy separatystyczne, a nawet grupy przestępcze. W dużej mierze zależy to od ich możliwości logistycznych, finansowych i terytorialnych, a wśród czynników powodujących zainteresowane powyższych grup użyciem dronów warto zwrócić uwagę na opisane poniżej aspekty.

Nieszczelna obrona przeciwlotnicza

Rozmieszczenie dronów staje się naturalnym rozszerzeniem narzędzi już dostępnych na wojnie. Dodatkowo cały czas prowadzone są testy, które zwiększają potencjał bojowy bezzałogowych bojowych statków powietrznych w wielu sytuacjach, takich jak niszczenie lub wprowadzanie w błąd obrony przeciwlotniczej. Przewaga wynikająca z używania niewykrywalnych bezzałogowców, zwłaszcza tych kontrolowanych przez sztuczną inteligencję

[18] BBC, *Anti-drone protest at RAF Waddington*, https://www.bbc.com/news/uk-england-lincolnshire-41536818, dostęp: 20.10.2020.

bądź wspomaganych jej algorytmami, stałaby się jednym z najcenniejszych elementów uzbrojenia na wyposażeniu organizacji terrorystycznych.

Niezdolność do wyeliminowania zagrożenia z powietrza wskazuje na potrzebę wzmocnienia skuteczności obrony przeciwlotniczej. Jest to silnie związane z trwającymi konfliktami, w których wykorzystywane są nowe technologie, co prowadzi do globalnej konkurencji w pokonywaniu systemów przeciwlotniczych[19].

Jednym z wielu przykładów wykorzystania nieszczelnej obrony przeciwlotniczej jest wspomniany wyżej atak przeprowadzony przez Houthi na saudyjskie obiekty naftowe z użyciem dronów we wrześniu 2019 roku. Nawet państwa o potężnych zasobach i zdolnościach w zakresie bezpieczeństwa mogą być ofiarami ataków terrorystycznych powodujących śmierć ludzi i naruszenie integralności infrastruktury krytycznej. Obecnie celów, zwłaszcza infrastruktury krytycznej, nie można zabezpieczyć ani przesunąć, jeśli obrona przeciwlotnicza nie zapewni im ochrony, a atakujący mają do dyspozycji szeroką gamę broni elektronicznej i kinetycznej. Nieszczelna obrona przeciwlotnicza, a tym samym brak możliwości skutecznej obrony przed atakami przy użyciu dronów, umożliwia terrorystom zadawanie strat, nie tylko w ludziach, lecz także finansowych czy wizerunkowych.

Dezinformacja i propaganda przy wykorzystaniu zaawansowanej technologii

Użycie dronów, zwłaszcza wyposażonych w algorytmy sztucznej inteligencji, może stanowić idealny materiał propagandowy dla organizacji terrorystycznych. Niektóre z nich, takie jak Państwo Islamskie czy al-Kaida, będą preferować wywieranie wpływu i głośno manifestować sukces w postaci skutecznego użycia tego rodzaju broni. Biorąc pod uwagę tendencje organizacji terrorystycznych do demonstrowania swojej siły – zwłaszcza w przypadku dwóch wyżej wymienionych organizacji — można przypuszczać, że będą umieszczać dowody ich użycia w mediach społecznościowych w nadziei, że pozytywnie wpłynie to na ich procesy rekrutacyjne.

Łatwość zastosowania i eksploatacji

Wydaje się, że terroryści raczej nie opracują własnej sztucznej inteligencji, która sterowałaby ich dronami — grupom ekstremistycznym przeważnie zależy na zakupie bądź

[19] J. V. Parachini, P. A. Wilson, *Drone-Era Warfare Shows the Operational Limits of Air Defense Systems*, https://www.rand.org/blog/2020/07/drone-era-warfare-shows-the-operational-limits-of-air.html, dostęp: 21.09.2020.

zdobyciu broni gotowej do natychmiastowego użycia. Ponadto wątpliwym jest, aby organizacje terrorystyczne posiadały w swoich szeregach inżynierów wykwalifikowanych na tyle, aby opracować SI potrafiącą sterować dronami. Prawdopodobnym jest natomiast, że po nabyciu drona wyposażonego w algorytmy sztucznej inteligencji (poprzez zakup, kradzież lub ewentualne przekazanie przez państwo-sponsora) członkowie przynajmniej części przytoczonych na początku artykułów organizacji terrorystycznych byliby w stanie umiejętnie posługiwać się takim sprzętem i należycie określić cel ataku, uzbroić platformę i w odpowiedni sposób ją utrzymać. Przeszkody w programowaniu drona i zapewnieniu obsługi technicznej nie powinny stanowić problemu, jeśli broń jest już zbudowana i wyposażona w odpowiednie oprogramowanie, czyli w znacznym stopniu gotowa do użycia. Jeśli bezzałogowce zostaną wyposażone w sztuczną inteligencję, inżynierowie będący członkami organizacji terrorystycznych zaznajomieni z tego rodzaju oprogramowaniem nie napotkają raczej trudności z jego modyfikacją czy adaptacją, dzięki czemu terroryści będą mogli z łatwością z nich korzystać.

Rój dronów – zagrożenie XXI wieku

Roje dronów stanowią ogromne zagrożenie dla systemów obronnych państw na całym świecie. Zatrzymanie dużej liczby statków powietrznych gotowych do wyeliminowania przeciwnika może być trudne. Skoncentrowany atak wydaje się być doskonałym sposobem dla organizacji terrorystycznych na skuteczną realizację misji. Jednak przeprowadzenie tego rodzaju ataku przez drony kontrolowane przez operatorów ludzkich wydaje się niemożliwe – nie byliby oni w stanie kontrolować toru lotu każdego pojazdu w roju tak skutecznie jak sztuczna inteligencja. Kontrola ludzka byłaby stosunkowo bardziej chaotyczna niż kontrola prowadzona przez SI ze względu na brak szybkiego i przejrzystego kanału komunikacyjnego podczas intensywnego ataku. Tym samym tylko sztuczna inteligencja, która sama przeprowadza atak, jest w stanie sterować ogromną liczbą maszyn omijających systemy obrony powietrznej w sposób doskonale zsynchronizowany, zachowując jednocześnie kontrolę nad swoimi zasobami.

Ponadto możliwe jest, że drony będą mogły przenosić ładunek bojowy o wadze nawet do 10 ton raczej wcześniej niż później. W Rosji, która jest jednym z głównych aktorów rozwijających technologię sztucznej inteligencji, rozpoczęto już prace nad zaawansowanymi dronami, które będą operować na małych wysokościach z prędkością 1400 kilometrów na godzinę i przenosić

ładunki w przedziale 2,8-8 ton[20]. Dlatego atak roju dronów przenoszących co najmniej kilka ton ładunków wybuchowych stałby się bronią o niewyobrażalnej sile destrukcji.

DEEP FAKE

Termin „deep fake" jest używany w „odniesieniu do realistycznych zdjęć, audio, wideo i innych podróbek generowanych przy użyciu technologii sztucznej inteligencji"[21] i po raz pierwszy został użyty w 2017 roku. Najczęściej deep fake'i tworzone są poprzez wykorzystanie technik uczenia maszynowego, w szczególności generatywnych sieci przeciwstawnych. W procesie rywalizacji pomiędzy dwoma różnymi systemami uczenia maszynowego jeden z nich (generator) tworzy rodzaj danych wyjściowych (nagania audio, zdjęcia, materiał wideo), a drugi (dyskryminator) uczy się identyfikacji fałszywych efektów pracy generatora. „Konkurencja" trwa tak długo, jak długo generator doskonali swoją pracę do tego stopnia, że dyskryminator nie jest w stanie odróżnić treści fałszywych od prawdziwych.

Deep fake'i mają wiele pożytecznych zastosowań. Mogą być wykorzystywane np. przez nauczycieli w procesie edukacji do prowadzenia „innowacyjnych lekcji, które są o wiele bardziej angażujące"[22] niż tradycyjne lekcje poprzez np. „przywrócenie do życia" postaci historycznych. W medycynie deep fake'i stosowane są do celów syntetyzowania „fałszywych obrazów medycznych w celu wyszkolenia algorytmów wykrywania chorób rzadkich"[23]. Zastosowanie znajdują też w dziedzinie rozrywki i kultury: jedno z muzeów na Florydzie stworzyło wystawę poświęconą Salvadorowi Dalemu, w której przedstawiono „naturalnej wielkości rekonstrukcję Dalego za pomocą techniki montażu wideo wzbogaconego o uczenie maszynowe"[24].

Pomimo powyższych wskazań, deep fake'i mogą również stanowić szeroki zakres zagrożeń dla bezpieczeństwa krajowego i międzynarodowego. Autorzy badania przeprowadzonego na University College London w 2020 roku stwierdzili, że „fałszywe treści audio lub wideo zostały uznane przez ekspertów za najbardziej niepokojące wykorzystanie sztucznej inteligencji pod

[20] R. McDermott, *Moscow Unveils Further Advances in Drone Technology*, Eurasia Daily Monitor, Volume: 16, Issue: 139.
[21] L. Harris, *Deep Fakes And National Security*, Congressional Research Service, https://crsreports.congress.gov/product/pdf/IF/IF11333, dostęp: 2.11.2020.
[22] A. Jaiman, *Positive Use Cases Of Deepfakes*, Toward Data Science, https://towardsdatascience.com/positive-use-cases-of-deepfakes-49f510056387, dostęp: 3.11.2020.
[23] L. Harris, *Deep Fakes And National Security*, Congressional Research Service, https://crsreports.congress.gov/product/pdf/IF/IF11333, dostęp: 2.11.2020.
[24] D. Lee, *Deepfake Salvador Dalí Takes Selfies With Museum Visitors*, The Verge, https://www.theverge.com/2019/5/10/18540953/salvador-dali-lives-deepfake-museum, dostęp: 4.11.2020.

względem jej potencjalnych zastosowań w przestępczości lub terroryzmie [...]"[25]. Deep fake'i mogą być również orężem w operacjach informacyjnych[26] i wojnie informacyjnej.

Niebezpieczne zastosowanie deep fake'ów

Wykorzystywanie SI do tworzenia deep fake'ów jest raczej tanie i może być dokonywane za pomocą powszechnie dostępnego oprogramowania, co powoduje, że „nawet niewykwalifikowani operatorzy mogą pobierać wymagane narzędzia programowe i, wykorzystując publicznie dostępne dane, tworzyć coraz bardziej przekonujące podrobione treści"[27]. Chociaż z całą pewnością nie każdy byłby w stanie produkować deep fake'i o jakości wystarczającej, by oszukać innych, to jednak ich tworzenie nie wymaga aż tak zaawansowanej wiedzy i umiejętności technicznych, jak się powszechnie uważa.

Jednym z przykładów wykorzystywania deep fake'ów w celach niezgodnych z prawem jest rozpowszechnianie fałszywych nagrań wideo przedstawiających osoby publiczne, zwłaszcza polityków zachowujących się nieodpowiednio, które to materiały mogą podważyć zaufanie społeczeństwa do takich osób. Przykładem może być zmanipulowane nagranie wideo, które pokazywało spikerkę amerykańskiej Izby Reprezentantów Nancy Pelosi, jak gdyby była odurzona alkoholem[28]. Operacja taka może zostać podjęta w celu podważenia zaufania obywateli do osoby piastującej państwowe stanowisko, co z kolei może osłabiać sam proces demokratyczny. Inną możliwością jest tworzenie fałszywych zdjęć lub filmów w celu szantażowania osób, które piastują ważne funkcje państwowe, aby zmusić je do dzielenia się informacjami o charakterze niejawnym[29], co miałoby szkodliwe skutki dla ich krajów.

Również terroryści mogą używać deep fake'ów dla swoich celów. Wśród możliwych scenariuszy istnieje ten, w którym członkowie organizacji terrorystycznej wykorzystują deep fake'i do podszycia się pod krewnych lub osoby nadzorujące czyjąś pracę, dążąc ostatecznie do

[25] University College London, *'Deepfakes' Ranked As Most Serious AI Crime Threat*, https://www.ucl.ac.uk/news/2020/aug/deepfakes-ranked-most-serious-ai-crime-threat, dostęp 4.11.2020. Link do artykułu: https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-020-00123-8.
[26] K. Hartmann and K. Giles, *The Next Generation of Cyber-Enabled Information Warfare*, https://ccdcoe.org/uploads/2020/05/CyCon_2020_13_Hartmann_Giles.pdf, dostęp: 7.02.2021.
[27] L. Harris, *Deep Fakes And National Security*, Congressional Research Service, https://crsreports.congress.gov/product/pdf/IF/IF11333, dostęp: 2.11.2020.
[28] A. Zegart, *In The Deepfake Era, Counterterrorism Is Harder*, The Atlantic, https://www.theatlantic.com/ideas/archive/2019/09/us-intelligence-needs-another-reinvention/597787/, dostęp: 17.11.2020.
[29] L. Harris, *Deep Fakes And National Security*, Congressional Research Service, https://crsreports.congress.gov/product/pdf/IF/IF11333, dostęp: 2.11.2020.

wyłudzenia funduszy, które mogłyby zostać wykorzystane do finansowania ich działalności. Terroryści mogliby to zrobić replikując głos takich osób przy użyciu programu do klonowania głosów (co ciekawe, taki program jest w stanie nie tylko „naśladować głos wejściowy, ale także zmienić go tak, aby odzwierciedlał inną płeć lub nawet inny akcent”[30]). W 2019 roku cyberprzestępcy zadziałali właśnie w opisany powyżej sposób: wykorzystali technologię sztucznej inteligencji do podszycia się pod szefa firmy i wyłudzili od jego pracownika przelew opiewający na kwotę 243 tys. dolarów[31]. Opierając się na fakcie, że prosty ładunek wybuchowy, który miał zostać zdetonowany podczas mistrzostw świata w piłce nożnej w Niemczech w 2006 roku, został stworzony z „zbiornika propanu, zegarka, baterii i plastikowej butli wypełnionej gazem”[32] i kosztował zaledwie 500 dolarów, liczba ataków, które terroryści byliby w stanie sfinansować, a tym samym szkody, które mogliby wyrządzić wchodząc w posiadanie takiej sumy pieniędzy, są niewyobrażalne.

Inną niebezpieczną alternatywą jest ta, w której terroryści generują realistycznie wyglądające treści (zdjęcia lub filmy) w celu zintensyfikowania radykalizacji i rozszerzenia kampanii rekrutacyjnych. Takie fałszywe materiały mogłyby pokazywać chociażby amerykańskich, brytyjskich lub francuskich żołnierzy popełniających zbrodnie wojenne (np. poprzez znęcanie się nad schwytanymi dżihadystami lub podejrzanymi o terroryzm, torturowanie ich), co nie tylko delegitymizowałoby działania antyterrorystyczne, ale także docierało do potencjalnych rekrutów i było czynnikiem wzmagającym ich radykalizację. Najlepiej ilustrują to przykłady niektórych z kontrterrorystycznych taktyk stosowanych w czasie wojny z terroryzmem.

Powszechnie uznaje się, że nie wszystkie środki antyterrorystyczne zastosowane przez USA w wojnie z terroryzmem przyniosły oczekiwane rezultaty. W rzeczywistości niektóre z nich wręcz przeciwnie — przyczyniły się do pojawienia się nowych przeciwników bądź radykalizacji istniejących. Były wśród nich przypadki niewłaściwego traktowania więźniów poprzez poddawanie ich torturom lub przenoszenie ich z kraju do kraju bez ich zgody. Nawet

[30] Future Work Institute, *Deepfake Video And Audio Recordings*, https://futureworkinstitute.com/deepfake-video-and-audio-recordings/, dostęp: 7.11.2020.
[31] C. Stupp, *Fraudsters Used AI To Mimic CEO'S Voice In Unusual Cybercrime Case*, WSJ, https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402, dostęp: 10.11.2020.
[32] D. Temple-Raston, *How Much Does A Terrorist Attack Cost? A Lot Less Than You'd Think*, NPR, https://www.npr.org/sections/parallels/2014/06/25/325240653/how-much-does-a-terrorist-attack-cost-a-lot-less-than-you-think?t=1605889247748, dostęp: 5.11.2020.

najmniejsze zarzuty o niewłaściwe traktowanie muzułmanów lub torturowanie ich przez zachodnich żołnierzy mają głęboki wpływ na postrzeganie świata zachodniego przez wyznawców Allaha, a tym samym mogą motywować ich do wyrządzania szkód szeroko rozumianemu Zachodowi. Studium przypadku z wojny z terroryzmem wspierające tę hipotezę to skandal, do którego doszło w Abu Ghraib — jednym z wielu obiektów, w których osoby podejrzane o terroryzm były poddawane wzmocnionym technikom przesłuchań, w tym „przemocy fizycznej [...] poniżaniu seksualnemu, przykuwaniu łańcuchem, wstrząsom elektrycznym i deprywacji sensorycznej”[33]. Zdjęcia torturowanych podejrzanych zostały upublicznione w 2004 roku, w następstwie czego „zakapturzony mężczyzna i pies gnębiący więźniów stały się ikonicznymi symbolami zachodniego wysiłku wojennego”[34], które z kolei zaczęły podsycać propagandę dżihadystów, przedstawiających torturowanych jako niesprawiedliwie skrzywdzonych przez zachodnich żołnierzy, ułatwiając tym samym wysiłki rekrutacyjne terrorystów. Dostępna obecnie technologia sztucznej inteligencji pozwoliłaby terrorystom nie tylko na tworzenie fałszywych zdjęć przedstawiających niewłaściwie traktowanych przez członków zachodnich sił zbrojnych muzułmanów, ale także na stworzenie fałszywych filmów z ich udziałem. Tworząc deep fake’i i szerząc tego rodzaju dezinformację, terroryści działaliby na rzecz ułatwienia i wzmocnienia procesu radykalizacji postaw wielu potencjalnych rekrutów, a tym samym udoskonalaliby swoje wysiłki rekrutacyjne lub motywowali ludzi do przeprowadzania samodzielnych ataków w miejscach, w których żyją (ataki samozwańczych terrorystów, tzw. samotnych wilków).

ZAKOŃCZENIE

Rozwój technologiczny ułatwia codzienne życie ludziom na całym świecie, niezależnie od miejsca, w którym mieszkają. Niemniej jednak oprócz korzyści i usprawnień, jakie przynosi, ma on jeszcze drugie oblicze, które objawia się, kiedy zdobycze nowej technologii trafiają w niepowołane ręce.

Wykorzystanie przez terrorystów nowych technologii — wśród nich sztucznej inteligencji — stanowi poważne zagrożenie. Chociaż w przypadku większości organizacji terrorystycznych wejście w posiadanie broni opartej na tak nowoczesnej technologii jest raczej znikome, to takie

[33] C. Kennedy-Pipe, *IEDs, Martyrs, Civil Wars and Terrorists.* [w]: C. Kennedy-Pipe, G. Clubb and S. Mabon, ed., Terrorism and Political Violence. London: Sage, s.158.
[34] C. Kennedy-Pipe, *IEDs, Martyrs, Civil Wars and Terrorists.* [w]: C. Kennedy-Pipe, G. Clubb and S. Mabon, ed., Terrorism and Political Violence. London: Sage, s.158.

ryzyko musi być wzięte pod uwagę i zostać dokładnie przeanalizowane. Opisane w tym artykule rzeczywiste i potencjalne wykorzystanie dronów, a także deep fake'ów stanowi jedynie niewielki ułamek tego, jak organizacje terrorystyczne mogą wykorzystać nowe technologie w swojej działalności (oprócz wymienionych przykładów terroryści mogą posłużyć się drukiem 3D w celu wyprodukowania broni lub amunicji, jak również wejść w posiadanie opartych na sztucznej inteligencji autonomicznych i półautonomicznych pojazdów, które mogą zostać wykorzystane w celu przeprowadzenia zamachów). Zagrożenia dla bezpieczeństwa płynące z rozwoju technologicznego powinny być stale monitorowane oraz pozostać obiektem nieustannych badań, także w Polsce. Jest to kluczowe dla procesu budowania międzynarodowego potencjału bezpieczeństwa i stanowi fundament dla rozwijania systemu zwalczania zagrożeń terrorystycznych.

BIBLIOGRAFIA
REFERENCES LIST

BBC, *Anti-drone protest at RAF Waddington*, https://www.bbc.com/news/uk-england-lincolnshire-41536818, (dostęp: 20.10.2020).

Bird E., Fox-Skelly J., Jenner N., Larbey R., Weitkamp E. and Winfield A., *The Ethics Of Artificial Intelligence: Issues And Initiatives*. Brussels 2020.

Builtin.com, *What Is Artificial Intelligence? How Does AI Work?* https://builtin.com/artificial-intelligence, (dostęp: 1.11.2020).

Future Work Institute, *Deepfake Video And Audio Recordings*, https://futureworkinstitute.com/deepfake-video-and-audio-recordings/, (dostęp: 7.11.2020).

Gibbons-Neff T., *ISIS used an armed drone to kill two Kurdish fighters and wound French troops, report says*, https://www.washingtonpost.com/news/checkpoint/wp/2016/10/11/isis-used-an-armed-drone-to-kill-two-kurdish-fighters-and-wound-french-troops-report-says, (dostęp: 21.09.2020).

Guibert N., *Irak : Paris confirme qu'un drone piégé a blessé deux membres des forces spéciales françaises à Erbil,* https://www.lemonde.fr/proche-orient/article/2016/10/11/irak-deux-commandos-francais-gravement-blesses-a-erbil-par-un-drone-piege_5011751_3218.html, (dostęp: 21.09.2020).

Harris L., *Deep Fakes And National Security*, Congressional Research Service, https://crsreports.congress.gov/product/pdf/IF/IF11333, (dostęp: 2.11.2020).

Hartmann K. and Giles K., *The Next Generation of Cyber-Enabled Information Warfare*, https://ccdcoe.org/uploads/2020/05/CyCon_2020_13_Hartmann_Giles.pdf, (dostęp: 7.02.2021).

Hoenig M., *Hezbollah and the Use of Drones as a Weapon of Terrorism,* https://fas.org/pir-pubs/hezbollah-use-drones-weapon-terrorism, (dostęp: 14.10.2020).

Jaiman A., *Positive Use Cases Of Deepfakes*, Toward Data Science, https://towardsdatascience.com/positive-use-cases-of-deepfakes-49f510056387, (dostęp: 3.11.2020).

Kumar N., *Saudi Arabia Drone Attack: Sign of Changing Character of Hybrid War,* https://www.vifindia.org/article/2019/october/01/saudi-arabia-drone-attack-sign-of-changing-character-of-hybrid-war, (dostęp: 22.09.2020).

Lee D., *Deepfake Salvador Dalí Takes Selfies With Museum Visitors*, The Verge, https://www.theverge.com/2019/5/10/18540953/salvador-dali-lives-deepfake-museum, (dostęp: 4.11.2020).

Kennedy-Pipe C., *IEDs, Martyrs, Civil Wars and Terrorists.* [w]: C. Kennedy-Pipe, G. Clubb and S. Mabon, ed., Terrorism and Political Violence. London: Sage, s.158.

McDermott R., *Moscow Unveils Further Advances in Drone Technology,* Eurasia Daily Monitor, Volume: 16:139, 2019.

McKinsey & Company, *Artificial Intelligence And Southeast Asia's Future*, https://www.mckinsey.com/~/media/mckinsey/featured%20insights/artificial%20intelligence/ai%20and%20se%20asia%20future/artificial-intelligence-and-southeast-asias-future.ashx, dostęp: 22.10.2020, s. 4.

Moy G., Shekh S., Oxenham M. and Ellis-Steinborner S., *Recent Advances In Artificial Intelligence And Their Impact On Defence*, https://www.dst.defence.gov.au/sites/default/files/publications/documents/DST-Group-TR-3716_0.pdf, (dostęp 16.10.2020).

Parachini J. V., Wilson P. A., *Drone-Era Warfare Shows the Operational Limits of Air Defense Systems*, https://www.rand.org/blog/2020/07/drone-era-warfare-shows-the-operational-limits-of-air.html, (dostęp: 21.09.2020).

Temple-Raston D., *How Much Does A Terrorist Attack Cost? A Lot Less Than You'd Think*, NPR, https://www.npr.org/sections/parallels/2014/06/25/325240653/how-much-does-a-terrorist-attack-cost-a-lot-less-than-you-think?t=1605889247748, (dostęp: 5.11.2020).

Rogoway T.*, ISIS Drone Dropping Bomblet On Abrams Tank Is A Sign Of What's To Come,* https://www.thedrive.com/the-war-zone/7155/isis-drone-dropping-bomblet-on-abrams-tank-is-a-sign-of-whats-to-come, (dostęp: 21.09.2020).

Sayler K., *Artificial Intelligence And National Security*, https://fas.org/sgp/crs/natsec/R45178.pdf, (dostęp: 11.11.2020).

Stupp C., *Fraudsters Used AI To Mimic CEO'S Voice In Unusual Cybercrime Case*, WSJ, https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402, (dostęp: 10.11.2020).

Techjury.Net, *Infographic: How AI Is Being Deployed Across Industries*, Robotics Business Review, https://www.roboticsbusinessreview.com/ai/infographic-how-ai-is-being-deployed-across-industries/, (dostęp: 28.10.2020).

University College London, *'Deepfakes' Ranked As Most Serious AI Crime Threat*, https://www.ucl.ac.uk/news/2020/aug/deepfakes-ranked-most-serious-ai-crime-threat, (dostęp 4.11.2020).

Van der Veer R., *Terrorism in the age of technology*, https://www.clingendael.org/pub/2019/strategic-monitor-2019-2020/terrorism-in-the-age-of-technology, (dostęp: 18.09.2020).

Ware J., *Terrorist groups, artificial intelligence, and killer drones,* https://warontherocks.com/2019/09/terrorist-groups-artificial-intelligence-and-killer-drones, (dostęp: 21.09.2020).

Zegart A., *In The Deepfake Era, Counterterrorism Is Harder*, The Atlantic, https://www.theatlantic.com/ideas/archive/2019/09/us-intelligence-needs-another-reinvention/597787/, (dostęp: 17.11.2020).