Aleksander Ksawery Olech

Alan Lis

TECHNOLOGIA I TERRORYZM

SZTUCZNA INTELIGENCJA W DOBIE ZAGROŻEŃ TERRORYSTYCZNYCH

INSTYTUT NOWEJ EUROPY

ZESPÓŁ

AUTORZY:

Aleksander Ksawery Olech

Alan Lis

ANALITYCY:

Sylwia Gliwa

Natalia Matiaszczyk

Aymen Gatri

Jakub Klepek

Cosmin Timofte

WSPARCIE ANALITYCZNE:

Małgorzata Cichy

Stanisław Apriłaszwili

MAPY I GRAFIKI:

Natalia Matiaszczyk

Aleksander Ksawery Olech

WSPARCIE JĘZYKOWE:

Małgorzata Cichy

Cosmin Timofte

SPIS TREŚCI

ABSTRAKT

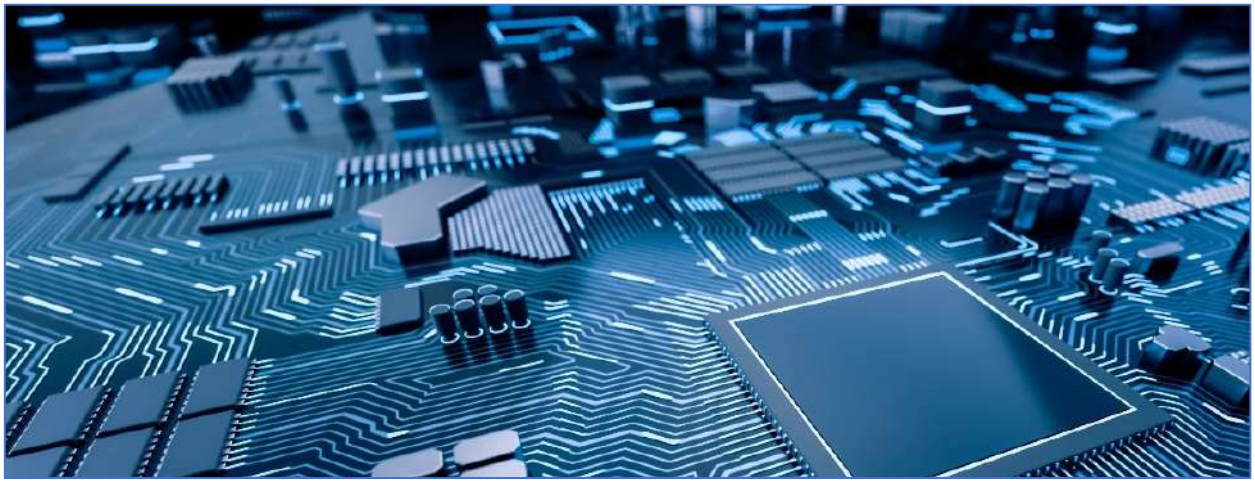
Rewolucje technologiczne są ważnym elementem postępu ludzkości mając wpływ zarówno na pokojowe rozwiązania służące cywilizacjom, jak i konflikty zbrojne. Zaawansowane technologie doprowadziły do gruntownych zmian w relacjach pomiędzy państwami, a pojawienie się m.in. broni jądrowej jest jednym z wielu przykładów, gdzie rozwój militarny miał wpływ na budowanie potęgi poszczególnych mocarstw. Współczesne wyzwania dla bezpieczeństwa są związane m.in. z zagrożeniami hybrydowymi, dezinformacją oraz szkodliwym wykorzystywaniem nowych technologii, w tym sztucznej inteligencji (SI).

Raport rozpoczyna się od przedstawienia definicji SI i jej wpływu na współczesny świat. Wśród niezliczonych korzyści, szczególny nacisk położono na sektor handlu, opieki zdrowotnej i wojska, jednocześnie opisano wyzwania, jakie stwarza próba ustanowienia zasad etycznych dotyczących prowadzenia badań nad SI oraz jej wady w zakresie przyszłego zatrudniania pracowników. Następnie przeanalizowano wysiłki trzech konkurujących ze sobą światowych potęg (USA, Chiny i Rosja) w celu zdobycia przewagi w nowym, pozornym wyścigu zbrojeń o dominację w zakresie SI, gdzie poszczególne państwa będą się starać wykorzystać jej potencjał do zwiększenia potęgi gospodarczej i militarnej.

Wszechobecna integracja technologii ze społeczeństwem oraz jej wykorzystywanie przez podmioty niepaństwowe, stawia w centrum uwagi koncepcję „zagrożeń hybrydowych". W raporcie zbadano ich nieuchwytny charakter oraz strategie, które stają się częścią rewolucyjnego typu wojny, obejmującej zarówno konwencjonalne, jak i niekonwencjonalne współczesne taktyki walki. Uwagę poświęcono także organizacjom terrorystycznym szczegółowo opisując ich działalność. W rozważaniach wzięto pod uwagę motywacje i strategiczne korzyści, jakie terroryści uzyskaliby wykorzystując

technologie wspierane przez sztuczną inteligencję, którą wykradli lub została im dostarczona przez inne podmioty. Ujęto przykłady obejmujące potencjał poszczególnych grup terrorystycznych w celu przeprowadzenia zamachów, zwłaszcza korzystając z dronów, pokonując mechanizmy obronne państw lub atakując infrastrukturę krytyczną, a ponadto wskazano na potencjalne zastosowanie technologii w celach rekrutacyjnych. Podjęto się również weryfikacji ryzyka wykorzystywania druku 3D przez organizacje terrorystyczne, co wiąże się ze stworzeniem broni domowej roboty, która jest prawie niemożliwa do wykrycia przez służby bezpieczeństwa.

Na koniec został zbadany aspekt sztucznej inteligencji jako technologii podwójnego zastosowania. Studium przypadków autonomicznych pojazdów i tzw. deep fake'ów ma kluczowe znaczenie dla zrozumienia zarówno korzystnych, jak i negatywnych zastosowań sztucznej inteligencji. Po weryfikacji zagrożeń i dostępnych danych, zaprezentowano zmiany w środowisku bezpieczeństwa oraz korzyści dla społeczeństwa płynące z autonomicznych pojazdów, przy jednoczesnym podkreśleniu ryzyka ich zhakowania, co stanowi fizyczne zagrożenie z racji ich możliwego wykorzystania przez zorganizowane grupy przestępcze lub organizacje terrorystyczne. Raport kończy się szeregiem rekomendacji dotyczących przeciwdziałania poddanym analizie zagrożeniom.



Słowa kluczowe: SI, terroryzm, technologia, hybrydowy, bezpieczeństwo, drony,

WSTĘP

Terroryzm jest współcześnie postrzegany jako główne zagrożenie dla globalnego porządku. Negatywny charakter tego zjawiska, nawet w postaci tylko jednego przeprowadzonego ataku, potrafi całkowicie zaburzyć funkcjonowanie państw i organizacji międzynarodowych. Destrukcyjne efekty działalności terrorystycznej mają wpływ na sytuację ekonomiczną, polityczną, społeczną oraz utrudniają proces wzmacniania potencjału bezpieczeństwa. Niespodziewany atak terrorystyczny stawia pod znakiem zapytania skuteczność organizacji struktur antyterrorystycznych oraz metody zwalczania takich niebezpieczeństw.

Terroryzm jako forma walki, cechujący się manifestacją przekonań i poglądów o charakterze politycznym, religijnym, ideologicznym lub jednej sprawy, poprzez agresję i przemoc przeciw państwu, była wykorzystywana wielokrotnie w historii ludzkości. Na przestrzeni lat zmieniały się jedynie narzędzia, z których mogli korzystać terroryści. Obecnie wciąż dochodzi do ataków przy wykorzystaniu broni białej, ale terroryści korzystają także z materiałów wybuchowych, karabinów maszynowych oraz pocisków sterowanych. Rozrost rynku broni doprowadził do militaryzacji grup terrorystycznych, które z powodzeniem zdobywają nowe środki bojowe, a następnie wykorzystują je w atakach terrorystycznych. Taki stan rzeczy oddziałuje bezpośrednio na bezpieczeństwo poszczególnych państw i społeczeństw.

Postęp technologiczny ma bez wątpienia ogromny wpływ na życie każdego człowieka. Znacząco ułatwia życie codziennie, oferując szybki transport, łatwe zakupy, kontakt przez Internet, a także loty w kosmos. Jednocześnie rozwijane są takie gałęzie jak wojskowa czy informatyczna. Technologia staje się wszechobecna, a jej możliwości, w kontekście rozwoju przyszłości, są w ludzkim postrzeganiu praktycznie nieograniczone. Tym samym pojawiające się projekty wykorzystujące sztuczną inteligencję oraz

ulepszanie systemów symulujących ludzkie zachowania, są dla wielu naturalnym procesem progresu, który czyni ludzkość.

Sztuczna inteligencja jest postrzegana jako produkt przyszłości, który może być przełomem w rozwoju technologicznym. Jej użycie ma prowadzić do znaczącego przyśpieszenia wszelkich procesów, przy wykorzystaniu maszynowych (komputerowych) funkcji poznawania świata poprzez uczenie się oraz rozwiązywanie problemów. Głównym celem jest opracowanie systemu, którym można sterować, ale byłby on zależny od człowieka. Byłaby to forma wykorzystania wysoko zaawansowanego organizmu, który z powodzeniem może realizować procesy naturalnie przypisane ludziom. Co więcej, sztuczna inteligencja – w oparciu o niezliczoną ilość danych – podejmowałaby najlepsze i najskuteczniejsze decyzje w trakcie realizowanych zadań. Wydaje się, że jest to idealny przykład rozwiniętej technologii, która znacząco wzmocniłaby potencjał ludzki. Wykorzystanie takich rozwiązań informatycznych miałoby z pewnością zastosowanie w każdej z dziedzin życia, także w ramach prowadzonych wojen lub akcji terrorystycznych.

Należy podkreślić, że zaawansowane systemy informatyczne mogą zostać użyte nie tylko w celu, aby wygrać wyścig o miano najbardziej rozwiniętego technologicznie kraju. Jest to także element rywalizacji zbrojnej, gdzie korzystając z dronów, sterowanych rakiet, a także systemów dowodzenia można uzyskać przewagę militarną. Z drugiej strony, spopularyzowanie i regularne wykorzystanie nowego rodzaju broni, doprowadzi do tego, iż zdobędą ją także inne podmioty, zarówno państwowe jak i niepaństwowe. Realnym jest, że terroryści uzyskają lub otrzymają technologię, za pomocą której mogliby przeprowadzić ataki terrorystyczne. Już teraz wykorzystują choćby drony oraz szkodliwe oprogramowania komputerowe (cyberterroryzm).

Zaawansowana technologia w rękach organizacji terrorystycznych stanowi poważne zagrożenie dla bezpieczeństwa wielu państw. Dodatkowo, na nowo identyfikuje

charakter prowadzenia konfliktów zbrojnych, przez co zwiększa się poziom zagrożenia terrorystycznego. Oprócz współczesnych niebezpieczeństw pojawiłyby się wyzwania o charakterze informatycznym, gdzie terroryści mogliby korzystać z wysokorozwiniętych technologii, a być może również ze sztucznej inteligencji.

Niniejszy raport stanowi wszechstronny przegląd badań dotyczących rozwijających się technologii, sztucznej inteligencji, terroryzmu, zagrożeń hybrydowych, dezinformacji oraz największych organizacji terrorystycznych na świecie. Jest to swego rodzaju przewodnik, który ma na celu ukazanie wielu niebezpieczeństw przy użyciu nowoczesnych narzędzi, również przez grupy terrorystyczne. Oprócz tego, z uwagi na rywalizację pomiędzy USA, Chinami, Rosją oraz państwami na Bliskim Wschodzie, a tym samym trwający wyścig technologiczny, trzeba stale analizować pojawiające się wyzwania dla bezpieczeństwa globalnego. Bez wątpienia jednym z największych problemów, przed którym stoi ludzkość, jest cel i sposób użycia zaawansowanych systemów. Jeśli istnieje ryzyko, że zabójcza broń lub nowe systemy będą wciąż rozwijanie na rzecz walki pomiędzy mocarstwami lub zostaną wykorzystane przez terrorystów w celu naruszenia międzynarodowego porządku i realizacji swoich żądań, to należy reagować już teraz. Kluczem do skutecznego realizowania strategii na rzecz bezpieczeństwa jest zapobieganie. Analiza i określenie zagrożeń są pierwszym etapem w procesie zwalczania terroryzmu.

Zagrożenie w postaci organizacji terrorystycznych posiadających i korzystających z zaawansowanych systemów nie wydaje się być bardzo odległe. Tym jednak różnią się przewidywania od rzeczywiści – dostrzegamy niebezpieczeństwo dopiero wtedy, gdy staje się realne. Terroryzm ma wiele definicji, tak samo jak wiele państw w różny sposób określa zagrożenia terrorystyczne. Prawdą jest, że niektóre działania mogą zostać określone przez jedno mocarstwo terroryzmem, a przez inne jako działania militarne na rzecz bezpieczeństwa. Tak samo realnym jest wykorzystanie organizacji terrorystycznych do realizacji celów któregoś z państw.

Niech poniższe opracowanie będzie jednym z etapów procesu naukowego mającego na celu określenie współczesnych relacji w środowisku bezpieczeństwa. Jest to ważne, dopóki sztuczna inteligencja nie jest jeszcze w rękach terrorystów, a światowe mocarstwa mają wciąż szansę na wykorzystanie zaawansowanych technologii do innych celów niż prowadzenie wojny.

SZTUCZNA INTELIGENCJA: DEFINICJA, ZALETY I WADY

W niniejszej sekcji zostanie przedstawiona ogólna idea kryjąca się pod pojęciem sztucznej inteligencji (SI). Szczególny nacisk zostanie położony na wyjaśnienie tego, czym właściwie jest sztuczna inteligencja i co kryje się pod tym terminem, jak również na omówieniu korzyści, jakie przynosi ona w sektorze handlu, medycynie i kwestiach militarnych. Dla zachowania równowagi zostaną również przedstawione oraz wyjaśnione niedogodności i wyzwania jakie SI może stwarzać, a jako przykłady zobrazowano problemy etyczne i zwiększanie bezrobocia, do którego może się ona przyczyniać.

Definicja 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]. 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 zachowaniami, takie jak zdolność do uczenia się, autokorekty lub rozumienia języka[6]. Systemy oparte na sztucznej inteligencji mogą być oparte na oprogramowaniu i działać w świecie wirtualnym (przykładem są tutaj systemy rozpoznawania twarzy i mowy, czy też oprogramowanie przeznaczone do analizy

[1]McKinsey & Company, 2017. *Artificial Intelligence And Southeast Asia's Future*. [online] s.4. Available at: 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.
[2] Sayler, K., 2020. *Artificial Intelligence And National Security*. [online] <https://fas.org/sgp/crs/natsec/R45178.pdf>, dostęp: 11.11.2020.
[3] Sayler, K., 2020. *Artificial Intelligence And National Security*. [online] <https://fas.org/sgp/crs/natsec/R45178.pdf>, dostęp: 11.11.2020.
[4] Moy, G., Shekh, S., Oxenham, M. and Ellis-Steinborner, S., 2020. *Recent Advances In Artificial Intelligence And Their Impact On Defence*. [online] <https://www.dst.defence.gov.au/sites/default/files/publications/documents/DST-Group-TR-3716_0.pdf>, dostęp 16.10.2020.
[5] Builtin.com. n.d. *What Is Artificial Intelligence? How Does AI Work?*. [online] Available at: <https://builtin.com/artificial-intelligence>, dostęp: 1.11.2020.
[6] Techjury.Net, 2019. *Infographic: How AI Is Being Deployed Across Industries*. [online] Robotics Business Review. <https://www.roboticsbusinessreview.com/ai/infographic-how-ai-is-being-deployed-across-industries/>, dostęp: 28.10.2020.

obrazu), jak również być wbudowane w urządzenia sprzętowe (autonomiczne pojazdy, drony itp.)[7].

Istnieją różne rodzaje sztucznej inteligencji. Szczególnie interesującym przykładem jest szkolenie maszynowe. Jest to zdolność do uczenia lub przystosowywania się do danego środowiska (w przypadku robotów) w taki sposób, aby urządzenia wyposażone w sztuczną inteligencję 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, dwa główne z nich to tzw. uczenie się nadzorowane i tzw. uczenie się bez nadzoru[8]. Urządzenia zdolne do samouczenia się, mogą prognozować przyszłe zachowania lub wyniki projektu, a wszystko to bez potrzeby ingerencji człowieka. Chociaż samo 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].

[7]Bird, E., Fox-Skelly, J., Jenner, N., Larbey, R., Weitkamp, E. and Winfield, A. *The Ethics Of Artificial Intelligence: Issues And Initiatives*. Brussels 2020.
[8] Moy, G., Shekh, S., Oxenham, M. and Ellis-Steinborner, S., 2020. *Recent Advances In Artificial Intelligence And Their Impact On Defence*. [online] <https://www.dst.defence.gov.au/sites/default/files/publications/documents/DST-Group-TR-3716_0.pdf>, dostęp: 16.10.2020.
[9]Bird, E., Fox-Skelly, J., Jenner, N., Larbey, R., Weitkamp, E. and Winfield, A. *The Ethics Of Artificial Intelligence: Issues And Initiatives*. Brussels 2020.
[10] Techjury.Net, 2019. *Infographic: How AI Is Being Deployed Across Industries*. [online] Robotics Business Review. <https://www.roboticsbusinessreview.com/ai/infographic-how-ai-is-being-deployed-across-industries/>, dostęp: 28.10.2020.

Korzyści wynikające z wykorzystania sztucznej inteligencji

Pożytek z zastosowania sztucznej inteligencji jest bardzo dużo i poprawiają one jakość życia ludzi poprzez wiele, różnorodnych zastosowań. Istotnie, sztuczna inteligencja ma – i z pewnością nadal będzie miała – ogromny wpływ na życie ludzi, znacząco zmieniając ich codzienną rzeczywistość. SI stanowi pozytywną zmianę na wielu różnych poziomach w całym szeregu branż, dziedzin i dyscyplin, takich jak edukacja, media, rolnictwo czy bankowość. Niestety, z uwagi na fakt, iż zakres korzyści w tych sektorach i poza nimi jest zbyt szeroki, aby można go było opisać w tej publikacji, walory płynące z inwestowania w sztuczną inteligencję zostaną pokrótce przedstawione na przykładzie trzech wybranych sektorów: handlu, medycyny i wojska.

Sektor handlu

Sektor handlu został w ostatnich latach znacząco zmieniony przez SI. Sztuczna inteligencja pozwoliła przedsiębiorstwom, które wprowadziły tę technologię do swojej działalności, uzyskać przewagę finansową nad firmami, które zdecydowały się na bardziej tradycyjne lub konserwatywne prowadzenie interesów. Sztuczna inteligencja sprawdziła się w sektorze handlu i pozostanie w nim, dlatego też przedsiębiorstwa, które obecnie z niej nie korzystają, będą prawdopodobnie musiały zdecydować się na jej wprowadzenie, aby pozostać konkurencyjne.

Handel jest jedną z branż wyjątkowo „bogatych" w dane, z ogromną ilością czynników, które wpływają na bieżące i nadchodzące trendy oraz decyzje klientów. Wyjątkowo trudno jest zrozumieć – i przewidzieć – tę dynamikę, ale sztuczna inteligencja oferuje sprzedawcom pomoc, której potrzebują, aby to zrobić. Algorytmy SI są w stanie przeanalizować znacznie więcej danych, niż może przetworzyć ludzki mózg, znacznie szybciej i z mniejszym prawdopodobieństwem błędu, niż w przypadku ludzi. Ponadto sztuczna inteligencja może być wykorzystywana do celów wykrywania zmian

upodobań klientów, poszukiwania niepozornych wzorców danych, pozwalając tym samym sprzedawcom zaoferować „właściwą promocję, we właściwym czasie, właściwej osobie i na właściwym urządzeniu”[11]. Może również rozpoznawać i przewidywać nadchodzące trendy – a wszystko to w sposób bardziej efektywny, skuteczny i w krótszym czasie niż ludzie. Ostatecznie sztuczna inteligencja może przyspieszyć proces decyzyjny i pomóc w podejmowaniu bardziej świadomych decyzji, umożliwiając w ten sposób przedsiębiorstwom prosperowanie na wyższym poziomie.

Poza tym, SI może być wykorzystywana w logistyce i optymalizacji łańcuchów dostaw, przyczyniając się do oszczędzania czasu i środków finansowych.

Sektor medyczny

Istnieje wiele przykładów ilustrujących, jak sztuczna inteligencja, wraz z innymi osiągnięciami technologicznymi, może być wykorzystywana w medycynie i sektorze opieki zdrowotnej. Chociaż tylko kilka z nich zostanie tu przedstawionych, należy zaznaczyć, że korzyści płynące z SI dla tego sektora jest zdecydowanie więcej. Kilka godnych uwagi przykładów, oprócz omówionych poniżej, to na przykład poprawa doświadczenia szpitalnego pacjentów poprzez sprawniejsze, niż w przypadku ludzi, wykonywanie niektórych zadań administracyjnych, zarządzanie danymi i wywiadem medycznym pacjentów, a nawet pomoc w operacjach (liczba operacji wspomaganych przez roboty w ostatnich latach niezwykle wzrosła). Ponadto sztuczna inteligencja obniża również koszty systemu opieki zdrowotnej[12,13].

[11] Saker, R., 2020. *The Impact Of Artificial Intelligence In Retail*. [online] My Total Retail. <https://www.mytotalretail.com/article/the-impact-of-artificial-intelligence-in-retail/>, dostęp: 25.10.2020].
[12] University of California, 2016. *Big Data, Analytics & Artificial Intelligence. The Future Of Health Care Is Here*. [online] San Francisco. Available at: <https://www.gehealthcare.com/static/pulse/uploads/2016/12/GE-Healthcare-White-Paper_FINAL.pdf>, dostęp: 9.11.2020.
[13] Daley, S., 2020. *32 Examples Of AI In Healthcare That Will Make You Feel Better About The Future*. [online] Built In. <https://builtin.com/artificial-intelligence/artificial-intelligence-healthcare>, dostęp: 22.10.2020.

Jedną z kluczowych korzyści płynących z funkcji, jakie sztuczna inteligencja pełni w opiece zdrowotnej, jest usprawnienie procesu diagnostycznego – w istocie, algorytmy SI są w stanie diagnozować choroby w sposób dokładniejszy i szybszy niż człowiek. Przykładem tego jest zastosowanie przez mikrobiologów klinicznych pracujących w szpitalu akademickim Beth Israel Deaconess Medical Centre na Uniwersytecie Harvarda mikroskopów wspomaganych sztuczną inteligencją do diagnozowania chorób krwi[14]. Dzięki zastosowaniu sprzętu wspomaganego SI byli oni w stanie zrobić to szybciej niż przeciętnie, a tym samym zwiększyli oni szanse pacjentów na powrót do zdrowia. Mikrobiolodzy „nauczyli" sprzęt wyposażony w sztuczną inteligencję rozpoznawać specyficzne bakterie (jedną z nich była E. coli), który po „przeszkoleniu" osiągnął ponad 90% dokładności. „Wraz z dalszym rozwojem i szkoleniem [...] platformy wspomagane przez sztuczną inteligencję mogłyby być w przyszłości wykorzystywane jako w pełni zautomatyzowany system klasyfikacji chorób"[15]. Ponadto, sztuczna inteligencja mogłaby poniekąd rozwiązać problem niedoboru naukowców w tym sektorze (oczekuje się, że w nadchodzących latach będzie on doświadczał jeszcze większego problemu z niewystarczającą liczbą wysoko wykwalifikowanego personelu niż obecnie, na przykład w USA).

Innym zastosowaniem sztucznej inteligencji w medycynie jest pomoc w opracowywaniu nowych leków. SI może zaoferować firmom biotechnologicznym i biofarmaceutycznym dokładniejsze i skuteczniejsze sposoby prowadzenia niezbędnych badań. Na przykład, kanadyjska firma Deep Genomics wykorzystuje platformę SI, która pomaga badaczom w szybszym znajdowaniu odpowiednich kandydatów do testowania

[14] Mitchell, J., 2017. *BIDMC Researchers Use Artificial Intelligence To Identify Bacteria Quickly And Accurately*. [online] Bidmc.org. <https://www.bidmc.org/about-bidmc/news/bidmc-researchers-use-artificial-intelligence-to-identify-bacteria-quickly-and-accurately>, dostęp: 4.11.2020.
[15] Mitchell, J., 2017. *BIDMC Researchers Use Artificial Intelligence To Identify Bacteria Quickly And Accurately*. [online] Bidmc.org. <https://www.bidmc.org/about-bidmc/news/bidmc-researchers-use-artificial-intelligence-to-identify-bacteria-quickly-and-accurately>, dostęp: 4.11.2020.

leków rozwojowych, co z kolei znacznie skraca proces – potencjalnie ratując więcej istnień ludzkich – jak również zmniejsza nakłady finansowe[16].

Poza powyższym, sztuczną inteligencję wykorzystano również do pomocy w zwalczaniu rozprzestrzeniania się pandemii COVID-19, czego przykład zostanie przedstawiony w sekcji poświęconej rozwojowi SI przez Chiny.

Sektor wojskowy

Rosnący potencjał sztucznej inteligencji może mieć istotne konsekwencje dla bezpieczeństwa narodowego. W związku z tym wiele krajów zaangażowało się w opracowywanie różnych zastosowań SI do celów wojskowych. Obecnie sztuczna inteligencja jest wykorzystywana w dziedzinie operacji informacyjnych, gromadzenia i analizy danych wywiadowczych, logistyki, jak również w całkowicie lub częściowo autonomicznych pojazdach. Co więcej, SI została już włączona do operacji wojskowych, na przykład w Syrii i Iraku.

Spośród wielu możliwych przykładów, które można tu przytoczyć, omówiony zostanie postęp w rozpoznawaniu i analizie obrazu[17], a także jego implikacje dla sił zbrojnych. Wśród innych obszarów, rozwój SI w tym zakresie znajdzie szczególnie adekwatne miejsce w operacjach nadzoru i monitorowania zagrożeń. Operacje te wymagają zwykle długich godzin poświęconych na monotonne przeszukiwanie powtarzających się obrazów bądź nagrań. Ponieważ sztuczna inteligencja jest w stanie analizować obrazy podobnie do tego, jak robi to ludzki mózg, a nawet jeszcze dokładniej niż ludzie są w stanie to robić, takie monotonne zadania mogą być lepiej wykonywane przez bezzałogowe pojazdy wyposażone w SI, które można wykorzystać np. do patrolowania

[16] Daley, S., 2020. *32 Examples Of AI In Healthcare That Will Make You Feel Better About The Future*. [online] Built In. <https://builtin.com/artificial-intelligence/artificial-intelligence-healthcare>, dostęp: 22.11.2020.
[17] Moy, G., Shekh, S., Oxenham, M. and Ellis-Steinborner, S., 2020. *Recent Advances In Artificial Intelligence And Their Impact On Defence*. [online] <https://www.dst.defence.gov.au/sites/default/files/publications/documents/DST-Group-TR-3716_0.pdf>, dostęp: 16.11.2020.

danych obszarów czy identyfikowania potencjalnych zagrożeń, a wszystko to przy wykonywaniu zadania ze zmniejszonym prawdopodobieństwem błędu, niż w przypadku człowieka. W istocie, sztuczna inteligencja może pomagać operatorom w wykrywaniu nietypowych wzorców w filmach i obrazach, umożliwiając im szybsze i bezpieczniejsze realizowanie misji, co dodatkowo zmniejsza ryzyko dla żołnierzy przebywających „w terenie". Przykładem zastosowania SI w omawianym obszarze jest *Project Maven*, prowadzony przez wojsko amerykańskie w celu identyfikacji potencjalnych wrogów[18].

Wyzwania w procesie rozwoju sztucznej inteligencji

Pomimo wielu korzyści związanych z SI, istnieje jeszcze druga strona jej rozwoju, którą również należy uwzględnić, a mianowicie ta dotycząca problemów i trudności, do których sztuczna inteligencja może się przyczynić. Kwestia ta zostanie wyjaśniona na dwóch przykładach: wątpliwości dotyczących obszaru etyki i możliwości przyczyniania się do zwiększenia bezrobocia przez SI.

Kwestie etyczne

Wraz z rozwojem SI pojawiają się pytania dotyczące kwestii etycznych i moralnych tej technologii. Kwestia etyki jest rzeczywiście jednym z najczęściej poruszanych tematów podczas omawiania negatywnych stron rozwoju SI. Technologia sztucznej inteligencji oferuje osobom będącym w jej posiadaniu potężne możliwości, które mogą być wykorzystane nie tylko do szlachetnych celów, ale również do wyrządzania szkody innym i być użyte jako środek do podejmowania wszelkich niemoralnych i niezgodnych z prawem działań, które jej operatorzy chcą, przy jej pomocy, wykonać. Dla przykładu, sztuczną inteligencję można wykorzystać do celów naruszania prywatności ludzi, poddając ich stronniczej i nadmiernej inwigilacji (sztuczna inteligencja jest w ten szczególny sposób nadużywana przez władze chińskie, co zostanie przedstawione w części po-

[18] Zostanie on omówiony nieco szerzej w części dotyczącej rozwoju sztucznej inteligencji przez USA.

święconej rozwojowi SI przez Chiny) lub naruszając wolność słowa (w Indiach narzędzia wyposażone w SI zostały wykorzystane do automatycznego usuwania treści – co zwiększa ryzyko cenzury).

Wykorzystanie SI w działaniach militarnych jest tematem wielu debat i dyskusji. Mimo, że od II wojny światowej siły zbrojne używają częściowo autonomicznych systemów, znaczący postęp w rozwoju sztucznej inteligencji spowodował, że wykorzystanie automatyki wojskowej osiągnęło punkt krytyczny[19]. Chociaż, jak wskazano powyżej, SI ma potencjał, aby wnieść wiele udoskonaleń do sektora wojskowego, które mogą być bardzo pomocne dla żołnierzy i pracowników cywilnych sił zbrojnych, należy pamiętać, że sztuczna inteligencja jest również uważana za zmieniającą działania wojenne w takim samym stopniu, jak „broń jądrowa, samoloty, komputery i biotechnologia"[20]. Stosowanie sztucznej inteligencji w działaniach wojennych skutkuje co najmniej kilkoma kwestiami moralnymi i etycznymi. Jedną z nich jest obawa, że systemy wyposażone w SI i wykorzystywane w walce, pozbawione ludzkiego osądu, mogą naruszać zasady międzynarodowego prawa humanitarnego, na przykład poprzez naruszenie zasady proporcjonalności lub poprzez bezprawne atakowanie cywilów, omyłkowo przyjmując ich za bojowników wroga. To z kolei prowadzi do kolejnej kwestii związanej z użyciem SI w działaniach wojennych – odpowiedzialności. Mianowicie, kto powinien być odpowiedzialny za zbrodnie wojenne popełnione przez autonomiczny system – osoba, która go zaprogramowała, ta, która go obsługuje, czy przełożony nadzorujący operację. Pomimo że kwestia ta była już wielokrotnie poruszana, stanowi ona nadal otwartą debatę, z różnymi odpowiedziami na powyższe kwestie.

W związku z tym konieczne jest, aby rozwój sztucznej inteligencji – zarówno do celów cywilnych, jak i wojskowych – był prowadzony zgodnie z określonymi zasadami

[19] Bird, E., Fox-Skelly, J., Jenner, N., Larbey, R., Weitkamp, E. and Winfield, A. *The Ethics Of Artificial Intelligence: Issues And Initiatives*. Brussels 2020.
[20] Allen, G. and Chan, T., 2017. *Artificial Intelligence And National Security*. [online] Belfer Center for Science and International Affairs, s.1. <https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf>, dostęp: 8.11.2020.

i normami. Jednym z krajów, które w niedalekiej przeszłości podkreśliły swoje zaangażowanie na rzecz etycznego rozwoju i wykorzystania SI, są Stany Zjednoczone. Zgodnie z oświadczeniem wydanym 31 października 2019 r., przez doradców Pentagonu należących do Rady Innowacji Obronnych, istnieje potrzeba uwzględnienia zasad etycznych rozwoju sztucznej inteligencji[21]. Grupa szesnastu ekspertów zaproponowała pięć głównych zasad, którymi należy się kierować przy rozwoju SI, pośród których znalazły się odpowiedzialność, sprawiedliwość, możliwość identyfikacji, wiarygodność, a także zdolność do zarządzania systemami SI. Najbardziej oczywistym przesłaniem jest to, że to ludzie są odpowiedzialni za rozwój, rozmieszczenie i użytkowanie maszyn wyposażonych w SI[22]. Pentagon stale współpracuje z ekspertami w celu uniknięcia ewentualnych szkód spowodowanych niewłaściwym użyciem technologii przez żołnierzy USA, a także, amerykańskiej technologii udoskonalonej i użytkowanej przez inne kraje. Można więc argumentować, że Stany Zjednoczone chcą prowadzić przejrzyste badania nad rozwojem sztucznej inteligencji, jeśli chodzi o etykę, i jednocześnie opowiadają się za rozwojem SI z poszanowaniem zasad państwa prawa.

Istnieją jednak jeszcze inne inicjatywy prowadzone przez różne organizacje i instytucje w wielu krajach, mające na celu zapewnienie etycznego i moralnego rozwoju SI we wszystkich sektorach. Cel taki obrały m.in.: niemiecki Institute for Ethics in Artificial Intelligence, brytyjskie Institute for Ethical Artificial Intelligence in Education oraz Institute for Ethical AI & Machine Learning.

Co więcej, w zeszłym roku Unia Europejska (UE) opublikowała swój zestaw wymogów, które musi spełniać SI, aby być uznana za wiarygodną. Dość obszerny wykaz zaleceń zaproponowanych przez UE obejmuje: nadzór ludzki, solidność techniczną

[21] U.S. Dept of Defense, 2020. *DOD Adopts Ethical Principles for Artificial Intelligence*, [online] https://www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/, dostęp: 12.10.2020.
[22] U.S. Dept of Defense, 2020. *DOD Adopts Ethical Principles for Artificial Intelligence*, [online] Available at: https://www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/, dostęp: 12.10.2020.

gwarantującą bezpieczeństwo, ochronę prywatności i zarządzanie danymi, przejrzystość, różnorodność, niedyskryminację i sprawiedliwość, dobrostan społeczny i środowiskowy oraz odpowiedzialność[23].

Biorąc pod uwagę wszystkie przedstawione argumenty i perspektywy, warto zakończyć tę część stwierdzeniem, że rozwój SI musi odbywać się w sposób budujący zaufanie i zrozumienie oraz respektujący prawa człowieka i obywatela[24] w imię zagwarantowania bezpiecznego wykorzystania jego potencjału.

Potencjalny wzrost bezrobocia

Prawdą jest, że rozwijający się sektor SI oznacza stałe zapotrzebowanie na coraz większą liczbę naukowców, programistów, etc.; jednakże osoby zatrudnione w innych branżach niekoniecznie podzielają entuzjazm dla sztucznej inteligencji. Należy zaznaczyć, że rozwój SI w wielu sektorach zmniejsza zapotrzebowanie na pracowników, co ostatecznie może prowadzić do zwiększenia bezrobocia.

Ponieważ sztuczna inteligencja jest w stanie wykonywać wiele zadań dokładniej, taniej i szybciej niż ludzie, dużo zadań jest automatyzowanych do tego stopnia, że zmniejsza się zapotrzebowanie na pracowników. SI może nie powodować masowego bezrobocia w wyniku jej wdrożenia, jednakże może – na dużą skalę – zastąpić ludzi wykonujących prace wymagające niskich kwalifikacji, którzy, ze względu na brak bardziej zaawansowanych umiejętności, mogą mieć ograniczone szanse na znalezienie zatrudnienia w innym miejscu. Jak wynika z raportu opublikowanego przez McKinsey Global Institute w 2017 r. technologie opracowane do tej pory mogłyby zautomatyzować ponad połowę zadań wykonywanych w ramach pracy w takich krajach jak Tajlandia

[23] Bird, E., Fox-Skelly, J., Jenner, N., Larbey, R., Weitkamp, E. and Winfield, A. *The Ethics Of Artificial Intelligence: Issues And Initiatives*. Brussels 2020.
[24] Dignum, V., 2018. *Ethics in artificial intelligence: introduction to the special issue*. Ethics and Information Technology, 20, s. 1-3.

(55%), Indonezja (52%) czy Malezja (51%)[25]. Choć zastąpienie człowieka sztuczną inteligencją nie nastąpi natychmiastowo, to jednak w miarę upływu czasu może pozostawić dużą liczbę osób bez pracy.

Aby zilustrować, że sztuczna inteligencja może również powodować bezrobocie w krajach bogatszych niż wymienione powyżej, należy zwrócić uwagę na USA. Od 2000 roku w kraju tym likwidacji uległo ponad 5 milionów miejsc pracy w fabrykach. Los Angeles Times przewidział, że wraz z postępem ery autonomicznych samochodów może dojść do utraty kolejnych 5 milionów miejsc pracy w całym kraju, a większość zwolnionych kierowców „będzie należeć do tej samej grupy demograficznej"[26] co pracownicy fabryki, którzy zostali wcześniej zwolnieni, ponieważ ich praca została zautomatyzowana. Aby jeszcze bardziej podkreślić to zjawisko, można wspomnieć, iż wiele miast na całym świecie zadeklarowało przejście na korzystanie z autonomicznych autobusów w przyszłości, wśród nich Nowy Jork, Singapur czy Edynburg[27]. Kierowcy nie będą jednak jedynymi, którzy będą musieli szukać nowego zatrudnienia – dołączą do nich prawdopodobnie m.in. pracownicy stacji paliw. Należy również podkreślić, że nie tylko pracownicy fizyczni stoją w obliczu możliwości utraty źródła dochodu, ponieważ sztuczna inteligencja wykazała już swój potencjał w zakresie redukcji miejsc pracy także dla pracowników umysłowych, np. w urzędach pocztowych i sektorze obsługi klienta[28].

[25] McKinsey & Company, 2017. *Artificial Intelligence And Southeast Asia's Future*. [online] s.4. 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.
[26] Greenhouse, S., 2016. *Op-Ed: Autonomous Vehicles Could Cost America 5 Million Jobs. What Should We Do About It?*. [online] Los Angeles Times. <https://www.latimes.com/opinion/op-ed/la-oe-greenhouse-driverless-job-loss-20160922-snap-story.html>, dostęp: 12 .10.2020.
[27] Bird, E., Fox-Skelly, J., Jenner, N., Larbey, R., Weitkamp, E. and Winfield, A. *The Ethics Of Artificial Intelligence: Issues And Initiatives*. Brussels 2020.
[28] Rotman, D., 2013. *How Technology Is Destroying Jobs*. [online] MIT Technology Review. <https://www.technologyreview.com/2013/06/12/178008/how-technology-is-destroying-jobs/>, dostęp: 24.10.2020.

KRAJE, KTÓRE ROZWIJAJĄ SI I ICH WYŚCIG TECHNOLOGICZNY

Międzynarodowy wyścig na rzecz rozwoju SI

Jak wskazano powyżej, sztuczna inteligencja jest dziedziną technologii, która niesie istotne zmiany dla wielu sektorów, w tym dla sektora bezpieczeństwa, zarówno na poziomie międzynarodowym, jak i krajowym. Wiele krajów bierze udział w międzynarodowym wyścigu na rzecz opracowania najbardziej zaawansowanych systemów SI, zarówno do celów wojskowych, jak i cywilnych.

Wśród krajów, które rozwijają SI znajdują się m.in. Stany Zjednoczone, Chiny, Rosja, Kanada, Niemcy, Wielka Brytania, Indie i Japonia. Każdy z nich ma swoją indywidualną ścieżkę rozwoju sztucznej inteligencji. Według wielu opracowań liderami tej rywalizacji są Stany Zjednoczone i Chiny, za którymi podąża Rosja. Zdecydowana większość pozostałych uczestników wyścigu ma trudności z konkurowaniem z którymkolwiek z tych trzech mocarstw. Z tego powodu, niektóre kraje starają się wysunąć na pierwszy plan, rozwijając konkretne obszary sztucznej inteligencji, czego przykładem jest Wielka Brytania, której władze ogłosiły w 2018 r., że planują, iż kraj ten stanie się światowym liderem w dziedzinie rozwoju „etycznej sztucznej inteligencji". Matthew

Gould, były brytyjski dyrektor generalny ds. technologii cyfrowych i mediów, stwierdził, że brytyjscy naukowcy mają „brać pod uwagę etykę [w rozwoju SI] na każdym kroku, a nie spychać ją na dalszy plan"[29]. Z kolei Niemcy, uznając, że potencjał ich pozaeuropejskich konkurentów jest o wiele większy, ogłosiły w 2018 roku, iż ich celem jest zostanie wiodącym ośrodkiem rozwoju SI w Europie[30].

Jednak nie tylko państwa silne i stabilne gospodarczo rozwijają SI. Również kraje mniejsze, takie jak Wietnam i Malezja, dostrzegły korzyści płynące z rozwoju sztucznej inteligencji i wykazały zainteresowanie rozwojem tej technologii we własnym zakresie.[31]

Rządy na całym świecie są świadome, że SI znacznie zmieni światową równowagę sił militarnych, a zmiana ta wpłynie na przekształcenia w globalnym krajobrazie politycznym. SI oferuje zastrzyk znacznej siły technologicznej i wojskowej dla mniejszych i słabszych państw (pod względem ich możliwości gospodarczych, liczby ludności lub potencjału wojskowego). Można więc argumentować, że sztuczna inteligencja z pewnością jest jednym z najpotężniejszych multiplikatorów sił w XXI wieku.

Spośród wszystkich krajów, które w ostatnich latach koncentrowały się na rozwoju SI, przedstawione zostaną tutaj Stany Zjednoczone, Chiny i Rosja, czyli trzy państwa, które są najczęściej postrzegane jako wiodące prym w jej rozwoju. Kraje te wydały ogromne sumy pieniędzy, chociaż trzeba podkreślić, że kwoty przeznaczone na rozwój sztucznej inteligencji przez Rosję są mniejsze niż w przypadku USA i Chin. Pomimo faktu, iż wysiłki każdego z wyżej wymienionych państw wymagają bardziej szczegółowych badań i weryfikacji, autorzy niniejszego raportu założyli, że kwestia zagrożenia ze

[29] Renstrom, J., 2018. *The UK Wants To Be The World Leader In Ethical AI*. [online] Slate. https://slate.com/technology/2018/08/the-u-k-wants-to-be-the-world-leader-in-ethical-a-i.html, dostęp: 6.11.2020.
[30] European Commission, n.d. 2020. *Germany AI Strategy Report*. [online] European Commission. <https://knowledge4policy.ec.europa.eu/ai-watch/germany-ai-strategy-report_en>, dostęp: 13.11.2020.
[31] McKinsey & Company, 2017. *Artificial Intelligence And Southeast Asia's Future*. [online] 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.

strony podmiotów niepaństwowych nadużywających i wykorzystujących sztuczną inteligencję do realizacji własnych celów, wymaga szczególnej uwagi i bardziej dogłębnej analizy w ramach niniejszego opracowania. Niemniej jednak, w pracy zawarto opisy rozwoju sztucznej inteligencji przez trzy kraje dominujące w tym globalnym wyścigu technologicznym.

Stany Zjednoczone

Można postawić tezę, że Stany Zjednoczone były największym beneficjentem ostatniej fali rozwoju technologicznego i nie powinno dziwić zatem, że są „domem" dla niektórych z największych i najważniejszych światowych firm technologicznych, do których zalicza się Apple, Facebook czy Google. Rozwój sztucznej inteligencji jest kolejnym etapem rozwoju cyfrowego, a podkreślając jego znaczenie prezydent Stanów Zjednoczonych Donald Trump powiedział, że „dalsze amerykańskie przywództwo w dziedzinie sztucznej inteligencji ma ogromne znaczenie dla utrzymania bezpieczeństwa gospodarczego i narodowego Stanów Zjednoczonych [...]".[32] Szereg sprawozdań, analiz, artykułów itp., potwierdza, że to Stany Zjednoczone przewodzą globalnemu wyścigowi na rzecz rozwoju SI, zarówno w jej konkretnych, bardziej specyficznych aspektach, jak i w ujęciu ogólnym[33,34,35,36].

---

[32] Srivastava, S., 2020. *State Of Artificial Intelligence In US: Becoming Technology Superpower*. [online] Analytics Insight. https://www.analyticsinsight.net/state-of-artificial-intelligence-in-us-becoming-technology-superpower/, dostęp: 25.10.2020.
[33] Center for Data Innovation, 2019. *Who Is Winning The AI Race: China, The EU Or The United States?*. [online] Who Is Winning the AI Race: China, the EU or the United States?. https://s3.amazonaws.com/www2.datainnovation.org/2019-china-eu-us-ai.pdf , dostęp: 2.10.2020.
[34] Lopez, C., 2020. *Where It Counts, U.S. Leads In Artificial Intelligence.* [online] defense.gov. https://www.defense.gov/Explore/News/Article/article/2269200/where-it-counts-us-leads-in-artificial-intelligence/, dostęp: 25.10.2020.
[35] Banerjee, I. and Sheenan, M., 2020. *America'S Got AI Talent: US' Big Lead In AI Research Is Built On Importing Researchers*. [online] macropolo.org. Dostępne pod linkiem: https://macropolo.org/americas-got-ai-talent-us-big-lead-in-ai-research-is-built-on-importing-researchers/?rp=e, dostęp: 25.10.2020.
[36]McKinsey & Company, 2017. *Artificial Intelligence And Southeast Asia's Future*. [online]. 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].

Rzeczywiście, w ciągu ostatnich lat władze Stanów Zjednoczonych udowodniły, z jaką powagą traktują rozwój SI. Wśród wielu przykładów, *The U.S. National Defense Strategy of 2018* wskazała sztuczną inteligencję jako jedną z technologii, które pozwolą USA „walczyć i wygrywać wojny przyszłości"[37]. Aby uniemożliwić Chinom i Rosji wyprzedzenie USA w wyścigu zbrojeń SI, w 2018 roku, w ramach Departamentu Obrony, utworzono Joint Artificial Intelligence Centre. Do jego głównych zadań należy, m.in. przyspieszenie procesu wdrażania i adaptacji sztucznej inteligencji [a także] obrona amerykańskiej infrastruktury krytycznej przed złośliwą działalnością cybernetyczną, która mogłaby spowodować znaczący incydent cybernetyczny[38]. Zaś w lutym 2019 roku prezydent Trump uruchomił American Artificial Intelligence Initiative, która ma „wspierać innowacje w dziedzinie sztucznej inteligencji, które z kolei mają zwiększyć dobrobyt, wzmocnić bezpieczeństwo narodowe i poprawić jakość życia Amerykanów"[39].

Co ciekawe, władze USA postanowiły nawiązać współpracę ze Zjednoczonym Królestwem i niedawno podpisały deklarację w sprawie współpracy w zakresie badań i rozwoju nad sztuczną inteligencją, poprzez którą chcą promować „wzajemne dobro, dobrobyt i bezpieczeństwo obecnych i przyszłych pokoleń"[40].

Stany Zjednoczone, podobnie jak inne kraje rozwijające sztuczną inteligencję, dokonują postępów w tej dziedzinie zarówno w celach wojskowych, jak i cywilnych, przy czym te ostatnie obejmują projekty, które mają także pomóc w walce z pandemią

[37] 2018. *Summary Of The 2018 National Defense Strategy Of The United States Of America*. s.3.
[38] Dostępne pod linkiem. https://dodcio.defense.gov/About-DoD-CIO/Organization/JAIC/, dostęp 22.10.2020.
[39] The White House Office of Science and Technology Policy, 2020. *American Artificial Intelligence Initiative: Year One Annual Reports*. s. iii.
[40] Deklaracja dostępna pod linkiem: https://www.state.gov/declaration-of-the-united-states-of-america-and-the-united-kingdom-of-great-britain-and-northern-ireland-on-cooperation-in-artificial-intelligence-research-and-development-a-shared-vision-for-driving/, dostęp: 20.10.2020.

COVID-19[41]. Wśród militarnego rozwoju SI przykładem są wysiłki podejmowane przez różne rodzaje amerykańskich sił zbrojnych na rzecz wprowadzenia półautonomicznych i w pełni autonomicznych pojazdów[42]. Niektóre testy zostały już przeprowadzone przez Siły Powietrzne USA (program Loyal Wingman), Armię (Robotic Combat Vehicles, z autonomicznymi funkcjami nadzoru, nawigacji i usuwania IED – improwizowanych ładunków wybuchowych[43]), lub Marynarkę Wojenną (Anti-Submarine Warfare Continuous Trail Unmanned Vessel, zwany „Sea Hunter", który, w przypadku pomyślnego wejścia do służby, „zapewniłby Marynarce Wojennej możliwość samodzielnej nawigacji na otwartym morzu, wymiany modułowej ładowności i koordynacji misji z innymi statkami bezzałogowymi"[44], przy zachowaniu możliwości nieprzerwanego operowania przez okres kilku miesięcy[45]). Co więcej, kilka lat temu wojsko amerykańskie wprowadziło program SI o nazwie „Project Maven", który wykorzystuje techniki nauki maszynowej, do pomocy amerykańskim żołnierzom w identyfikowaniu celów na filmach bądź zdjęciach wykonanych przez drony. „Project Maven" został wdrożony w różnych zakątkach Ziemi, na przykład na Bliskim Wschodzie i w Afryce[46].

Innym przykładem zastosowania SI przez siły zbrojne USA jest nowy system przeznaczony dla Sił Powietrznych, który został uruchomiony w tym roku, zwany Advanced Battle Management System (ABMS). ABMS obejmuje wykorzystanie sił zbrojnych na ziemi, w powietrzu i na morzu poprzez połączenie w cyberprzestrzeni (przy użyciu 4G i 5G), która jest wspierana przez sztuczną inteligencję i nadzorowana przez

---

[41] Lopez, C., 2020. *Where It Counts, U.S. Leads In Artificial Intelligence*. [online] defense.gov. https://www.defense.gov/Explore/News/Article/article/2269200/where-it-counts-us-leads-in-artificial-intelligence/, dostęp: 25.10.2020.
[42] Congressional Research Service, 2020. *Artificial Intelligence And National Security*. s.13.
[43] Congressional Research Service, 2020. *Artificial Intelligence And National Security*. s.13.
[44] Congressional Research Service, 2020. *Artificial Intelligence And National Security*. s.14.
[45] Defense Advanced Research Projects Agency, 2018. *ACTUV "Sea Hunter" Prototype Transitions to Office of Naval Research for Further Development.* [online] https://www.darpa.mil/news-events/2018-01-30a, dostęp: 18.10.2020.
[46] McLeary, P., 2018. *Pentagon'S Big AI Program, Maven, Already Hunts Data In Middle East, Africa*. [online] <https://breakingdefense.com/2018/05/pentagons-big-ai-program-maven-already-hunts-data-in-middle-east-africa/>, dostęp: 11.11.2020.

ludzi. System łączy 35 platform wojskowych w 30 lokalizacjach i jest oparty na czterech wojskowych związkach. Wielu amerykańskich dowódców było pozytywnie zaskoczonych łatwością eliminowania różnych zagrożeń przy użyciu ABMS. Wprawdzie na początku testu, który odbył się we wrześniu 2020 r., niektórzy z nich byli sceptyczni i zaniepokojeni wykorzystaniem sztucznej inteligencji[47], jednak po wykazaniu możliwości ABMS, wskazali na potrzebę rozwoju tego rodzaju systemu. Dodali oni, że system ten jest niezbędny do konkurowania w międzynarodowym środowisku bezpieczeństwa, jak również do odstrasza przeciwników, którzy także korzystają z tak zaawansowanej technologii. Dodatkowo warto nadmienić, iż były to największe w historii amerykańskie ćwiczenia wojskowe z wykorzystaniem sztucznej inteligencji[48].

Chiny

Chiny są uważane za jeden z krajów, które są najintensywniej zaangażowane w globalny wyścig na rzecz rozwoju SI. Chociaż niektórzy postrzegają Chiny jako światowego lidera, zdecydowanie częściej są one stawiane w tyle za USA w tej rywalizacji[49]. Niemniej jednak mówi się, że Pekin poczynił, i czyni nadal, szybsze postępy w zakresie rozwoju SI niż jakiekolwiek inne państwo. Władze w Pekinie ogłosiły swoje ambicje, aby do 2030 roku Chiny stały się światowym liderem rozwoju SI[50], ponieważ zdały sobie sprawę – wraz z innymi krajami – że sztuczna inteligencja jest kluczem do posiadania mocarstwowej pozycji w przyszłości i ktokolwiek opanowałby jej rozwój, jak powiedział

[47] Daily Military Defense, *Hypervelocity weapons systems are tested in support of the Advanced Battle Management System*. [online] https://www.youtube.com/watch?v=XgwZmkT8VX0&feature=emb_logo, dostęp: 16.09.2020.
[48] Pope, C., 2020. *Advanced Battle Management System field test brings Joint Force together across all domains during second onramp.* [online] https://www.af.mil/News/Article-Display/Article/2336618/advanced-battle-management-system-field-test-brings-joint-force-together-across, dostęp: 16.10.2020.
[49] Center for Data Innovation, 2019. *Who Is Winning The AI Race: China, The EU Or The United States?*. [online] Who Is Winning the AI Race: China, the EU or the United States?. https://s3.amazonaws.com/www2.datainnovation.org/2019-china-eu-us-ai.pdf, dostęp 2.10.2020.
[50] Webster, G., Creemers, R., Triolo, P. and Kania, E., 2017. All Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017). [online] https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/, dostęp: 1.10.2020.

prezydent Rosji Władimir Putin, „będzie władcą świata"[51]. Chińscy przywódcy wyższego szczebla doskonale zdają sobie sprawę, że technologia sztucznej inteligencji jest niezbędna dla rozwoju militarnego, jak również dla skutecznego konkurowania z największymi potęgami gospodarczymi na świecie.

Chiny poczyniły ogromne inwestycje w sztuczną inteligencję, wydając duże kwoty na przykład na edukację w zakresie SI. W 2018 roku chińskie Ministerstwo Edukacji uruchomiło szereg inicjatyw, które mają na celu m.in. rozwój 50 światowej klasy ośrodków badawczych w dziedzinie sztucznej inteligencji oraz przeszkolenie ponad 500 instruktorów i 5000 studentów w ciągu najbliższych kilku lat[52].

Chiny rozwijają SI zarówno w sposób korzystny dla swoich obywateli (i ludzkości w szerszym ujęciu), jak i niepokojący z jednego z wielu powodów. Pekin poczynił szybkie postępy w sektorze opieki zdrowotnej, m.in. poprzez rozwój klinik medycznych prowadzonych przez sztuczną inteligencję, zdolnych do „zapewnienia konsultacji online w odniesieniu do ponad 2000 powszechnych chorób oraz do natychmiastowej odpowiedzi na dziesiątki tysięcy zapytań medycznych i zdrowotnych, z zachowaniem międzynarodowego standardowego poziomu dokładności",[53] oraz rozwijanie głębokiego uczenia w celu przyspieszenia przetwarzania obrazów medycznych, co z kolei powinno pomóc w znacznie szybszym diagnozowaniu nowotworów i innych poważnych schorzeń. Ponadto należy podkreślić, że w ciągu ostatnich kilku miesięcy wielu chińskich badaczy i naukowców zajmujących się sztuczną inteligencją zaangażowanych było w walkę z pandemią Covid-19.

---

[51] The Verge, 2017. Putin Says The Nation That Leads In AI 'Will Be The Ruler Of The World'. [online] https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world, dostęp: 5.10.2020.
[52] Center for Data Innovation, 2019. *Who Is Winning The AI Race: China, The EU Or The United States?*. [online] Who Is Winning the AI Race: China, the EU or the United States?, s.19. Dostępne pod linkiem: https://s3.amazonaws.com/www2.datainnovation.org/2019-china-eu-us-ai.pdf, dostęp: 2.10.2020.
[53] Koh, D., 2019. *Ping An Good Doctor Launches Commercial Operation Of One-Minute Clinics In China*. [online] https://www.mobihealthnews.com/news/asia-pacific/ping-good-doctor-launches-commercial-operation-one-minute-clinics-china, dostęp: 8.10.2020.

Niemniej jednak nie każdy aspekt rozwoju chińskiej SI jest korzystny i pożyteczny dla przeciętnego obywatela i szlachetny w swojej naturze, gdyż rząd Chin wykorzystuje sztuczną inteligencję również w sposób, który wyraźnie narusza wolności obywatelskie i prywatność ludzi. Według raportów opublikowanych w 2019 roku sztuczna inteligencja umożliwiła władzom chińskim poddanie mniejszości muzułmańskich mieszkających w Chinach, zwłaszcza Ujgurów, masowej inwigilacji na niespotykaną dotąd skalę[54]. Chińskie władze i służby porządkowe mają często stosować algorytmy sztucznej inteligencji w celu zestawiania danych osobowych, w tym danych uzyskanych za pomocą systemu rozpoznawania twarzy, a tym samym identyfikacji obywateli przeznaczonych do zatrzymania. W rzeczywistości rząd chiński wykorzystał już systemy monitorowania, aby umieścić ponad milion swoich obywateli w obozach reedukacyjnych za przestępstwo wyrażania swojej muzułmańskiej tożsamości[55].

Rosja

W 2019 roku Rosja przyjęła strategię rozwoju sztucznej inteligencji do roku 2030 – *National Strategy for the Development of Artificial Intelligence*[56]*.* Dokument ten ma na celu m.in. zwiększenie wydatków na badania i rozwój technologii SI, a także stworzenie systemu regulacji stosunków społecznych, które powstaną w związku z wykorzystaniem sztucznej inteligencji. Ponadto w 2020 roku uruchomiono federalny projekt rozwoju SI w ramach Programu Gospodarki Cyfrowej Federacji Rosyjskiej.[57]

---

[54] Shu, C., 2019. *Leaked Chinese Government Documents Detail How Tech Is Used To Escalate The Persecution Of Uighurs.* [online] https://techcrunch.com/2019/11/24/leaked-chinese-government-documents-detail-how-tech-is-used-to-escalate-the-persecution-of-uighurs/>, dostęp: 7.11.2020.

[55] Bird, E., Fox-Skelly, J., Jenner, N., Larbey, R., Weitkamp, E. and Winfield, A. *The Ethics Of Artificial Intelligence: Issues And Initiatives*. Brussels 2020. s. 14.

[56] Sukhankin, S., 2019. *Russia Adopts National Strategy for Development of Artificial Intelligence*. Eurasia Daily Monitor 16(163). [online] https://jamestown.org/program/russia-adopts-national-strategy-for-development-of-artificial-intelligence/, dostęp: 18.10.2020.

[57] Министерство цифрового развития связи и массовых коммуникаций Российской Федерации, 2020. *Цифровая экономика РФ*. [online] https://digital.gov.ru/ru/activity/directions/858, dostęp; 25.11.2020.

Wraz z intensywnymi pracami nad rozwojem wojskowej SI, które zostaną pokrótce opisane poniżej, Moskwa rozwija tę technologię także dla celów cywilnych. Dla przykładu, jedna z firm, która nadzoruje rosyjski transport kolejowy, testuje autonomiczne pociągi[58]. Ponadto podjęła ona próbę wykorzystania sztucznej inteligencji do przewidywania popytu na transport i zapotrzebowania na bilety, chociaż system ten wymaga dalszego rozwoju, ponieważ wykazał on jak dotąd wiele nieprawidłowości. Co więcej, sztuczna inteligencja znalazła swoje zastosowanie również w sektorze edukacji. Istnieją plany, aby wykorzystać ją w przyszłości do analizy ocen studentów i ich postępów w nauce, a także do kontroli aktywności studentów podczas zajęć, ich śladu cyfrowego i uczestnictwa w życiu uniwersyteckim.

Podobnie jak inne państwa, Moskwa od pewnego czasu dąży do rozwoju sztucznej inteligencji także dla celów wojskowych. Jak stwierdził Władimir Putin, sztuczna inteligencja będzie miała większą wartość dla bezpieczeństwa niż głowice jądrowe[59]. Z kolei rosyjskie Ministerstwo Obrony wielokrotnie dało do zrozumienia, że wojsko rosyjskie posiada już szeroką gamę uzbrojenia opartego na technologii SI, np. drony (które prawdopodobnie zostały użyte podczas agresji na Ukrainę) czy roboty podwodne[60]. W 2018 roku Putin ujawnił, że Rosja zbudowała bezzałogową łódź podwodną, zdolną do przenoszenia broni jądrowej[61]. Szacuje się, że zostaną one wprowadzone do służby do 2027 roku.

---

[58] Коновалова, Н. 2019. *Беспилотная «Ласточка». На железнодорожном салоне в Щербинке показали уникальную технологию.* [online] https://spbvedomosti.ru/news/financy/bespilotnaya-lastochka-na-zheleznodorozhnom-salone-v-shcherbinke-pokazali-unikalnuyu-tekhnologiyu/, dostęp: 20.10.2020.

[59] IZ., 2019, *Путин сравнил преимущества искусственного интеллекта и ядерного оружия.* [online] https://iz.ru/928464/2019-10-03/putin-sravnil-preimushchestva-iskusstvennogo-intellekta-i-iadernogo-oruzhiia, dostęp: 12.11.2020.

[60] Савчук, Т., 2020. *Пентагон занепокоєний використанням Росією штучного інтелекту у військовій сфері. Ось чому* [online] https://www.radiosvoboda.org/a/pentagon-zanepokoyenyy-vykorystannyam-rosiyeyu-shtuxhnogo-intelektu-u-viyskoviy-sferi/30841807.html, dostęp: 12.11.2020.

[61] RBC. *Путин назвал срок спуска на воду подлодки с ядерным «Посейдоном»*. [online] https://www.rbc.ru/politics/20/02/2019/5c6d2c779a7947c9343f1028, dostęp: 13.11.2020.

Co jednak ciekawe, pomimo wszystkich projektów związanych z rozwojem SI realizowanych w Rosji, wydatki Kremla w tym zakresie nie dorównują inwestycjom innych mocarstw konkurujących z Rosją w wyścigu o dominację w rozwoju sztucznej inteligencji, potencjalnie pozostawiając ją, póki co, za USA i Chinami.

ZAGROŻENIA HYBRYDOWE I WOJNA HYBRYDOWA

Zagrożenia hybrydowe uważane są za jedno z najniebezpieczniejszych wyzwań XXI wieku, a pod względem skutków często porównywane są do regularnych konfliktów zbrojnych i klęsk żywiołowych. Stanowią poważne zagrożenie dla stabilności globalnej ze względu na ich potencjalną siłę destrukcyjną, niekonwencjonalność, oraz dużą zdolność ich koordynacji (z możliwością prowadzenia misji w kilku krajach jednocześnie). Zagrożenia hybrydowe są pierwszą fazą „ataków hybrydowych", które są rozumiane jako połączenie regularnych i nieregularnych działań wojennych o różnym nasileniu i mogą być podejmowane przez regularne siły zbrojne, a także organizacje przestępcze, terrorystów, a nawet ruchy polityczne.

Chociaż jednakowa definicja zagrożeń hybrydowych nie została jeszcze zaakceptowana przez wszystkie państwa, jednym z najpowszechniejszych rozumień dotyczących ich natury jest to, że podmioty realizujące elementy działań hybrydowych stosują wspomniane wyżej połączenie zarówno aspektów konwencjonalnej taktyki woj-

skowej, jak i niekonwencjonalnych (tzw. soft) metod, a w tym wojnę informacyjną, propagandę lub wykorzystywanie środków masowego przekazu do manipulowania świadomością publiczną dla swoich celów. Nietypowe zagrożenia, określane jako niekonwencjonalne, hybrydowe lub asymetryczne, to wszystkie działania realizowane przez podmioty, które biorą udział w konfliktach na szeroką skalę, wykorzystując różne taktyki walki na swoją korzyść. Dlatego wymagają one szczególnej uwagi analityków, ekspertów i badaczy w dziedzinie bezpieczeństwa międzynarodowego. Ponieważ zagrożenia te w generalnej deskrypcji są nieuchwytne, niezbędne jest ponowne zdefiniowanie pojęcia wojny i dostosowanie polityki bezpieczeństwa organizacji międzynarodowych, aby móc skutecznie je zwalczać.

Zjawisko zagrożeń hybrydowych często charakteryzuje się stosowaniem niekonwencjonalnych metod lub wykorzystaniem nowych rozwiązań technologicznych, które rewolucjonizują dotychczasowe możliwości bojowe poszczególnych podmiotów[62]. Ponadto **z**agrożenia hybrydowe często zawierają koncepcję wojny hybrydowej, rozumianej jako współistnienie klasycznych i nowych metod prowadzenia wojny[63]. Oznacza to między innymi stosowanie taktyk, takich jak wojna informacyjna, cyberataki i działania terrorystyczne, w celu wywarcia wpływu na społeczeństwa na różne sposoby[64]. Trzeba zaznaczyć, że zagrożenia o charakterze terrorystycznym wpisują się również w definicję obejmującą zagrożenia hybrydowe, podczas gdy wcześniej były one postrzegane jedynie jako część zagrożeń militarnych.

[62] T. Dziubek, *Obronność państwa a zagrożenia asymetryczne*¸ [w:] *Nowe zagrożenia bezpieczeństwa. Wyzwania XXI wieku*, (red.) K. Hennig, Wyższa Szkoła Humanistyczno-Ekonomiczna, Kraków 2015, s. 17.
[63] A. Gruszczak*, Hybrydowość współczesnych wojen – analiza krytyczna*, [w:] *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, (red.) W. Sokała, B. Zapała, Biuro Bezpieczeństwa Narodowego, Warszawa 2011, s. 11.
[64] T. Kubaczyk, *Wojna hybrydowa – (czy) nowy typ konfliktu zbrojnego we współczesnym świecie*, [w:] *Konflikt hybrydowy na Ukrainie. Aspekty teoretyczne i praktyczne*, (red.) B. Pacek, J. A. Grochocka, Piotrków Trybunalski 2017, s. 24.

Unia Europejska zdefiniowała zagrożenia hybrydowe jako połączenie działań wywierających nacisk oraz wywrotowych poprzez metody konwencjonalne i niekonwencjonalne (tj. dyplomatyczne, wojskowe, ekonomiczne, technologiczne), które mogą być wykorzystywane w sposób skoordynowany przez podmioty państwowe lub niepaństwowe do osiągnięcia określonych celów przy jednoczesnym braku formalnej deklaracji wypowiedzenia wojny[65].

Rys. Zagrożenia Hybrydowe

Źródło: opracowanie własne na podstawie: S. Purton, *"What's in a name?... That which we call a rose by any other name would smell as sweet." Or, why half of winning an Irregular War is agreeing what it is...,* The International symposium on Military Operational Research, 26th Symposium, 2009, s. 9.

[65] J. Maas, *Hybrid Threat and CSDP*, ss. 125-130, [w:] J. Rehrl (Ed.), Handbook on CSDP - The Common Security and Defence Policy of the European Union, Austria 2019.

Inną bardzo ważną kwestią jest zrozumienie strategii aktorów, którzy starają się wykorzystać te zagrożenia, aby osiągnąć swoje cele. Zagrożenie hybrydowe występuje wtedy, gdy państwo lub podmiot niepaństwowy ma zdolność i pozorną chęć zastosowania strategii hybrydowej (kompleksowy schemat osiągania celów geopolitycznych i strategicznych). Zagrożenie hybrydowe przejawia się w działaniach, które nie są zgodne z bezpośrednimi konwencjonalnymi działaniami wojskowymi i mogą być prowadzone przez długi czas o różnym nasileniu[66]. Metody hybrydowe można również dostrzec w możliwościach organizacyjnych organizacji terrorystycznych. Dzięki innowacyjnej strategii współcześni ekstremiści nie są uzależnieni od wsparcia państw[67].

Organizacja Traktatu Północnoatlantyckiego postrzega wojnę hybrydową jako gwałtowny konflikt, który charakteryzuje się równoczesnym stosowaniem taktyk konwencjonalnych i nieregularnych, które mogą obejmować zarówno podmioty państwowe, jak i niepaństwowe i są wykorzystywane płynnie, z pominięciem ograniczeń fizycznego pola bitwy lub terytorium. Każdy atak hybrydowy jest wymierzony jednocześnie w państwo i społeczeństwo. Co ważne, narzędzia wymagane do prowadzenia wojny hybrydowej nie pozwalają na rozróżnienia między podmiotami państwowymi i niepaństwowymi, przy czym podmioty niepaństwowe (takie jak grupy ekstremistyczne) są w stanie prowadzić ten rodzaj wojny w równym stopniu co podmiot państwowy i jego wojsko[68].

W ostatnim czasie termin „wojna hybrydowa"[69] był częściej używany w trakcie politycznych i naukowych forów dyskusyjnych, dotyczących polityki bezpieczeństwa, z

---

[66] NATO Energy Security Centre of Excellence, *Hybrid Threats: Overcoming Ambiguity, Building Resilience,* No 11 2017, s. 6.
[67] A. Dengg, M. N. Schurian, *On the Concept of Hybrid Threats*, s. 26, [w:] Networked Insecurity – Hybrid Threatsin the 21st Century, Vienna 2016.
[68] S. Bachmann, *Hybrid Threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats: mapping the new frontier of global risk and security management*, Amicus Curiae 2011 (88), ss. 24-25.
[69] Freier, N. P., *Known Unknowns: Unconventional "Strategic Shocks",* Defense Strategy Development, Carlisle Barracks, PA: U.S. Army War College Strategic Studies Institute, 2008.

przekonaniem, że jest to nowa forma zagrożenia. Media i opinia publiczna również przyjęły ten termin. Tak więc „wojna hybrydowa" wydaje się być najnowszym terminem symbolizującym tę zmianę w prowadzeniu wojny, którą wywołały zagrożenia hybrydowe[70].

Alternatywną definicję proponują badacze specjalizujący się w cyberbezpieczeństwie, a także systemach rozpowszechniania i przechowywania informacji. W ich opinii zagrożenia hybrydowe opisuje się jako element nieregularnych działań wojennych i cyberwojennych, charakteryzujących się celową próbą zaciemnienia przepływu dokładnych informacji do opinii publicznej lub ustanowienia grupy rządzącej w ramach podmiotu sektora publicznego lub prywatnego. Ataki hybrydowe mogą być przeprowadzane zarówno przez podmioty państwowe, jak i niepaństwowe, a ich celem jest wykorzystanie słabych punktów w celu wywołania niezgody społecznej, ekonomicznej lub organizacyjnej w konkretnej grupie docelowe[71]. Zagrożenia hybrydowe obejmują zakres pomiędzy konfliktami międzynarodowymi (lub zewnętrznymi) i wewnątrzpaństwowymi (lub wewnętrznymi)[72].

Cyberwojna jest częścią wojny hybrydowej i służy jako wiodący przykład wykorzystania nowych technologii jako części taktyki wykorzystywanej w ramach zagrożeń

Freier zwraca uwagę na wszystkie wysiłki kampanii hybrydowych zmierzających do powstrzymania wpływów USA bez bezpośredniego konfrontowania się z USA w konwencjonalny sposób militarny. Rosjanie są bardzo prawdopodobnie zainteresowani cofnięciem amerykańskich / zachodnich wpływów w Eurazji, a skutki te mogą świadczyć o rosyjskiej strategii hybrydowej Istnieją bardzo realne, krótkoterminowe cele strategiczne, które można osiągnąć bezpieczniej i skuteczniej za pomocą środków hybrydowych niż w przypadku inwazji wojskowej na pełną skalę.

[70] Armed Forces Journal, 2009. *The War of New Words: Why Military History Trumps Buzzwords*, Armed Forces Journal, [online] <http://www.armedforcesjournal.com/essay-the-war-of-new-words>, dostęp: 24.10.2020.

[71] M. Kaâniche, (ed.), *Applying Resilience to Hybrid Threats,* IEEE Security and Privacy Magazine 17(5), September 2019, s. 78.

[72] D. Raugh, *Is the Hybrid Threat a True Threat?,* Journal of Strategic Security 9(2), June 2016, ss. 1-13.

hybrydowych. Zasadniczo cyberwojna odnosi się do nieustannych wysiłków polegających na wykorzystywaniu systemów sieci komputerowych, które przeprowadzają cyberataki w imieniu podmiotu państwowego lub niepaństwowego na infrastrukturę celu[73].

Jednym z przykładów prowadzenia wojny hybrydowej jest wykorzystanie Internetu w celu szerzenia dezinformacji. Należy podkreślić, że bardzo powszechne jest stosowanie takich taktyk przez organizacje terrorystyczne jak Państwo Islamskie i Al-Kaida. Jest to przykład wskazujący na wykorzystanie narzędzi pierwotnie postrzeganych jako pokojowe (np. media społecznościowe), do prowadzenia lub wspierania taktyk wojny hybrydowej[74]. Należy wziąć pod uwagę, że Państwo Islamskie jest również postrzegane jako „aktor hybrydowy", który jest w stanie sukcesywnie realizować swoje operacje, chociażby poprzez znaczną ekspansję terytorialną w Syrii i Iraku[75]. Ponadto aktywna obecność ISIS w mediach społecznościowych w celach propagandowych również stanowi ważny element działalności hybrydowej[76].

W odniesieniu do organizacji terrorystycznych określenie „zagrożenia hybrydowe" staje się zatem znakiem rozpoznawczym grup ekstremistycznych, które prowadzą nieregularną działalność, ale posiadają pewne znaczące zdolności uważane za zaawansowane i które wcześniej wydawały się znakiem charakterystycznym dla regularnych strategii państw[77]. Co ważne, większość podmiotów niepaństwowych (organizacji terrorystycznych) nie ma narzędzi do prowadzenia regularnych działań wojennych, ale

---

[73] S. Bachmann, *Hybrid wars: the 21st-century's new threats to global peace and security*, Scientia Militaria, South African Journal of Military Studies, Vol 43, No. 1, 2015, s. 82.
[74] A. J. Piazza, A. Guler, *The Online Caliphate: Internet Usage and ISIS Support in the Arab World*, Terrorism and Political Violence, May 2019.
R. Cohen-Almagor, *Jihad Online: How Do Terrorists Use the Internet?,* Advances in Intelligent Systems and Computing, Hull 2017.
B. Salama, *The Resilience of the Islamic State,* Institut für Friedenssicherung und Konflikt management, Vienna 2016.
[75] E. Tenenbaum, *La manœuvre hybride dans l'art opératif, Stratégique*, No 111, Paris 2016, s. 56.
[76] S. Taillat, *Un mode de guerre hybride dissymétrique ? Le cyberespace*, Stratégique, No 111, Paris 2016, ss. 89, 95.
[77] E. Hoorickx, *Countering "Hybrid Threats": Belgium and the Euro-Atlantic Strategy,* Security & Strategy No 131 October 2017, ss. 6-7.

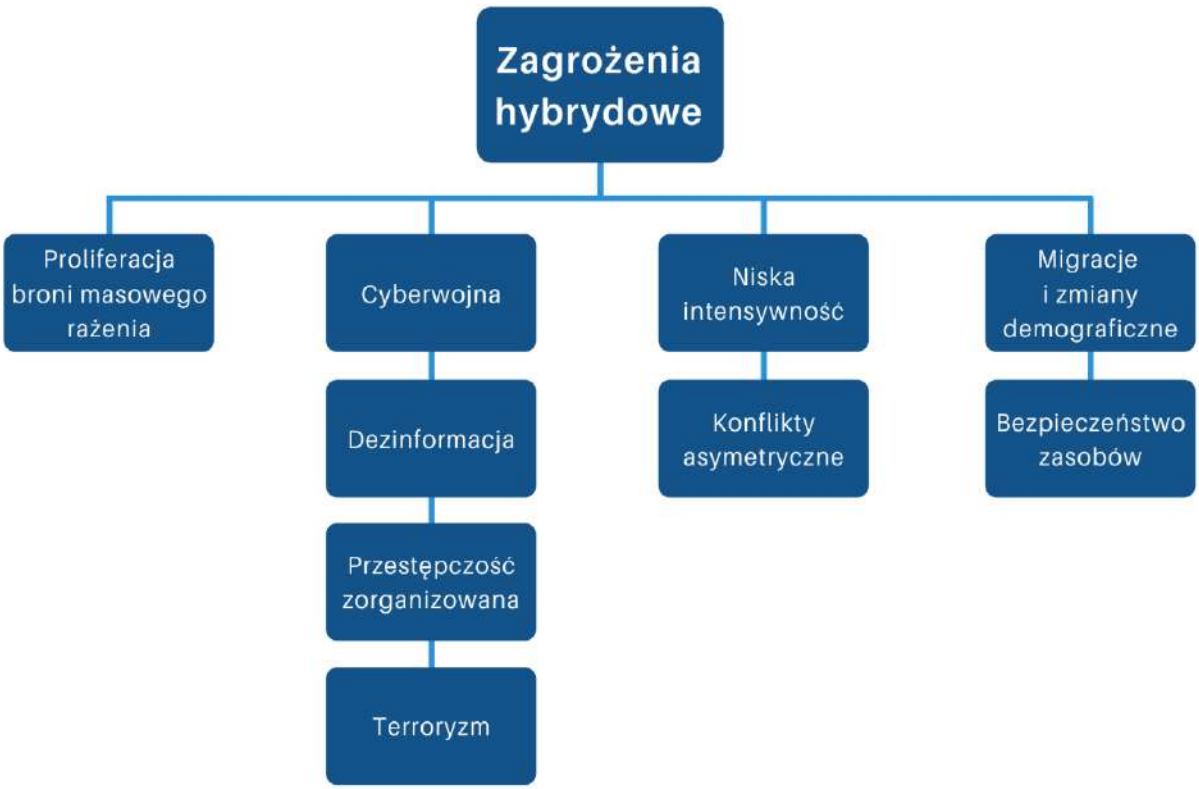
jednocześnie mogą być sponsorowani i uczestniczyć w pośredniej strategii niektórych państw[78].

Charakterystycznymi elementami działalności hybrydowej prowadzonej przez organizacje terrorystyczne są[79]:

- Taktyka mieszana. Zagrożenia hybrydowe łączą konwencjonalne zdolności wojskowe z taktyką partyzancką małych jednostek, które wykorzystują mobilne systemy walki na odległość.
- Ruchome struktury. W ramach działań hybrydowych tworzone są oddziały skupione terrorystów (żołnierzy) oraz rozproszone, zapewniając stałą realizację działań.
- Terroryzm. Zagrożenia hybrydowe wykorzystują działalność terrorystyczną do rozprzestrzeniania nienawiści i wzbudzania strachu. Celem terrorystów jest wpływ na osoby, które sprzeciwiają się ich ideologiom.
- Nieprzestrzeganie prawa międzynarodowego. Zagrożenia hybrydowe nie są objęte przepisami prawa międzynarodowego, stanowiąc ograniczenie, które można wykorzystać.
- Wojna informacyjna. Zagrożenia hybrydowe wykorzystują globalny dostęp do informacji oraz narzędzi umożliwiających udostępnianie treści propagandowych, a także w celu gromadzenia funduszy, rekrutacji i szkoleń.
- Przestępczość zorganizowana. Zagrożenia hybrydowe wykorzystują elementy przestępczości (m.in. handel bronią, narkotykami, porwania) w celu pozyskiwania funduszy do walki i dalszego rozwoju.

[78] G. Lasconjarias, J. A. Larsen (red.), *NATO's Response to Hybrid Threats,* Rome 2015, s. 101.
[79] S. Jasper, S. Moreland, *ISIS: An Adaptive Hybrid Threat in Transition*, Small Wars Jorunal, October 2016, s. 2.

Wyk. Multiwektorowa natura zagrożeń hybrydowych



Źródło: opracowanie własne na podstawie: A. A. Otaiku, *A Framework for Hybrid Warfare: Threats, Challenges and Solutions*, Journal of Defense Management, Volume 8, Issue 3, 2018, s. 4.

Współczesne zagrożenia hybrydowe różnią się od tych, które można było dostrzec w przeszłości, gdyż są znacznie bardziej zabójcze ze względu na szereg ewoluujących technologii. Całkiem nowe perspektywy zostały uwolnione przez systemy autonomiczne i sztuczną inteligencję, na przykład bezzałogowe statki powietrzne (UAV), które są coraz częściej postrzegane jako tanie, ale wyrafinowane systemy do rozpoznania, zakłócenia infrastruktury krytycznej lub przeprowadzenia ataku bombowego.

Ponadto Internet i sieci internetowe pozwalają podmiotom państwowym i niepaństwowym prowadzić nowe operacje. Sieć internetowa może być wykorzystywana do hakowania infrastruktury krytycznej, wpływania na procesy wyborcze, przeprowadzania kampanii dezinformacyjnych i propagandowych, kradzieży informacji i udostępniania wrażliwych danych w przestrzeni publicznej. W najgorszych przypadkach cyberprzestępca przejmuje kontrolę nad zasobami, takimi jak systemy wojskowe i struktury dowodzenia[80].

[80] D. Fiott, R. Parkes, *Protecting Europe. The EU's response to hybrid threats*, European Union Institute for Security Studies, Paris 2019, s. 5.

DEFINIOWANIE TERRORYZMU

Z natury destrukcyjny charakter terroryzmu wywierał bezpośredni wpływ na podmioty państwowe i niepaństwowe w całej historii ludzkości. Forma tych ataków, przeprowadzanych przez różne grupy lub osoby, była podstawą do określenia szczególnych cech terroryzmu przez społeczność międzynarodową. Te postrzegane cechy, które pojawiły się pierwotnie w XX wieku i które zostaną omówione poniżej, doprowadziły do zrozumienia, że w takich atakach na ogół występuje aktor niepaństwowy przeprowadzający brutalny atak na aktora państwowego. Współczesne definicje obejmują takie formy walki, które są wykorzystywane do osiągnięcia określonej grupy celów; ataki terrorystyczne charakteryzują się agresją i zamiarem destabilizacji, oraz szerzenia strachu, zamieszania i niepokoju w społeczeństwie.

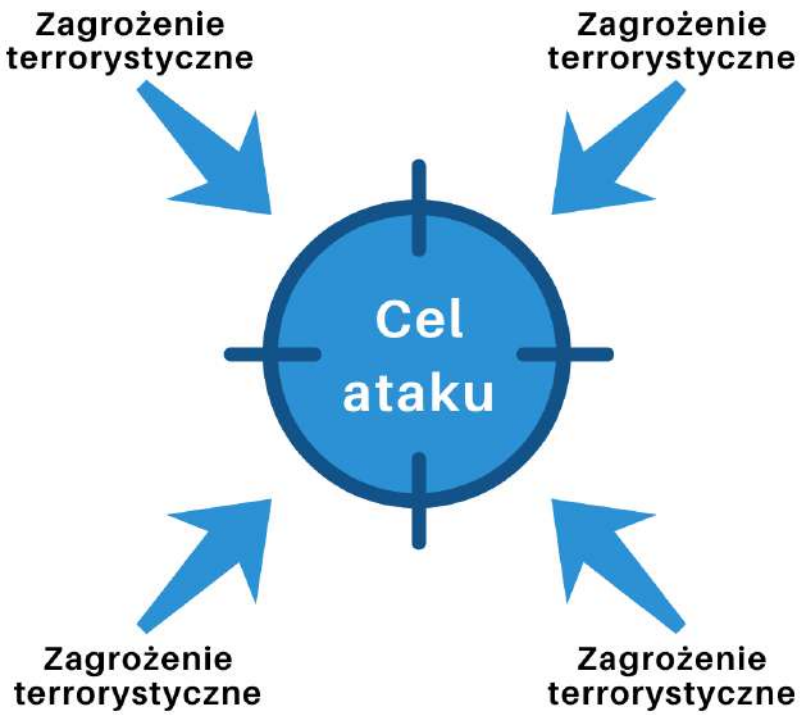
Analiza terroryzmu i podejmowanych w jego ramach działań wiąże się z charakterystyką należących do niego zwrotów i pojęć. Jego interpretowanie, w związku z licznymi modyfikacjami i poszerzeniami, jest konieczne do określenia podmiotów, które będą odpowiedzialne za walkę z nim. Podstawową kwestią dla dalszego wywodu jest

odróżnienie terroru od terroryzmu[81]. Terror jest definiowany jako dominacja podmiotu silniejszego nad słabszym, objawiająca się jako dyktatura, totalitaryzm, tyrania, reżim, despotyzm. Natomiast terroryzm pierwotne określano jako agresję i przemoc słabszych przeciwko silniejszym w celu obalenia ich władzy, wywołania określonych działań, zwrócenia uwagi na problem lub demonstracji sił. Często jest on kojarzony z atakami na tle religijnym, których w ostatnich dekadach dokonywali głównie wyznawcy islamu[82]. Należy jednak wskazać, że działania terrorystyczne są również podejmowane przeciwko muzułmanom[83].

Aby dokładnie zrozumieć, czym jest zagrożenie terrorystyczne, należy najpierw ustalić ramy tego, co można zdefiniować jako zagrożenie. Definicja zagrożenia może mieć charakter niemilitarny, ale może dotyczyć ataku na czyjeś życie, ograniczać znacząco działalność polityczną rządu lub podmiotów w państwie. Inną równie akceptowalną definicję można dostrzec w przypadku określeń o charakterze militarnym, gdzie występuje wyraźne ryzyko skrzywdzenia kogoś lub sygnalizowanie chęci wyrządzenia szkody. Pomimo różnych poglądów na temat tego, co można uznać za zagrożenie, sam termin kojarzy się z obawami lub ryzykiem związanym z bezpieczeństwem podmiotu, który jest celem.

[81] R. I. Iulian, *International terrorism in the 21st century – 16 years after 9/11 2001*, CBU International conference on innovations in science and education March 22-24, Prague 2017, Czech Republic.
[82] C. Sikorski, D. Schmuck, J. Matthes, A. Binder, *"Muslims are not Terrorists": Islamic State Coverage, Journalistic Differentiation Between Terrorism and Islam, Fear Reactions, and Attitudes Toward Muslims*, , „Mass Communication and Society", 2017, vol. 20, Issue 6: „Media, Terrorism and Society", s. 825–848; R. A. Abdulla, *Islam, Jihad, and Terrorism in Post-9/11 Arabic Discussion Boards*, „Journal of Computer-Mediated Communication", 12(3), article 15, s. 1-16.
[83] M. Kerdemelidis, M. Reid, *Wellbeing recovery after mass shootings: information for the response to the Christchurch mosque attacks 2019*, „Canterbury District Health Board", 28.05.2019, s. 2–5.

Rys. Wielowymiarowe zagrożenia terrorystyczne



Źródło: opracowanie własne

Niemniej jednak podjęto wysiłki, aby wzmocnić to, co można określić jako walkę z zagrożeniami terrorystycznymi. Międzynarodowe definiowanie na potrzeby bezpieczeństwa i obronności pierwotnie ujęto w Konwencji Ligi Narodów z 16 listopada 1937 roku. Konwencja została podpisana przez 25 państw, ale ratyfikowana tylko przez Indie, dlatego też nie weszła w życie[84]. Następnie w 1999 roku Rada Bezpieczeństwa ONZ przyjęła rezolucję 1269, w której wskazała, że wszystkie praktyki, niezależnie od miejsca i czasu, stosowane przeciwko bezpieczeństwu oraz zagrażające międzynarodowemu porządkowi i pokojowi, są działaniami terrorystycznymi[85]. Ponownie w 2018 roku Biuro

[84] R. D., Law, *Terrorism: A History*, Cambridge 2009, ss. 155–157.
[85] Security Council, *Resolution 1269 (1999)*, Adopted by the Security Council at its 4053rd meeting, on 19 October 1999.

Narodów Zjednoczonych ds. Narkotyków i Przestępczości (United Nations Office On Drugs And Crime, UNODC) zdefiniowało terroryzm jako wykorzystywanie metody przymusu lub groźbę wykorzystania przemocy w celu szerzenia strachu i osiągnięcia dążeń politycznych lub ideologicznych[86].

Unia Europejska przedkłada definicję terroryzmu, która ma celu deskrypcję zjawiska stanowiącego zagrożenie dla państw członkowskich. Działania terrorystyczne to przestępstwa, które ze względu na swój charakter mogą wyrządzić poważne szkody państwu lub organizacji międzynarodowej i są określane jako przestępstwa terrorystyczne, jeżeli zostają popełnione w celu: poważnego zastraszenia ludności; bezprawnego zmuszenie rządu lub organizacji międzynarodowej do podjęcia lub zaniechania jakiegoś działania; bądź poważnej destabilizacji lub zniszczenia podstawowych struktur politycznych, konstytucyjnych, gospodarczych lub społecznych danego państwa lub danej organizacji międzynarodowej. Są to następujące czyny umyślne, określone zgodnie z prawem krajowym jako przestępstwa[87]:

a) ataki na życie ludzkie, które mogą powodować śmierć;

b) ataki na integralność fizyczną osoby;

c) porwania lub branie zakładników;

d) spowodowanie rozległych zniszczeń obiektów rządowych lub obiektów użyteczności publicznej, systemu transportowego, infrastruktury, w tym systemu informacyjnego, stałych platform umieszczonych na szelfie kontynentalnym, miejsca publicznego lub mienia prywatnego – jeżeli zniszczenia te mogą zagrozić życiu ludzkiemu lub spowodować poważne straty gospodarcze;

---

[86] United Nations Office on Drugs and Crime, *Education for justice university module series counter-terrorism – Module 1 introduction to international terrorism*, UN, Vienna 2018, s. 1.
[87] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW, 31.3.2017.

e) zajęcie statku powietrznego, statku wodnego lub innego środka transportu publicznego lub towarowego;

f) wytwarzanie, posiadanie, nabywanie, przewożenie, dostarczanie lub używanie materiałów wybuchowych lub broni, w tym broni chemicznej, biologicznej, radiologicznej lub jądrowej, jak również badania nad taką bronią i rozwój broni chemicznej, biologicznej, radiologicznej lub jądrowej;

g) uwalnianie substancji niebezpiecznych lub powodowanie pożarów, powodzi lub wybuchów, czego rezultatem jest zagrożenie życia ludzkiego;

h) zakłócanie lub przerywanie dostaw wody, energii elektrycznej lub wszelkich innych podstawowych zasobów naturalnych, czego rezultatem jest zagrożenie życia ludzkiego.

Za ataki są odpowiedzialne osoby, grupy terrorystyczne lub organizacje, których motywy i idee są uzasadniane wiarą, celami politycznymi, ekonomicznymi, społecznymi, narodowościowymi, a nawet ekologicznymi[88]. Terroryzm to zjawisko towarzyszące prawie wszystkim cywilizacjom na przestrzeni wieków, które oddziaływało na bezpieczeństwo w różnym nasileniu. Przybierając różne rozmiary, pod postacią agresji, przemocy lub zastraszenia, wykorzystywano go jako środek do prowadzenia walki o wybrane cele[89].

[88] E. Zabłocki, *Kategorie, zagrożenia: system bezpieczeństwa narodowego,* Wyższa Szkoła Informatyki, Zarządzania i Administracji w Warszawie, Warszawa 2013, s. 51–52.
[89] S. Bukowski, *Terroryzm europejski*, Wydawnictwo Naukowe Akademii Pomorskiej w Słupsku, Słupsk 2010, s. 21.

Map. Poziom zagrożenia terrorystycznego w Europie

Źródło: opracowanie własne

Nie ma jednak powszechnie akceptowalnej definicji terroryzmu, ponieważ istnieje wiele różnych podejść do tego zjawiska. Różnią się one w zależności od perspektywy kulturowej, religijnej, miejsca ataku oraz prawa krajowego. Ogólnie rzecz biorąc, terroryzm jest niepokojącą metodą powtarzających się gwałtownych działań, stosowaną przez (częściowo) tajnych aktorów indywidualnych, grupowych lub państwowych, z powodów idiosynkratycznych, kryminalnych lub politycznych, w których – w przeciwieństwie do zabójstwa – bezpośrednim celem przemocy nie są główni odbiorcy.

Bezpośrednie ludzkie ofiary przemocy są wybierane losowo lub selektywnie (reprezentują daną tożsamość lub symboliczne cele) z docelowej populacji i służą jako generatory wiadomości. Procesy komunikacji – oparte na zagrożeniu i przemocy – między terrorystami (organizacją), ofiarami (zagrożonymi) i celami, są wykorzystywane do manipulowania głównym celem (odbiorcami), przekształcając go w cel terroru, cel żądań lub cel uwagi, w zależności od tego, czy ideą jest zastraszanie, przymus lub propaganda"[90]. Zjawisko to jest definiowane w różny sposób nie tylko w poszczególnych krajach – rozbieżności często pojawiają się w charakterystyce i opisie wewnątrz samego państwa.

Trudność w definiowaniu terroryzmu wynika z braku spójności w jego charakteryzowaniu przez badaczy, polityków i dziennikarzy. Wynika to z faktu, że każdy spektakularny akt przemocy przeciwko społeczeństwu, umotywowany politycznie, jest określany jako „terroryzm". Różne działania, które niegdyś nie miały ze sobą nic wspólnego – jak wysadzenie samochodu, podłożenie bomby w parlamencie, zabójstwo polityka, porwanie dziennikarza, zatrucie jedzenia, zasztyletowanie na dworcu oraz dokonanie masakry w klubie podczas koncertu – są określane jako zamachy terrorystyczne[91]. Dlatego zachodzą różnice w definiowaniu i opisywaniu terroryzmu. Wielu badaczy myli różnego rodzaju działania, często nie odróżniając od siebie rebelii, separatyzmu, wojny lub nawet protestu. Może to być związane z założeniem, że to, co dla jednych jest terroryzmem, dla innych będzie usprawiedliwioną metodą walki narodowowyzwoleńczej, obroną tożsamości, ochroną wartości kulturowych lub wiary (uczuć religijnych)[92]. Należy przywoływać tutaj wystąpienie J. Arafata na forum Zgromadzenia Ogólnego ONZ z 1974 roku, w którym porównał on terrorystę do rewolucjonisty. Według niego wyraźnie zauważalna różnica sprowadza się do tego, jak postrzegamy dane zdarzenie.

[90] A. J., Jongman, A.P., Schmid, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature*, Transaction Publishers, New Brunswick 1988.
[91] R. Borkowski, *Terroryzm ponowoczesny*, Wydawnictwo Adam Marszałek, Toruń 2006, s. 40.
[92] Z. Cesarz, E. Stadmulller, *Problemy polityczne współczesnego świata*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2002, s. 351.

Ktokolwiek broniący słusznej sprawy (wg własnych przekonań), walczący o prawa i ideały, jednocześnie zmagający się z najeźdźcą, nie może być według J. Arafata nazwany terrorystą[93]. Jest to jednak zależne od poszczególnych, indywidualnie rozpatrywanych sytuacji, gdyż podstawowym błędem w definiowaniu terroryzmu jest generalizacja. Kolejne trudności omawianego problemu są spowodowane brakiem statystyk, które wyraźnie mówiłyby, które z popełnionych przestępstw miały charakter terrorystyczny. Jest to związane z przenikaniem zjawiska terroryzmu z działaniami w ramach zagrożeń hybrydowych (wojny hybrydowej), wojny oraz przestępstw. Brakuje też jednej, międzynarodowej definicji, która umożliwia klasyfikację. Często zdarza się, że nieznany jest motyw terrorysty, a jego działanie jest określanie np. jako atak na tle religijnym. Ważne jest również to, że większość teoretyków ma własne definicje terroryzmu, która ulegają ewolucji w zależności od występujących zdarzeń.

[93] United Nations, General Assembly, *Agenda Item 108 – Question of Palestine (Resumed from the 2268th meeting),* Wednesday, 13 November 1974, at 10.30 a.m. New York, A/PV.2282 and Corr.1.

ORGANIZACJE TERRORYSTYCZNE

W tej części ujęto największe organizacje terrorystycznych na świecie. Przedstawiono miejsca, w których pierwotnie funkcjonowały, potencjalne obszary, na których mogą podejmować swoje działania, a także wskazano ich główne źródła finansowania. Oprócz tego opisano pokrótce historię każdej z organizacji oraz podsumowano ich dotychczasowe działania.

AL-NUSRA FRONT/HAY'AT TAHRIR AL-SHAM (TAHRIR AL-SHAM)

Miejsce utworzenia: Syria i Irak (utworzono w 2011 r., ogłoszono w 2012 r.)

Potencjalne terytorium działań: Syria i Liban

Źródła utrzymania: cła, podatki, grzywny na terenie jej działania, składki od mniejszości religijnych, handel bronią z innymi grupami terrorystycznymi i przestępczymi, darowizny zagraniczne, sprzedaż ropy naftowej, przemyt, porwania dla okupu.

Podsumowanie działalności: W 2011 roku Abu Bakr al-Baghdadi, przywódca Państwa Islamskiego w Iraku (ISI, dawniej Al-Kaida w Iraku), wysłał swoich zaufanych zwolenników do Syrii, aby ustanowić przyczółek w tym kraju[94]. W styczniu 2012 roku pod przewodnictwem Abu Mohammada al-Julaniego grupa ogłosiła swoje istnienie jako Jabhat al-Nusra („Front of the Supporters"), aby rozpocząć ofensywę przeciwko reżimowi Baszara al-Assada. W 2013 roku Al-Baghdadi, obawiając się rosnącej niezależności Al-Nusry i różnic w taktyce działań, ogłosił utworzenie Islamskiego Państwa Iraku i Lewantu (ISIL) i zażądał, aby al-Julani poddał się jego przywództwu. Al-Nusra odrzuciła to żądanie i po raz pierwszy zidentyfikowała się jako oddział Al-Kaidy (AQ). Kierownictwo AQ wspierało Al-Nusrę, wysyłając członków swojej organizacji, aby kierowali rozwojem grupy. Jednak w lipcu 2016 roku Al-Nusra ogłosiła, że zmienia nazwę na Jabhat Fateh al-Sham (JFS, „Front for Conquering Syria"), ogłaszając jednocześnie niezależność od wszelkich podmiotów zewnętrznych. Ta zmiana była spowodowana chęcią ukrycia powiązań z Al-Kaidą, aby uzyskać wsparcie finansowe od państw Zatoki Perskiej oraz podjąć współpracę z innymi grupami rebeliantów na rzecz walki przeciwko Rosji i USA. Na początku 2017 roku JFS połączył się z czterema innymi organizacjami, tworząc Hay'at Tahrir al-Sham (HTS). Departament Stanu USA konsekwentnie odrzucał informacje, że zmiany nazwy mogły wpłynąć na bliskie powiązania grupy z AQ. Należy

[94] Center on Sanctions & Illicit Finance, *Al-Qaeda's Branch in Syria: Financial Assessment*, Washington, Foundation for Defense of Democracies, 2017.

podkreślić, że Jabhat al-Nusra (JN) stosuje te same metody, które stosował przywódca Al-Kaidy Ayman al-Zawahiri – mianowicie podżeganie do religijnej i społecznej rewolucji poprzez wykorzystanie rebelii. Wojna w Syrii zapewniła JN niemal idealne środowisko, w którym ta strategia może zostać wdrożona właśnie w imieniu Al-Kaidy. Niepokojącym jest fakt, że JN rośnie w siłę[95].

Map. Główne regiony operacji Al-Nusra Front

[95] J. Cafarella, *Jabat al-Nusra in Syria: An Islamic Emirate for Al-Qaeda*, Middle East Security Report, 25, 2014.

AL-QAEDA / AL-KAIDA

Miejsce utworzenia: Afganistan i Pakistan (1988 r.)

Potencjalne terytorium działań: cały świat

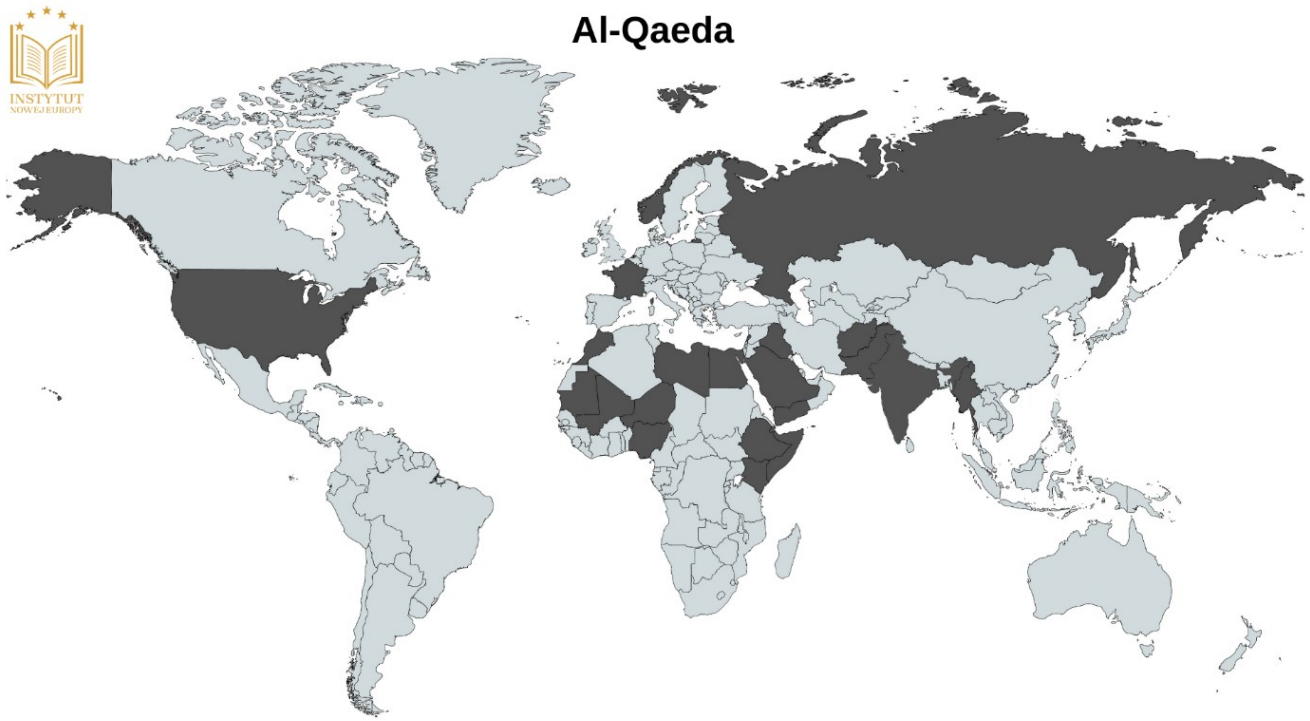
Źródła utrzymania: prywatni darczyńcy, islamskie organizacje i fundacje, sponsoring państwowy, handel narkotykami, napady na banki, porwania dla okupu.

Podsumowanie działalności:

Al-Kaida pierwotnie pomagała w finansowaniu, rekrutacji, transporcie i szkoleniu bojowników afgańskiego ruchu oporu przeciwko byłemu Związkowi Radzieckiemu. Obecnie grupa dąży do wyeliminowania zachodnich wpływów ze świata muzułmańskiego, obalenia „niewiernych" rządów w krajach muzułmańskich oraz ustanowienia islamskiego kalifatu, rządzonego własną interpretacją prawa szariatu, który ostatecznie miałby być fundamentem dla nowego porządku międzynarodowego. Istnieją trzy filary doktryny Al-Kaidy, które były wyrażane przez jej długoletniego przywódcę, Osamę bin Ladena, a są to: zjednoczenie światowej populacji muzułmańskiej w szariacie; wyzwolenie „świętej ziemi" z sojuszu „syjonistystów" i „krzyżowców"; oraz wyrównanie niesprawiedliwości ekonomicznych i społecznych. AQ od lat zobowiązane jest lojalnością wobec talibów, którzy zapewnili jej schronienie po atakach z 11 września, gdy Stany Zjednoczone podczas operacji militarnej dążyły do zniszczenia organizacji. Grupa posiada dowództwa regionalne, które operują głównie w Afryce Północnej i Sahelu (Al-Kaida w Islamskim Maghrebie (AQIM)), Afryce Wschodniej (al-Szabab), Jemenie (Al-Kaida na Półwyspie Arabskim (AQAP)), terytoriach Indii, Bangladeszu, Birmy, Afganistanu i Pakistanu (Al-Kaida na Subkontynencie Indyjskim (AQIS)) oraz w Syrii (Front Al-

Nusra)[96]. Przywódca Al-Kaidy, Ayman al-Zawahiri, prawdopodobnie zmarł z przyczyn naturalnych, jednak jego śmierć nie została jeszcze potwierdzona[97].

Map. Główne obszary operacji AQ



[96] A. Reed, *Al Qaeda in the Indian Subcontinent*, The International Centre for Counter-Terrorism, The Hague 2016, ss. 3-17.
[97] S. Tim, *Is al-Qaeda's leader dead? Report claims terror chief Ayman al-Zawahiri has died in Afghanistan from 'asthma-related breathing issues'*, https://www.dailymail.co.uk/news/article-8970231/Al-Qaedas-leader-Ayman-al-Zawahiri-died-reports-claim.html, dostęp: 10.12.2020.

PAŃSTWO ISLAMSKIE W IRAKU I LEWANCIE (ISIL / ISIS)

Miejsce utworzenia: Irak (Al-Kaida w Iraku: 2004; ISIS: 2013)

Potencjalne terytorium działań: cały świat

Źródła utrzymania: grabieże banków, wymuszenia i handel ludźmi, kontrola złóż ropy i gazu, wyłudzanie zasobów rolnych, sprzedaż dóbr kultury, porwania dla okupu, prywatni darczyńcy, darowizny od organizacji pozarządowych, pozyskiwanie funduszy za pośrednictwem nowoczesnych sieci komunikacyjnych[98].

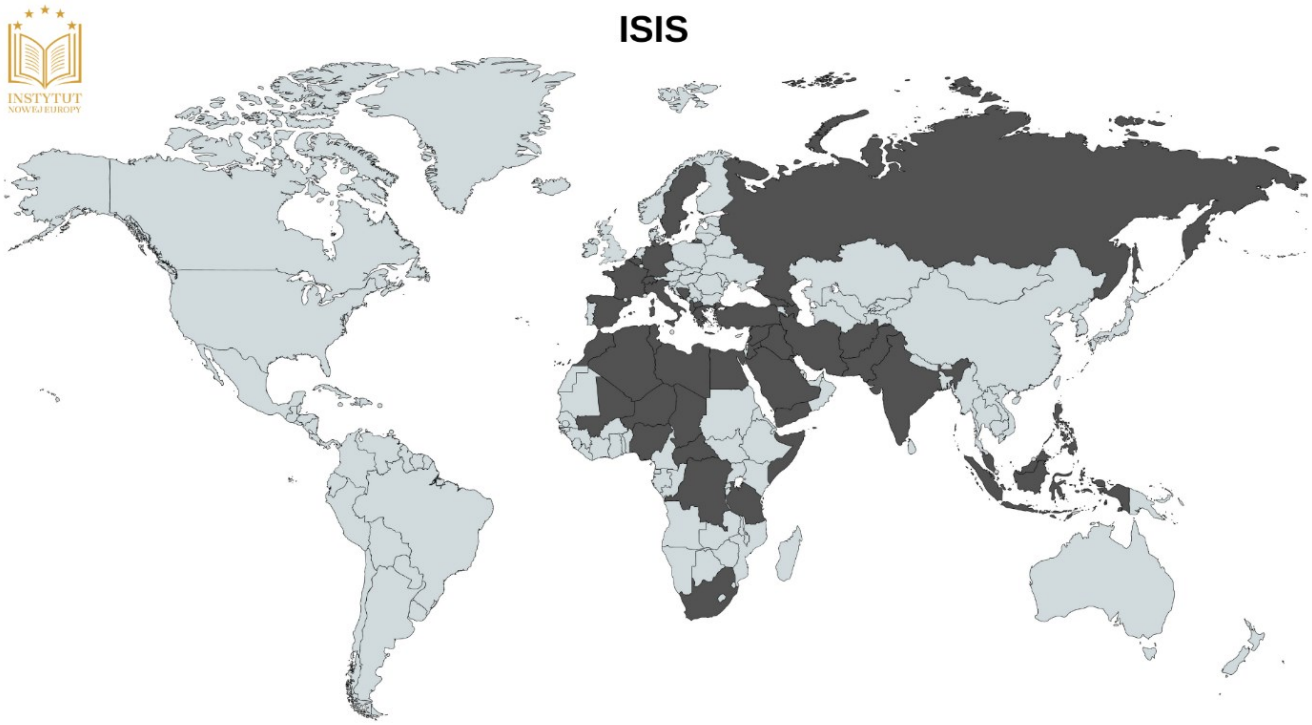
Podsumowanie działalności:

Organizacja Państwa Islamskiego (Islamskie Państwo Iraku i Lewantu, ISIL/ISIS, arabski akronim Daesz) pojawiła się jako jedno z głównych zagrożeń dla bezpieczeństwa międzynarodowego w ostatniej dekadzie[99]. ISIS kontynuuje działania, które wcześniej podejmowała Al-Kaida, ale jednocześnie w sposób bezprecedensowy rozwinęło własne struktury. W jego działaniach terrorystycznych nastąpiła swoista ewolucja z małych, mobilnych, rozproszonych, niedofinansowanych komórek, które przerodziły się w scentralizowaną, dobrze uzbrojoną i sprawującą kontrolę nad dużym terytorium, bogatym w zasoby, organizację. Pozwoliło to na realizację ambitnego planu stworzenia swoistego państwa, korzystając ze strategicznych zasobów finansowych uzyskiwanych na przestrzeni lat w ramach działalność terrorystycznej. Podobnie jak Hezbollah, ISIS posiada strukturę organizacyjną obejmującą administrację, sieci finansowe, międzynarodowy aparat wojskowy, a także organy odpowiadające za komunikację oraz propagandę[100]. ISIS jest organizacją, z inspiracji której przeprowadzanych jest najwięcej ataków terrorystycznych podejmowanych przez tzw. samotne wilki.

---

[98] FATF, 'Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)' (Paris, FATF/OECD, 2015).
[99] Congressional Research Service, 'The Islamic State and U.S. Policy' (Washington, CRS, 2018).
[100] European Parliament, The Financing of the 'Islamic State' in Iraq and Syria (ISIS), European Parliament's Committee on Foreign Affairs, Belgium 2017.

Map. Główne regiony operacji ISIS



BOKO HARAM

Miejsce utworzenia: Nigeria (2002 r.)

Potencjalne terytorium działań: Nigeria, Czad, Kamerun, Niger, Mali, Tunezja, Algieria, Mali, Burkina Faso, Kongo, Mozambik, Somalia, Egipt, Libia

Źródła utrzymania: porwania dla okupu, podatki i wymuszenia, grabież i kradzież pieniędzy z systemu bankowego, darowizny, własne firmy, rolnictwo, przemyt i handel narkotykami, bronią oraz ludźmi

Podsumowanie działalności:

Boko Haram (co w tłumaczeniu oznacza „zachodnia edukacja jest grzechem" lub „zachodnia edukacja jest zabroniona") to organizacja, która złożyła ISIS przysięgę wierności. Grupa ta promuje salaficko-dżihadystyczną odmianę islamu i dąży do ustanowienia kalifatu, czyli państwa islamskiego, w Nigerii i krajach sąsiadujących. Organizacja jest podzielona na frakcje terrorystyczne, posiadając zdecentralizowaną strukturę organizacyjną, w której można wyróżnić takie komórki jak: grupy bojowe, dostawcy broni, eksperci od materiałów wybuchowych, lekarze oraz specjaliści ds. wywiadu i obserwacji. Boko Haram przeprowadziło w swojej historii wiele ataków terrorystycznych na różne grupy religijne i polityczne, policję oraz siły wojskowe, a także zamachy na ludność cywilną. Szczyt ich działalności terrorystycznej przypada na lata 2014 i 2015[101]. Po tym okresie ich zaangażowanie nieco spadło, ale regularnie dochodzi do wielu brutalnych ataków, także na kobiety i dzieci[102]. Boko Haram jest radykalnym islamskim ruchem, który został ukształtowany na północy kraju, gdzie dominuje przestępczość i skrajne ubóstwo. Jej zadeklarowanym celem jest ustanowienie państwa na prawach

[101] Global Conflict Tracker, *Boko Haram in Nigeria,* https://www.cfr.org/global-conflict-tracker/conflict/boko-haram-nigeria, dostęp: 11.12.2020

[102] Agence France-Presse, *At least 110 dead in Nigeria after suspected Boko Haram attack,* https://www.theguardian.com/world/2020/nov/29/nigeria-attack-boko-haram-farm-workers-killed, dostęp: 11.12.2020.

szariatu, ale wykazuje niewielkie zainteresowanie faktycznym zarządzaniem lub rozwojem gospodarczym kraju. Ideologia grupy opiera się na fundamentalistycznym wahabickim systemie teologicznym i sprzeciwia się tradycyjnemu islamowi wyznawanemu w północnej Nigerii, który jest uznawany za raczej tolerancyjny. Boko Haram ma również swój bardziej radykalny odłam, Ansaru (islamski fundamentalistyczny dżihadyzm), który staje się coraz silniejszy, operując na coraz większym terytorium. W odpowiedzi na jej rozrost, nigerski rząd uznał, że Boko Haram, jako organizacja, jest w państwie nielegalna. Jednocześnie, nadużycia ze strony nigeryjskich służb bezpieczeństwa są często powodem dla uzyskiwania przez terrorystów poparcia w społeczeństwie. Trzeba jednak podkreślić, że walka między rządem a Boko Haram ma tragiczne konsekwencje humanitarne; wiele osób zostało przesiedlonych wewnętrznie w północnej Nigerii, a tysiące uchodźców uciekło do sąsiednich krajów.

Map. Główne regiony operacji Boko Haram

HOUTHIS / RUCH HUTI

Miejsce utworzenia: Jemen (1994 r.)

Potencjalne terytorium działań: Jemen, Arabia Saudyjska, Iran, Irak, Libia, Liban i Syria

Źródła utrzymania: finansowanie państwowe (Iran), darowizny zewnętrzne (Hezbollah i inne źródła)

Podsumowanie działalności:

Huti – oficjalnie znani jako Ansar Allah (zwolennicy Boga) – to ruch wojskowy i polityczny wspierany przez Iran. Jego członkowie, należący do mniejszościowej sekty Zaidi, wywodzącej się z szyickiego islamu, opowiadają się za regionalną autonomią Zaidis w północnym Jemenie. Ruch Huti powstał jako próba utrzymania autonomii plemiennej w północnym Jemenie i protestu przeciwko wpływom krajów zachodnich na Bliskim Wschodzie. Obecnie Huti dążą to tego, aby odgrywać większą rolę w rządzie Jemenu, ale nadal bronią interesów mniejszości Zaidi[103]. Ruch ten znany jest z silnej antyamerykańskiej i antysemickiej retoryki. Pozbawiony wielu opcji uzyskania wsparcia od sojuszników w regionie, Iran rutynowo wykorzystuje taktykę wspierania organizacji terrorystycznych, aby rozszerzyć swoje zasięgi na Bliskim Wschodzie i zantagonizować swoich przeciwników, jednocześnie minimalizując ryzyko uwikłania się bezpośrednio w konflikt. Huti byli szkoleni i otrzymywali sprzęt wojskowy od irańskiego Korpusu Strażników Rewolucji Islamskiej (IRGC)[104].

[103] The Wall Street Journal, *5 Things to Know About the Houthis of Yemen*, https://www.wsj.com/articles/BL-263B-3613, dostęp: 14.12.2020
[104] Al. Jazeera, *US hits Iran IRGC with sanctions over support of Yemen's Houthis,* https://www.aljazeera.com/news/2018/05/23/us-hits-iran-irgc-with-sanctions-over-support-of-yemens-houthis, dostęp: 15.12.2020.

Map. Główne regiony operacji Huti

HAMAS

Miejsce utworzenia: Strefa Gazy (1987 r.)

Potencjalne terytorium działań: Strefa Gazy, Zachodni Brzeg, Izrael, Katar, Egipt, Liban, Iran, Turcja, Jordania i Jemen

Źródła utrzymania: organizacje charytatywne, podatki, korupcja, kryptowaluty, inwestycje zagraniczne, finansowanie państwowe (m.in. Iran, Katar, Arabia Saudyjska)

Podsumowanie działalności:

Hamas wywodzi się z Bractwa Muzułmańskiego, które pojawiło się w Strefie Gazy pod koniec lat 80., podczas pierwszej palestyńskiej „intifady" (powstania) przeciwko Izraelowi. Ideologia grupy łączy islamizm z palestyńskim nacjonalizmem, a Hamas dąży do zniszczenia Izraela i utworzenia państwa islamskiego między Morzem Śródziemnym a rzeką Jordan. Hamas pragnie stworzenia państwa islamistycznego opartego na zasadach szariatu (prawa islamskiego). Organizacja terrorystyczna postrzega całą ziemię Mandatu Palestyny – z wyłączeniem 80% Palestyny, która stała się współczesną Jordanią – jako islamskie prawo pierworództwa, które zostało przywłaszczone. Przywództwo Hamasu było historycznie podzielone między jego zagraniczne biuro polityczne i rząd w Gazie, co powoduje, że dwie struktury mają czasami odmienne zdania. Wielokrotnie różni przywódcy Hamasu wysuwali sprzeczne stwierdzenia co do tego, czy skrzydło wojskowe ugrupowania o nazwie Izz ad-Din al-Kassam, powinno działać niezależnie, czy pod kierunkiem skrzydła politycznego. Hamas często współpracuje z innymi grupami w regionie, które angażują się w działania bojowe i terrorystyczne, ale ogranicza swoją aktywność do Izraela i terytoriów palestyńskich – co odróżnia tę organizację np. od Al-Kaidy, która wyraża dużo większe aspiracje międzynarodowe[105].

[105] Congressional Research Service, *Hamas: Background and Issues for Congress*, Washington 2010.

Map. Główne regiony operacji Hamasu

HEZBOLLAH

Miejsce utworzenia: Liban (1985 r.)

Potencjalne terytorium działań: Liban, Syria, Niemcy, Meksyk, Paragwaj, Argentyna, Brazylia, Iran, Zjednoczone Emiraty Arabskie, Irak, Stany Zjednoczone, Jemen, Egipt, Turcja, Rosja i Sudan

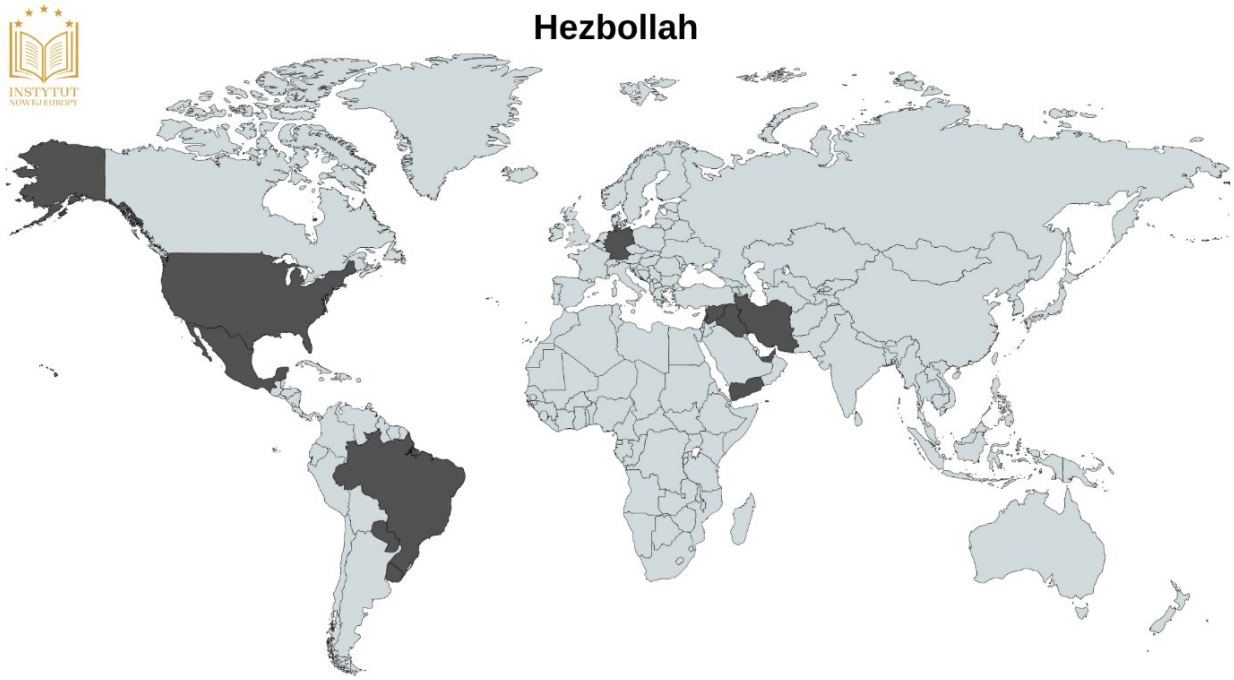
Źródła utrzymania: finansowanie państwowe (Iran), międzynarodowa działalność przestępcza, darowizny indywidualne i od organizacji, korzyści finansowe od międzynarodowych firm znajdujących się pod wpływem organizacji

Podsumowanie działalności:

Fundamenty pod hybrydową organizację terrorystyczną, jaką jest Hezbollah, zostały położone, kiedy została ona ustanowiona jako patronacka struktura dla proirańskich grup islamskich w Libanie, które podzielały wiarę w posłuszeństwo najwyższemu przywódcy Chomeiniemu (wilayat faqih) i chęć ostatecznego ustanowienia Republiki Islamskiej w Libanie, wzorowanej na modelu irańskim[106]. Iran zapewnia finansowanie i broń Hezbollahowi, a także nadzoruje strategię działań. Kolejnym krajem będącym pod wpływem Hezbollahu jest Syria, choć dynamika tych stosunków znacznie się zmieniła w ciągu ostatnich 17 lat. Interwencja wojskowa Hezbollahu w Syrii w 2012 roku w celu udzielenia pomocy reżimowi Assada przeciwko zbrojnej opozycji umożliwiła libańskiej partii zawiązanie partnerstwa z Damaszkiem[107].

[106] E. Azani, *The Hybrid Terrorist Organization: Hezbollah as a Case Study*, in Studies in Conflict & Terrorism, 36:11 (2013) ss. 899-916.
[107] Middle East Institute, *Hezbollah's Evolution: From Lebanese Militia to Regional Player*, Washington 2017/

Map. Główne regiony operacji Hezbollahu



PARTIA PRACUJĄCYCH KURDYSTANU - PKK

Miejsce utworzenia: południowo-wschodnia Turcja (1978 r.)

Potencjalne terytorium działań: Turcja, Irak, Syria, Iran, Czechy, Niemcy, Belgia, Rumunia, Austria, Grecja, Egipt, Turkmenistan, Rosja, Liban i Cypr

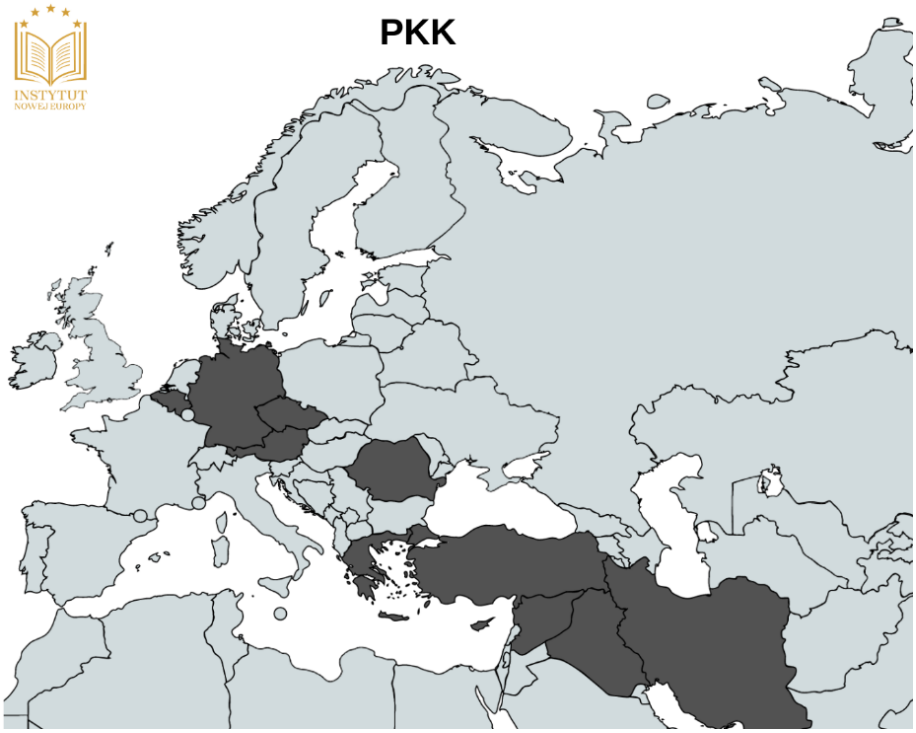
Źródła utrzymania: przemyt, handel narkotykami, finansowanie państwowe (reżim syryjski), grupy syryjskie w Libanie, Libańska Partia Komunistyczna, organizacje palestyńskie, diaspora kurdyjska w Niemczech, pranie pieniędzy, darowizny z innych źródeł

Podsumowanie działalności:

PKK powstała podczas spotkania Abdullaha Ocalana i jego współpracowników w Diyarbakir w Turcji 27 listopada 1978 roku[108]. Spotkanie to jest bardziej znane jako I Kongres PKK. W oświadczeniu o założeniu PKK odniesiono się do idei wyzwolenia Kurdów rozproszonych w Turcji, Syrii, Iranie i Iraku oraz utworzenia „Wielkiego Kurdystanu" w regionie. Zostało to uznane za długoterminowy cel organizacji[109]. Następnie, aby nadać nową siłę ruchowi kurdyjskiemu, a także koordynować działania komórek wojskowych i politycznych, w 2002 roku powstała organizacja wspierająca Kongres Wolności i Demokracji Kurdystanu – KADEK). Zgodnie ze stanowiskiem A. Ocalana, KADEK oświadczył, że cel ruchu zmienił się z „niepodległego Kurdystanu" na „demokratyczną Turcję". Nastąpiło to po tym, jak Departament Stanu USA 1 maja 2003 roku dodał KADEK do swojej listy Zagranicznych Organizacji Terrorystycznych, a KADEK został przemianowany na Kongra-Gel (Kongres Towarzystwa Kurdystanu). Mimo to, również ta organizacja została wkrótce potem wskazana przez Departament Stanu jako organizacja terrorystyczna.

[108] N. Gergin, H. Duru, H. Çetin, *Profile and Life Span of the PKK Guerillas*, Studies in Conflict & Terrorism, 38:3, (2015) ss. 219-232.
[109] E. Uslu, *Turkey's Kurdish Problem: Steps Toward a Solution*, *Studies in Conflict & Terrorism*, 30:2, (2007), ss. 157-172.

Map. Główne regiony operacji PKK



KATA'IB HEZBOLLAH

Miejsce utworzenia: Irak (2006-2007)

Potencjalne terytorium działań: Irak, Syria, Iran, Jordania, Liban, Turcja

Źródła utrzymania: finansowanie państwowe (głównie Iran), porwania dla okupu

Podsumowanie działalności:

Kata'ib Hezbollah (KH) jest sponsorowaną przez Iran antyamerykańską milicją szyicką, działającą głównie w Iraku i prowadzącą dodatkowe operacje w całej Syrii. Grupa jest ideologicznie lojalna wobec irańskiego reżimu[110]. Kata'ib Hezbollah to stosunkowo mała grupa, uważaną za najbardziej tajną szyicką milicję działającą w Iraku, która rekrutuje poprzez nawoływanie do walki z siłami USA. Jest to również grupa, za pomocą której Korpus Strażników Rewolucji Islamskiej – Siły Ghods, jedna z pięciu komórek tej organizacji – nadzoruje i wpływa na rząd w Iraku[111]. Ponadto, po wybuchu wojny domowej w Syrii grupa także ogłosiła swoje wsparcie na rzecz sił Assada. KH otrzymała ogromną pomoc od IRGC-QF w postaci wsparcia logistycznego, uzbrojenia oraz w ramach szkoleń wojskowych. Grupa jest czołowym członkiem Siły Mobilizacji Ludowej (PMF), grupy patronackiej szyickich grup bojowych, które zostały utworzone do walki z Państwem Islamskim w Iraku. W latach 2008-2011 KH kierowała większością swoich ataków na siły koalicyjne USA w Iraku. Od 2 lipca 2009 roku Kata'ib Hezbollah znajduje się na amerykańskiej liście organizacji terrorystycznych. Co ważne, po klęsce Państwa Islamskiego Kata'ib Hezbollah zaczęła wypełniać próżnię władzy stworzoną przez upadek Kalifatu[112]. Od 2017 roku KH zintensyfikowała swoje ataki na siły amerykańskie w Iraku.

---

[110] Counter Extremism Project, *Kata'ib Hezbollah,* https://www.counterextremism.com/threat/kata%E2%80%99ib-hezbollah, dostęp: 05.11.2020.
[111] United Against Nuclear Iran, *Kata'ib Hezbollah*, https://www.unitedagainstnuclearіran.com/report/kataib-hezbollah dostęp: 05.11.2020.
[112] Foundation for Defense of Democracies, *Kataib Hezbollah: Background and Analysis*, 2018.

Map. Główne regiony operacji Kata'ib Hezbollah

KORPUS STRAŻNIKÓW REWOLUCJI ISLAMSKIEJ

Miejsce utworzenia: Iran (1979 r.)

Potencjalne terytorium działań: Bliski Wschód

Źródło utrzymania: finansowanie państwowe (Iran)

Podsumowanie działalności:

Uznaje się, że kluczowym czynnikiem wzrostu potęgi IRGC był brak zaufania władz religijnych do tradycyjnej irańskiej armii. To skłoniło rządzących duchownych do stworzenia własnego, podpartego ideologią, ramienia wojskowego, które miało bronić rewolucji z 1979 roku. Oznacza to, że IRGC uzyskało zarówno ustanowione konstytucyjnie prawa, jak i status pozwalający na angażowanie się politycznie i militarnie[113]. Co jest warte podkreślenia, IRGC zapewnia szkolenia dla członków Hezbollahu od połowy lat 80., wykorzystując Siły Ghods (stanowiące część struktur IRGC), które pełnią kluczową rolę w polityce zagranicznej Iranu, wywierając wpływ na cały region i starając się wzmacniać proirańską koalicję[114]. Zaangażowane siły to od 10 000 do 15 000 osób. Szczególne zadania są powierzane właśnie Siłom Ghods, które działają w strefach konfliktów w Iraku i Syrii, walcząc z ISIS jako obcą organizacją terrorystyczną, a także z syryjskimi bojownikami sprzeciwiającymi się reżimowi Baszara al-Assada. Trzeba zaznaczyć, że koalicja sił irańskich, Hezbollahu oraz inne grupy wspierające irackie i syryjskie milicji miała ogromny wpływ na pokonanie ISIS w regionie[115]. Co istotne, Korpus Strażników Rewolucji Islamskiej został uznany za organizację terrorystyczną jedynie przez 3 kraje: USA, Arabię Saudyjską oraz Bahrajn.

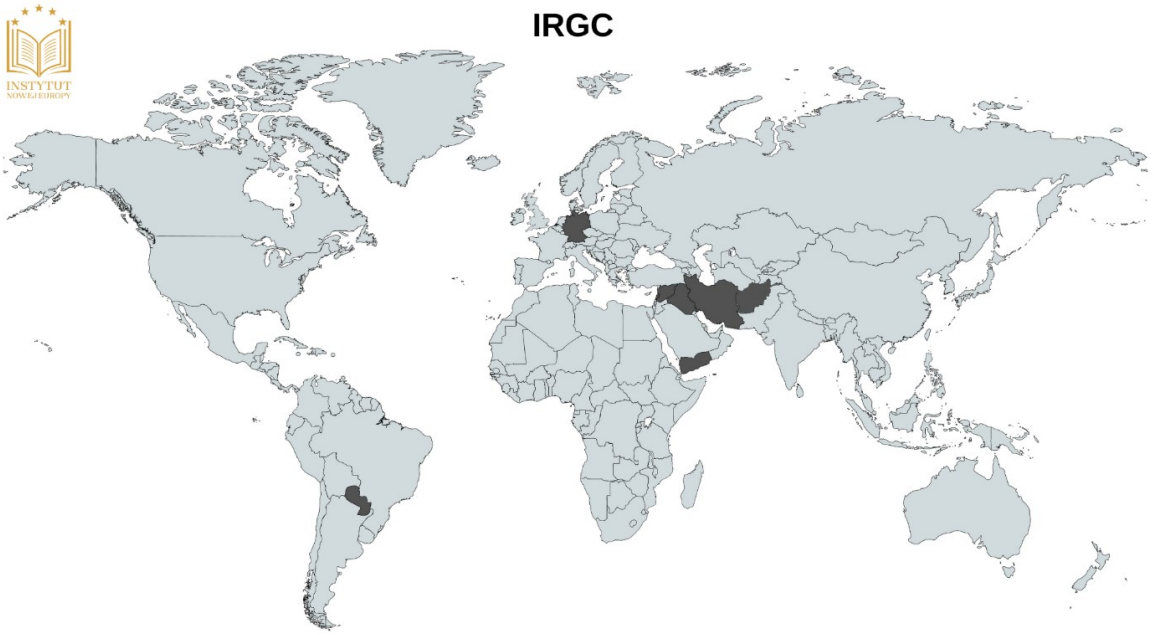
---

[113] Center for Strategic & International Studies, *The Iranian Islamic Revolutionary Guard Corps (IRGC) from an Iraqi View – a Lost Role or a Bright Future?* Available at: https://www.csis.org/analysis/iranian-islamic-revolutionary-guard-corps-irgc-iraqi-view-%E2%80%93-lost-role-or-bright-future, dostęp: 2.11.2020

[114] Wiegand, K. E., 'Reformation of a Terrorist Group: Hezbollah as a Lebanese Political Party', *Studies in Conflict & Terrorism,* 32 (2009) ss. 669-680

[115] Malakoutikhah, Z., 'Iran: Sponsoring or Combating Terrorism?', *Studies in Conflict & Terrorism,* 43, (2020), ss.. 913-939

Map. Główne regiony operacji IRGC



PALESTYŃSKI ISLAMSKI DŻIHAD

Miejsce utworzenia: Egipt (1979 r.)

Potencjalne terytorium działań: Izrael, Zachodni Brzeg i Gaza, Liban, Syria, Iran, Jordania, Jemen, Irak i Turcja

Źródło utrzymania: finansowanie przez Iran oraz Palestynę

Podsumowanie działalności:

Palestyński Islamski Dżihad (PIJ) wyznaje ekstremistyczną ideologię islamską, która traktuje zniszczenie Izraela jako część procesu doprowadzenia do islamskiej rewolucji w świecie arabskim[116]. PIJ przyznała się do szeregu ataków terrorystycznych na Izrael przeprowadzonych w latach 90-tych oraz znacząco zintensyfikowała swoją działalność terrorystyczną od wybuchu intifady Al-Aksa. PIJ w przeciwieństwie do Fatah oraz Hamasu nie ma ambicji politycznych i nigdy nie starała się o reprezentację w Autonomii Palestyńskiej (AP). Organizacja terrorystyczna utrzymuje się głównie dzięki zewnętrznemu wsparciu Iranu. Palestyński Islamski Dżihad chce przywrócić suwerenne Islamskie Państwo Palestyńskie z granicami geograficznymi Palestyny z mandatem sprzed 1948 roku. Członkowie PIJ postrzegają przemoc jako jedyny sposób na usunięcie Izraela z mapy Bliskiego Wschodu i odrzucają jakikolwiek układ o dwóch państwach, w którym Izrael i Palestyna współistnieją[117]. Na terytoriach palestyńskich Hamas i PIJ są uważani za rywali, pomimo ich powiązań jako sunnickie grupy dżihadystów zaangażowane w walkę przeciwko Izraelowi. Chociaż zdarzały się przypadki współpracy między Hama-

[116] *Palestinian public opinion and terrorism: A two-way street?,* Journal of Policing, Intelligence and Counter Terrorism, 10, (2015), ss. 71-87.
[117] Council on Foreign Relations, *Palestinian Islamic Jihad,* https://www.cfr.org/backgrounder/palestinian-islamic-jihad, dostęp: 05.12.2020.

sem a PIJ, to generalnie te dwie grupy pracują niezależnie i rywalizują o wsparcie zarówno wśród ludności palestyńskiej, jak i zewnętrznych zwolenników. Ponadto Hamas i PIJ często publicznie wyrażają swoje różnice[118].

Map. Główne regiony operacji PIJ

[118] Stanford University, *Mapping Militant Organizations*, https://web.stanford.edu/group/mappingmilitants/cgi-bin/pages/definitions, dostęp: 05.12.2020.

TALIBOWIE

Miejsce utworzenia: Afganistan (1994 r.)

Potencjalne terytorium działań: Afganistan, Pakistan, Irak, Rosja, Turkmenistan

Źródła utrzymania: handel narkotykami, finansowanie państwowe (np. Pakistan i Arabia Saudyjska), produkcja opium, darowizny zagraniczne, nielegalne wydobywanie klejnotów, porwania, wymuszenia, podatki nakładane na osoby pozostające pod ich kontrolą

Podsumowanie działalności:

Talibowie (co tłumaczy się jako „studenci") to współcześnie bardzo silna grupa, która wspierała afgańskie powstanie, a także później grupę Haqqani[119]. Talibowie to ruch islamistyczny, który dąży do ustanowienia kalifatu zgodnie z szariatem (prawem islamskim). Jego członkowie opowiadają się za salafizmem – surową i radykalną interpretacją islamu, uważając, że muzułmanie powinni naśladować działania pierwszego pokolenia przywódców muzułmańskich, znanych jako „Sprawiedliwi". Od 2001 r. Talibowie aktywnie walczą, aby USA i NATO opuściły Afganistan oraz delegitymizują obecny rząd Afganistanu. Talibowie stosują zarówno konwencjonalne, jak i niekonwencjonalne taktyki, aby realizować swoje cele. Charakteryzuje się to udziałem w polityce krajowej, a jednocześnie przeprowadzaniem ataków terrorystycznych. Władza grupy jest skoncentrowana i utrzymywana w rękach mułłów z plemion Kandahari Pasztunów, znanych jako Quetta Shura[120].

[119] Counter Extremist Project, *Taliban,* https://www.counterextremism.com/threat/taliban, dostęp: 07.12.2020.
[120] M. Semple, *Rhetoric, Ideology and Organizational Structure of the Taliban Movement*, United States Institute of Peace, Washington 2014.

Map. Główne regiony operacji Talibów

LASZKAR-I-TOIBA / LASHKAR-E-TAIBA

Miejsce utworzenia: Pakistan (1987 r.)

Potencjalne terytorium działań: Pakistan, Indie, Kaszmir, Sri Lanka, Bangladesz, Nepal, Malediwy, USA, Kanada, Australia, Syria, Liban i Egipt

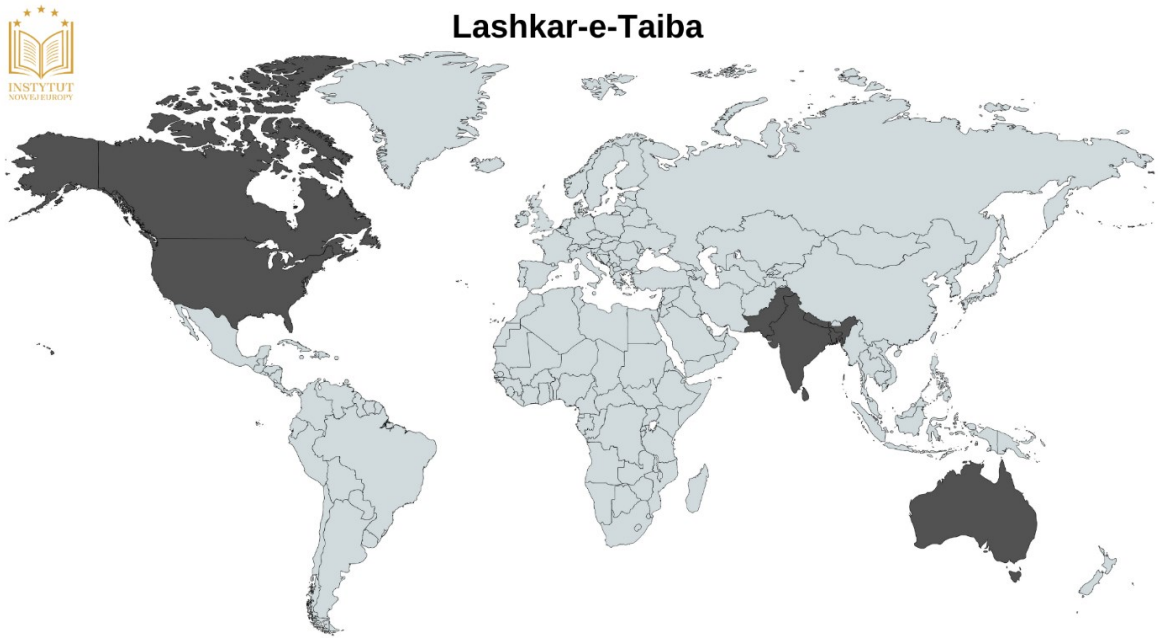
Źródła utrzymania: wsparcie ze strony firm, instytucji i organizacji z Pakistanu, datki od różnych organizacji i prywatnych firm, wymuszenia, handel narkotykami

Podsumowanie działalności:

Laszkar-e-Taiba (LeT), co oznacza „Armia Czystych", to brutalna grupa islamistów z siedzibą w Pakistanie. LeT postrzega walkę z indyjską kontrolą nad Dżammu i Kaszmirem jako część globalnej walki z uciskiem muzułmanów i dąży do ustanowienia islamskiego kalifatu na subkontynencie indyjskim[121]. Od swojego powstania w latach 90., LeT przeprowadził liczne ataki na cele wojskowe i cywilne w Indiach, szczególnie w północnej części kraju w stanach Dżammu i Kaszmir. LeT wyznaje Ahl-e-Hadith, która jest południowoazjatyckim odłamem salafizmu. Podobnie jak Al-Kaida i inne grupy salafickie, LeT stara się odzyskać to, co uważa za „ziemie muzułmańskie". Organizacja stworzyła solidną infrastrukturę w Pakistanie i przyciąga nowych rekrutów poprzez promowanie wizerunku organizacji walczącej z korupcją w państwie. Rząd w Pakistanie wspierał przez długi czas LeT, co grupa wykorzystała zwłaszcza w ciągu kilku pierwszych lat po atakach z 11 września, aby zapewnić wsparcie Al-Kaidzie oraz innym podmiotom podejmującym międzynarodowe operacje na rzecz dżihadu[122].

[121] J. Bajoria, *Lashkar-e-Taiba (Army of the Pure) (aka Lashkar e-Tayyiba, Lashkar e-Toiba; Lashkar-i-Taiba),* Council on Foreign Relations, New York 2010.
[122] S. Tankel, *Laskar-e-Taiba: From 9/11 to Mumbai,* London 2009, s. 5.

Map. Główne regiony operacji Laszkar-I-Toiba



WYKORZYSTANIE SZTUCZNEJ INTELIGENCJI PRZEZ TERRORYSTÓW

Ryzyko zdobycia przez terrorystów sztucznej inteligencji

Ze względu na międzynarodowe zagrożenie terroryzmem[123] panuje powszechne przekonanie, że organizacje ekstremistyczne mogą wykorzystywać sztuczną inteligencję do przeprowadzania ataków. Wśród organizacji, które dysponują wystarczającymi środkami finansowymi, by uzyskać dostęp do tak zaawansowanych technologii, na szczególną uwagę zasługują następujące: al-Kaida, ISIS, Hamas, Hezbollah, talibowie (Taliban), Partia Pracujących Kurdystanu (PKK), Palestyński Islamski Dżihad, Kata'ib Hezbollah, Laszkar-e-Toiba i Boko Haram. Poza własnymi finansami organizacji również fakt otrzymywania pomocy finansowej od państw jest ważnym czynnikiem wpływającym na możliwości pozyskiwania takich technologii i przekłada się na duże korzyści logistyczne i ekonomiczne dla tych organizacji, czego przykładem może być Hezbollah[124]. Taka współpraca ma zwykle miejsce, gdy państwa chcą realizować swoje cele i zamiary przy pomocy terrorystów zamiast angażować swoje własne siły zbrojne.

[123] Institute for Economics &Peace, Global Terrorism Index 2015 – Measuring and understanding the impact of terrorism, Sydney 2015. Institute for Economics &Peace, Global Terrorism Index 2017 - Measuring the impact of terrorism, Sydney 2017. Institute for Economics &Peace, Global Terrorism Index 2019 - Measuring the impact of terrorism, Sydney 2019.

[124] 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.

Możliwość pozyskania sztucznej inteligencji do przeprowadzenia śmiertelnego ataku jest realna, ale w większości przypadków raczej mało prawdopodobna. Niemniej jednak używanie najbardziej zaawansowanej broni na świecie, takiej jak zabójcze roboty[125] – i testowanie jej np. podczas operacji określanych jako „walka z terroryzmem" – może być pierwszym krokiem w kierunku wejścia na czarny rynek broni sterowanej przez sztuczną inteligencję. Taki rynek broni już istnieje, a organizacje terrorystyczne wyszukują i rekwirują także zachodni sprzęt, który zostałby użyty przeciwko nim. Terroryści zawsze starali się przejąć wysoce zaawansowaną broń, aby uzyskać większą przewagę, ale osiągnięcie tego celu stanowi niemałe wyzwanie. W tej części publikacji zostanie przedstawiona ocena możliwości przejęcia i wykorzystania technologii sztucznej inteligencji przez członków organizacji terrorystycznych.

Gdyby terroryści uzyskali dostęp do broni kontrolowanej przez sztuczną inteligencję, znacznie zwiększyłoby to zagrożenie dla społeczności międzynarodowej. Po pierwsze, nie byliby już ograniczani geograficznie i granicami do przeprowadzania ataków w innych krajach. Organizacje terrorystyczne mogą np. zaatakować obiekty w pobliżu granicy lub użyć drona na terenie Stanów Zjednoczonych lub Europy w celu przeprowadzenia ataku. Po drugie, zmniejszy się także ich zapotrzebowanie na zamachowców-samobójców ze względu na zastępowanie ich dronami. Po trzecie, organizacjom będzie łatwiej uzyskać tajne informacje o armiach przeciwnika dzięki operacjom hakerskim wspieranym przez sztuczną inteligencję. W tym scenariuszu organizacje terrorystyczne, którym udało się zdobyć taką technologię, stają się jednym z największych zagrożeń XXI wieku, ale taki obrót wydarzeń wydaje się być mało prawdopodobny. W przypadku państw wspierających terroryzm mało prawdopodobne jest, aby umożliwiły one wspieranym organizacjom terrorystycznym dostęp do najnowszych technologii, obawiając się utraty kontroli nad terrorystami; należy wziąć pod uwagę np. reperkusje działającego na własną rękę Hezbollahu, jeśli Iran udzieli mu tego rodzaju wsparcia.

[125] H. Liu, L. Van Rompaey, M. Maas, *Beyond Killer Robots: Networked Artificial Intelligence Systems Disrupting the Battlefield?*, Journal of international humanitarian legal studies 10 (2019), s. 77-88.

Nie jest to jednak wykluczone i patrząc na obecną sytuację międzynarodową, można postawić tezę, że terroryści będą wykorzystywani do realizacji celów poszczególnych państw.

Perspektywa wykorzystania sztucznej inteligencji w trakcie konfliktu zbrojnego wydaje się być równie kusząca, co niepokojąca. Podczas gdy sztuczna inteligencja może niezwykle szybko stać się tak skuteczna jak żołnierze, którzy przez lata zdobywali umiejętności i doświadczenie, w przeciwieństwie do nich pozbawiona jest kompasu moralnego. Użycie broni opartej na sztucznej inteligencji oznacza ograniczony, lub wręcz całkowity, brak zahamowań wpływających na zachowania bojowe oraz, w dłuższej perspektywie, na doktrynę. Organizacje terrorystyczne są odpowiedzialne za tysiące ofiar śmiertelnych, cywilnych i wojskowych, i nie przeszkadza im wykorzystywanie zaawansowanych technologii w celu zwiększenia tej liczby. Dla takich grup sztuczna inteligencja jest po prostu kolejnym środkiem walki z wrogiem – zmienia się narzędzie, ale nie ideologia. Charakterystyczna fanatyczna wiara w znaczenie ich agendy jest tym, na czym opierają się jako grupa. Dlatego nie będą ograniczały ich takie pojęcia, jak przyzwoitość, moralność czy proporcjonalność – przez co niewiele różnią się od robotów sterowanych przez sztuczną inteligencję. W rezultacie sama sztuczna inteligencja jest niczym innym jak środkiem do maksymalizacji szkód i minimalizacji strat. Ponadto drony mogą być używane do celów propagandowych, aby pochwalić się własnym postępem technologicznym. Konkludując, można postawić tezę, że fanatyczna natura terrorystów zmusi ich do użycia sztucznej inteligenci, np. w postaci drona wspieranego przez jej algorytmy, do przeprowadzania ataków na regularne wojsko lub cele cywilne, nawet jeśli takie wykorzystanie SI nie jest kluczowe dla ich operacji[126].

[126] 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.

BEZZAŁOGOWY STATEK POWIETRZNY – ŚMIERCIONOŚNA BROŃ DLA TERRORYSTÓW

Współcześnie globalne zagrożenia terrorystyczne wiążą się między innymi z wykorzystaniem sztucznej inteligencji, która obsługiwałaby uzbrojone roboty, pociski, a także służące do zabijania drony. Szansa organizacji terrorystycznych na uzyskanie dostępu do zaawansowanych technologii wzrasta ze względu na globalną konkurencję. Materiały prasowe, zdjęcia oraz filmy są wykorzystywane przez wiele państw, które chcą podkreślić swoje wysiłki i osiągnięcia w rozwoju sztucznej inteligencji. W przypadku większości mocarstw systemy ze wsparciem sztucznej inteligencji są konieczne na współczesnym polu bitwy. Wagę tego zjawiska tylko podkreślają przeszkody, jakie stawiają USA, Chiny, Rosja lub Iran agencjom wywiadowczym innych państw, w celu zabezpieczenia przed kradzieżą danych badawczych dotyczących SI. Jednak wzrost zainteresowania spowoduje dalszy rozwój i szerokie wykorzystanie technologii. W związku z tym potencjalnym rozprzestrzenieniem, również terroryści będą mieli szansę prowadzić działania z użyciem broni wspieranej przez sztuczną inteligencję. Wydarzenia te tworzą mocno niepokojący scenariusz, z którym prawdopodobnie trzeba będzie się wkrótce zmierzyć.

Bezzałogowe statki powietrzne, takie jak drony, mogą być pierwszym typem broni kontrolowanej przez sztuczną inteligencję i używanej w celach terrorystycznych. Ich prostota umożliwia terrorystom przeprowadzenie ataku bez angażowania dużej liczby osób lub logistyki. W zależności od skali ataku niektóre uderzenia mogą być koordynowane nawet przez jedną osobę. Istnieją przykłady organizacji terrorystycznych przeprowadzających ataki przy użyciu dronów wspieranych przez sztuczną inteligencję i są one wymienione poniżej.

Wykorzystanie przez terrorystów dronów sterowanych przez sztuczną inteligencję

Aktorzy niepaństwowi, w tym organizacje terrorystyczne, od lat próbują używać dronów przeciwko państwom. Według pojawiających się w mediach informacji miała już miejsce znaczna liczba takich wydarzeń i do końca 2016 roku żadne z nich nie było śmiertelne. Drony były zwykle używane do przelotu nad określoną częścią terytorium w celu zbierania informacji wywiadowczych na temat baz wojskowych oraz możliwego uzbrojenia. Mimo ograniczonych możliwości, terroryści byli w stanie przeprowadzać udane misje, ostrzeliwując obiekty wojskowe. Na początku XXI wieku najczęściej używano dronów w regionach Izraela i Pakistanu, niemniej jednak na przestrzeni lat stopniowo poprawiały się zdolności organizacji terrorystycznych i w ciągu ostatnich 5 lat odnotowano więcej ataków (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 atak przy użyciu tego rodzaju technologii, najprawdopodobniej dokonany przez Państwo Islamskie[127]. Do tego czasu, zgodnie z informacjami z Pentagonu, terroryści używali

[127] 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.

tylko podstawowych wersji dronów, które są łatwo zakupić i obsługiwać w celu prowadzenia obserwacji czy transportu materiałów wybuchowych. W ramach swojej taktyki siły amerykańskie użyły specjalnego sprzętu do pokonania bezzałogowców – „karabinów" przeciwdronowych – aby zakłócić sygnał pomiędzy maszyną a pilotem[128].

Tab. Przykłady zastosowań dronów przez organizacje terrorystyczne do 2015 roku

DATA	LOKALIZACJA	ORGANIZACJA TERRORYSTYCZNA
14 LIPCA 2014	Aszdod, Izrael	Hamas
23 SIERPNIA 2014	Okolice Muhafazy ar-Rakka, północna Syria	Państwo Islamskie
30 SIERPNIA 2014	Faludża, Irak	Państwo Islamskie
12 WRZEŚNIA 2014	Kobanî, północna Syria	Państwo Islamskie
21 WRZEŚNIA 2014	Okolice Arsalu, północno-wschodni Liban	Hezbollah
16 MARCA 2015	Okolice Faludży, Irak	Państwo Islamskie

Źródło: R. J. Bunker, *Terrorist and insurgent unmanned aerial vehicles: use, potentials, and military implications,* Strategic Studies Institute and U.S. Army War College Press, August 2015, s. 13-15.

Innym przykładem jest wysłanie przez ISIS bezzałogowego statku powietrznego załadowanego materiałami wybuchowymi do ataku na pozycje francuskie i kurdyjskie w północnej części Iraku, w Erbilu. Dwóch żołnierzy kurdyjskich zostało zabitych, a dwóch francuskich żołnierzy sił specjalnych zostało ciężko rannych. Materiały wybu-

[128] 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.

chowe były ukryte w małym samolocie wypełnionym styropianem. Jest to jedna z najpopularniejszych metod ISIS użycia dronów przez ISIS[129]. Należy podkreślić, że atak ten był początkiem działań terrorystycznych wspomaganych wysoko rozwiniętymi technologiami, a także wskazówką, w jakim kierunku pójdą ekstremiści.

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 jej przystosowania do użycia jako broni. Grupa wykorzystuje technologię dronów do obserwacji i namierzania, głównie w Iraku i Syrii. Pomimo rosnących strat terytorialnych, ISIS stale czyni postępy w modernizacji, produkcji i rozmieszczaniu dronów. Ponadto organizacja była w stanie zaatakować dronem czołg bojowy w Mosulu w 2017 roku[130].

Na początku 2019 roku miał miejsce bezprecedensowy atak: rój dronów zaatakował dwie rosyjskie bazy wojskowe w Syrii. Wspomniane drony posiadały czujniki barometryczne, które umożliwiały im zmianę wysokości, oraz wysoko rozwinięte wskazówki GPS z zaprogramowanymi konkretnymi celami do zniszczenia[131]. Innymi słowy, drony te po wypuszczeniu nie wymagały dalszych instrukcji ani wskazówek od terrorystów. Dziesięć z takich dronów było wyposażonych w ładunki wybuchowe i zeszło nad bazą lotniczą Humajmim, a trzy inne skierowały się na okręt wsparcia bojowego rosyjskiej marynarki wojennej w pobliżu Tartusu. Inną bronią były łuski wypełnione czterozotanem pentaerytrytolu (PETN), które przymocowane były do skrzydeł. Co gorsza, bezzałogowce latały na małych wysokościach, przez co nie mogły zostać wykryte przez systemy radarowe. Ich ataki z wielu kątów zostały zsynchronizowane w sposób, który

[129] 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.
[130] 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.
[131] M. Morton, *Inside The Chilling World Of Artificially Intelligent Drones*, https://www.theamericanconservative.com/articles/inside-the-chilling-proliferation-of-artificially-intelligent-drones, dostęp: 20.09.2020.

zmylił systemy obrony powietrznej. Ostatecznie jednak atak, który prawdopodobnie został przygotowany przez grupę syryjskich rebeliantów, nie powiódł się. Rosyjskie systemy zareagowały poprzez połączenie kinetycznych i elektronicznych modeli ochrony powietrza.

W tym samym roku zdalnie pilotowany przez jemeńskich rebeliantów Houthi statek zaatakował instalacje naftowe Arabii Saudyjskiej w Bukajku i Churais. Rebelianci celowali w największy na świecie zakład przetwórstwa ropy, który ma kluczowe znaczenie dla globalnych dostaw energii[132]. 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. Chociaż Arabia Saudyjska ma systemy 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.

Tego typu ataki są pierwszym krokiem symbolizującym, że postęp technologiczny może pozwolić atakującemu, przy wykorzystaniu nowoczesnej broni, na niezależne niszczenie (częściowe lub całkowite) infrastruktury wroga. Większość krajów biorących udział w wyścigu na rzecz rozwoju sztucznej inteligencji wykorzystuje mniejsze, szybsze i praktycznie niezależne drony, czego skutkiem będzie zwiększona dotkliwość przyszłych ataków. Jednocześnie rządy i firmy prywatne opracowujące tego typu zaawansowane technologie są narażone na niebezpieczeństwo działań szpiegowskich (sama ich liczba daje aktorom wiele możliwości kradzieży informacji poprzez cyberataki). Aktorzy niepaństwowi już teraz wykorzystują podobny sprzęt do zdobywania in-

[132] 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.

formacji o lokalizacji sił zbrojnych, rodzaju uzbrojenia czy potencjalnych ruchach żołnierzy. W tym sensie terroryści działają podobnie jak siły państwowe, a posiadanie zaawansowanych technologii pozwoli im walczyć na równych warunkach poprzez znajdowanie nowych sposobów zwalczania wroga (podobnie jak prywatne firmy wojskowe również działają porównywalnie do sił państwowych ze względu na posiadanie zaawansowanej technologii). W związku z tym wydaje się, że każdy aktor (państwowy czy niepaństwowy) musi zaakceptować rzeczywistość, w której bezzałogowe statki powietrzne sterowane przez sztuczną inteligencję stają się podstawowym narzędziem na polu bitwy, mimo że toczą się dyskusje i wysuwane są pytania o etykę rozmieszczania dronów na polu walki[133]. Użycie dronów stworzyło atmosferę strachu, w której niezbędne jest opracowanie środków zaradczych, aby zapobiec ich użyciu. Dlatego konieczne jest ulepszanie uzbrojenia defensywnego i ofensywnego, jeśli państwo chce pozostać kluczowym graczem w globalnym wyścigu.

Niemniej jednak prawda jest taka, że bezzałogowce są stosunkowo niedrogie i łatwe w produkcji, co oznacza, że ich utrata ma niewielki wpływ na działalność terrorystów. 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 przez grupy przestępcze, terrorystów, separatystów czy rebeliantów. W dużej mierze zależy to od możliwości logistycznych, finansowych i terytorialnych, niemniej jednak w tym kontekście należy wskazać następujące aspekty.

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

Użycie dronów na duże odległości

Większość grup terrorystycznych może przeprowadzić atak z dużej odległości. Posiadanie technologii pozwalającej namierzyć cel, a także skoordynować z nim zestaw działań, to doskonała broń w trakcie konfliktu zbrojnego. Największe organizacje terrorystyczne mają swoje siedziby na Bliskim Wschodzie i w Afryce lub próbują zająć część terytorium w obszarze swoich operacji. Jeśli jest to region, w którym regularnie ścierają się z państwową armią lub znajduje się on w pobliżu granicy, o wiele bardziej opłacalne jest dla organizacji terrorystycznych wysyłanie dronów z bombami. Odległość od siedziby grupy terrorystycznej może być trudna do przebycia, ale jeśli istnieje możliwość wysłania bezzałogowca, to przeprowadzenie ataku staje się łatwiejszym zadaniem. Jeśli organizacje osiągają przewagę w powietrzu dzięki użyciu drona, to staje się to nie tylko kwestią odległości lub logistyki, ale także pomnażania sił. Początkowo przy ataku dronami głównym celem terrorystów jest zaskoczenie przeciwnika, a następnie wyrządzenie jak największych szkód, najlepiej bez użycia własnych sił. Sterowane przez sztuczną inteligencję drony są w stanie namierzyć i wyeliminować cel, po czym natychmiast wrócić do kryjówki terrorystów. W tym scenariuszu walka z terrorystami na odległość nigdy nie była bardziej prawdopodobna.

Jeśli terroryści dokonają ataku przy użyciu dronów, to spotka się on z odpowiedzią władz państwowych, co będzie prowadzić do dalszej eskalacji konfliktu. Co ważne, terroryści mogą wykorzystywać jeden z ataków dronami jako sposób na odwrócenie uwagi, aby przeprowadzić podobny zamach w innym miejscu. Kiedy wszystkie zasoby państwowe skoncentrowane są na wyeliminowaniu zagrożenia w jednym miejscu, naturalny brak sił w innych miejscach z pewnością mógłby zostać wykorzystany. Anders Breivik zdetonował bombę przed siedzibą premiera Norwegii, aby odwrócić uwagę, po czym udał się na wyspę Utøya, gdzie zabił 69 osób. Terrorysta może pracować nad pozyskaniem i przygotowaniem wielu dronów do przeprowadzenia zsynchronizowanego ataku w wielu częściach gęsto zaludnionych obszarów. Tam, gdzie uderzy jeden

dron, odpowiedzą władze – będzie to powtarzający się wzorzec z większą liczbą uderzeń występujących po sobie. W ten sposób nadwerężone zostaną zasoby władz lokalnych, spowoduje to znacznie większy chaos i panikę. Możliwe, że sprawca nie będzie nawet musiał brać fizycznego udziału w ataku, ponieważ sztuczna inteligencja będzie w stanie koordynować i przeprowadzać atak przy niewielkim lub żadnym wkładzie ze strony terrorysty. Zapewni to również terrorystom większą anonimowość ze względu na brak konieczności ujawniania oraz mniejsze ryzyko schwytania, co oznacza przeprowadzenie kolejnych ataków w przyszłości.

Przystępna cena za zaawansowaną technologię

Prawdopodobne jest, że grupy terrorystyczne w końcu zdobędą drony sterowane przez sztuczną inteligencję. Cena tej unikatowej technologii rośnie każdego dnia, a jej powszechne zastosowanie przez Stany Zjednoczone, Chiny, Rosję, Indie, Zjednoczone Królestwo czy Niemcy spowoduje łatwiejszy do niej dostęp. Ogólnie rzecz biorąc, trudność w pozyskaniu dronów sterowanych przez sztuczną inteligencję będzie mniejsza niż się może się wydawać – istnieje kilka czynników, które prowadzą do takiego wniosku. Globalne zaangażowanie mocarstw w wojny na Bliskim Wschodzie i w Afryce, podobnie jak ciągłe doskonalenie systemów obronnych oraz koncentrowanie interesów państwa na bezpieczeństwie gospodarczym i regionalnym (a tym samym angażowanie dalszych środków w regionie), stwarza szansę organizacjom terrorystycznym na wyszukanie, zarekwirowanie, a nawet zakupienie takiego sprzętu. Przy czym nie jest to kwestia „jeśli", ale „kiedy i przeciw komu" będą go używać. Wykorzystanie tej broni – która jest już powszechnie używana przez armie państwowe – przez ekstremistów wprowadza nową dynamikę na polu bitwy.

Nowatorskość tej technologii sprawi, że początkowo trudno będzie ją zdobyć czy kupić. Jednak kwestią czasu, aż pierwsza grupa uzyska do niej dostęp i przeprowadzi ataki terrorystyczne. Może być sprzedawana przez jakieś państwo lub nabyta w

drodze nielegalnych inwestycji w państwach trzecich. Niemniej jednak koszt zakupu i przyszłej obsługi spadnie do „rozsądnego" poziomu dla co najmniej kilku organizacji terrorystycznych, które już teraz dysponują dużymi środkami finansowymi.

Map. Potencjalne terytorium działań na Bliskim Wschodzie

Niewymagający proces eksploatacji

Wydaje się, że terroryści raczej nie opracują własnej sztucznej inteligencji ani dronów. Nie mają czasu na tak długotrwały i wymagający finansowo proces – grupy ekstremistów muszą być zaopatrzone w konkretną broń gotową do natychmiastowego użycia. Proces nabycia zależy od dostawcy, zwłaszcza gdy organizacja nie ma własnej

produkcji ani odpowiednich inżynierów. Do operatora należy tylko kilka kwestii technicznych: określenie celu ataku, uzbrojenie platformy i jej utrzymanie. Przeszkody w programowaniu drona i zapewnieniu wsparcia technicznego nie powinny stanowić problemu, jeśli broń jest zmontowana i dostarczona, czyli 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.

Etykietowanie działalności terrorystycznej

Informacje o terrorystach biorących udział w ataku przeprowadzonym przy użyciu dronów sterowanych przez sztuczną inteligencję mogłyby zostać upublicznione w zależności od potrzeb sprawcy, kontekstu międzynarodowego, a przede wszystkim tego, czy istnieją wystarczające dowody, by winić organizację, a nie państwowego dostawcę. Niektóre organizacje terrorystyczne, takie jak Państwo Islamskie, Al-Kaida, czy Hamas, będą preferować wywieranie wpływu i głośno manifestować swój nowy sukces. Mogą też zrobić to, aby ogłosić społeczności międzynarodowej, że mają tego rodzaju broń i mogą w większym stopniu konkurować z wojskami państwowymi. Co więcej, zapewne wykorzystają swoje pierwsze ataki, aby szerzyć panikę, grożąc przeciwnikom kolejnymi zamachami. Z drugiej strony, pojawią się grupy, które nie będą chciały kojarzone z tego rodzaju morderczymi atakami – będą to prawdopodobnie mniejsze grupy nacjonalistyczne lub separatystyczne.

Biorąc pod uwagę tendencje organizacji terrorystycznych do demonstrowania swojej obecności i siły, można przypuszczać, że będą umieszczać dowody ich użycia w mediach społecznościowych. Jeśli do uderzenia dojdzie w obcym kraju, terroryści

mogą uruchomić drona na odległość i nie będzie potrzeby angażowania wielu członków jak ma to miejsce przy skumulowanym ataku terrorystycznym. Maszyna będzie mogła zostać wysłana np. z przedmieść Paryża, a celem może stać się Wieża Eiffla.

Oprócz powyższych, należy wziąć pod uwagę sytuację w której zostaną przeprowadzone ataki przez anonimowe lub niezidentyfikowane grupy. Takie działanie znacznie utrudni weryfikację sprawców oraz właściwe określenie, kto jest odpowiedzialny za zamach. Taki „anonimowy" atak mógłby zostać wykorzystany do zmylenia niektórych państw lub celowego wywołania konfliktu.

Obrona przeciwlotnicza

Ostatnio rozmieszczenie dronów przyspieszyło na wielu polach walki; staje się naturalnym rozszerzeniem narzędzi już dostępnych na wojnie. Dodatkowo cały czas prowadzone są testy, które zwiększą potencjał bojowy bezzałogowych bojowych statków powietrznych w wielu sytuacjach, takich jak niszczenie lub wprowadzanie w błąd obrony przeciwlotniczej. Przewaga wynikająca z używania niewykrywalnych bezzałogowców kontrolowanych przez sztuczną inteligencję stałaby się najważniejszym elementem uzbrojenia.

Jest oczywiste, że większość państw zaangażowanych w konflikty – jak te w Syrii czy w Libii – testuje nową broń. Co więcej, niektóre z tych prób dały znakomite rezultaty. Podczas konfliktu w Libii, Turcja dostarczyła drony dla Rządu Porozumienia Narodowego (GNA), który rzekomo zniszczył system przeciwlotniczy Pancyr-S1 przekazany przez Rosjan opozycyjnej Libijskiej Armii Narodowej (LNA). 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[134].

Organizacje terrorystyczne z pewnością będą starały się zdobyć tego rodzaju zaawansowaną broń. Dążą do tego, aby działać na tym samym poziomie, co organizmy państwowe, często okrutnie zaznaczając swoją obecność. Jednym z wielu przykładów są wspomniane wyżej saudyjskie obiekty naftowe, które były celem przeprowadzonych przez rebeliantów Houthi ataków rakietowych i 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 ich ochrony, a atakujący mają do dyspozycji szeroką gamę broni elektronicznej i kinetycznej.

Zwiększone wykorzystanie dronów do ataków

Tak długo, jak wysoko rozwinięte technologie mogące przechytrzyć i pokonać obronę przeciwlotniczą oraz zszokować społeczność międzynarodową nie są dostępne dla organizacji terrorystycznych, nie ma powodu do obaw. Niestety, dla większości krajów ważniejsze są umowy dwustronne i prywatne interesy, co powoduje, że poszukiwane uzbrojenie, często pożądane i łatwe do sprzedania na czarnym rynku, stają się dostępne. Dla terrorystów każda nowa technologia jest na wagę złota. Niektórzy aktorzy państwowi będą współpracować i udostępniać zaawansowane technologie, aby osiągnąć swoje cele. Dlatego ekstremiści raczej wcześniej niż później wejdą w posiadanie dronów kontrolowane przez sztuczną inteligencję. Pierwszym krokiem do

[134] 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.

uzyskania tej możliwości jest udostępnienie im nowych technologii i dostarczenie niewielkiej liczby dronów do przeprowadzenia ataków. Ewentualnie bojownicy mogą mieć możliwość odszukania lub zarekwirowania sprzętu przeciwników wystawionego na polu walki, co zdarzało się wielokrotnie na obszarach konfliktu. Szerokie wykorzystanie sprzętu wspieranego przez sztuczną inteligencję może zwiększyć szanse terrorystów na przejęcie takich urządzeń poprzez samo zwiększenie okazji do ich zajęcia. W konsekwencji terroryści nie tylko będą nadal mieć wpływ na sytuację w globalnym środowisku bezpieczeństwa, ale sztuczna inteligencja będzie odgrywać rolę wzmacniającą, ponieważ również będzie w stanie przeprowadzać ataki. W końcu zagrożenie zostanie podwojone i wymknie się spod kontroli.

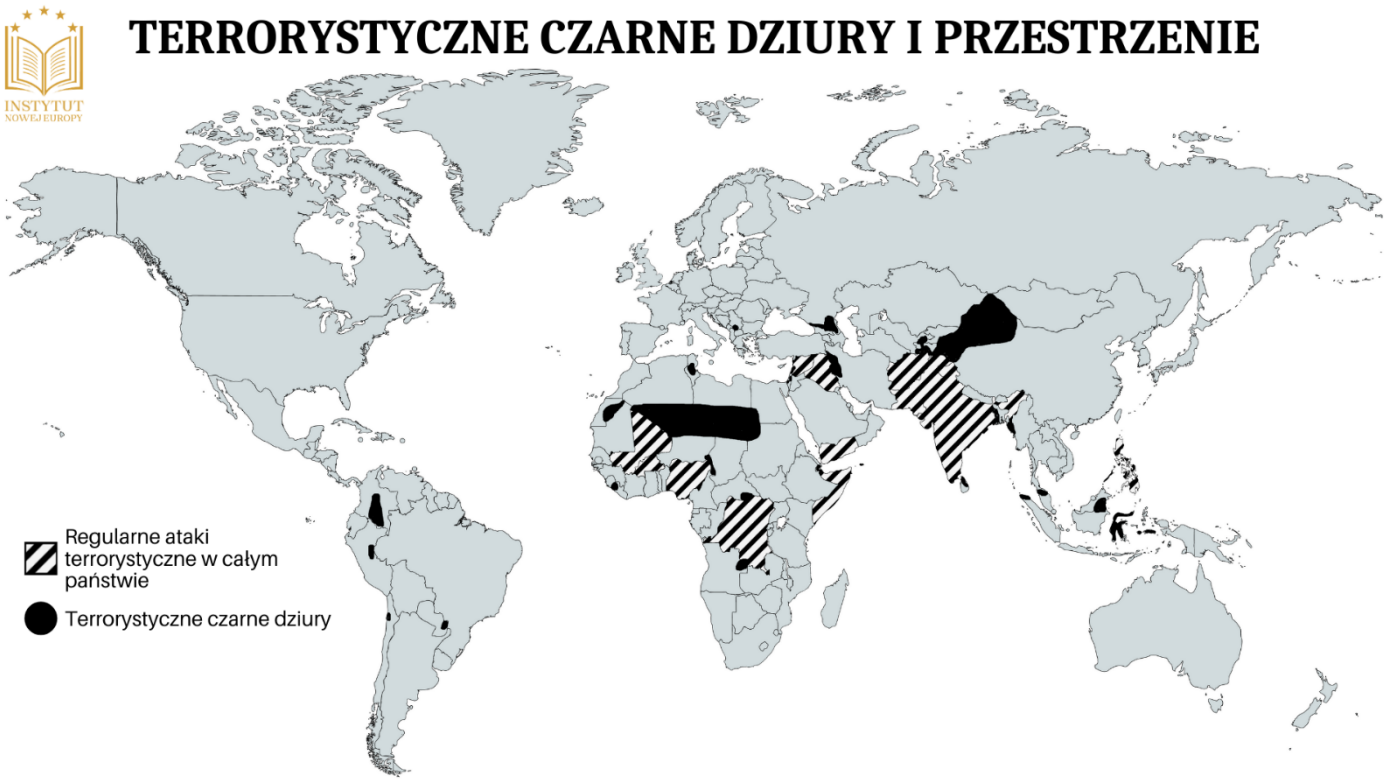
Wykorzystanie systemów sztucznej inteligencji przez terrorystów może nie być natychmiastowe, ponieważ muszą oni dostosować się i zrozumieć nową technologię. Niemniej jednak mają wiedzę na temat cyberbezpieczeństwa, potrafią włamywać się do systemów bezpieczeństwa czy wysyłać złośliwe aplikacje w celu przejęcia kontroli nad smartfonami i komputerami. To daje również możliwe do przekazania umiejętności, które pozwolą im szybko zrozumieć oprogramowanie sztucznej inteligencji.

Końcowe przemyślenia na temat dronów

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 w którym część dronów ostrzeliwuje obiekt, kolejne zrzucają bomby, a jeszcze inne wykonują loty patrolowe, wydaje się być doskonałym sposobem na realizację misji. Jednak przeprowadzenie tego rodzaju ataku przez ludzi kontrolujących drony wydaje się niemożliwe. Żaden oddział żołnierzy nie byłby w stanie kontrolować toru lotu każdego pojazdu w roju tak skutecznie, jak sztuczna inteligencja. W przypadku złożonego, specyficznego typu misji

jedna osoba powinna odpowiadać za jednego drona. W tym scenariuszu ludzka kontrola byłaby stosunkowo bardziej chaotyczna niż kontrola prowadzona przez sztuczną inteligencję ze względu na brak szybkiego i przejrzystego kanału komunikacyjnego podczas gwałtownego ataku. Dodatkowo technologia przeciwdronowa umożliwia broniącym się zagłuszanie sygnału z kontrolera. 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.

Map. Terrorystyczne czarne dziury i przestrzenie



Źródło: opracowanie własne na podstawie: Korteweg, R., Ehrhardt, D., *Terrorist Black Holes,* Center for Strategic Studies, Den Haag 2005, s. 34.

Ponadto możliwe jest, że drony będą mogły przenosić ładunek bojowy 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 2,8-8 ton[135]. Dlatego atak roju dronów przenoszących co najmniej kilka ton ładunków wybuchowych stałby się najbardziej śmiercionośną bronią na świecie (nie licząc broni jądrowej).

Oprócz wykorzystywania dronów sterowanych przez sztuczną inteligencję do zwiększania swojej siły terroryści mogą również rozważyć możliwość wykorzystania ich w celu zachowania anonimowości, czynnika ludzkiego podczas przeprowadzania ataku, zarówno zakończonego sukcesem, jak i niepowodzeniem. Jednak kluczowe ograniczenie tej taktyki uniemożliwia organizacji wykorzystanie jej do siania chaosu, gdyby próbowała udawać aktora państwowego: agencje wywiadowcze są niezwykle operatywnymi podmiotami, zdolnymi do porównywania informacji i identyfikowania tła używanego urządzenia w oparciu o cechy przedmiotu, okoliczności, w których przedmiot (lub inne, podobne do niego przedmioty) mógł zostać przyjęty lub użyty oraz wzorce składające się na atak. Agencje wywiadowcze są już świadome możliwości wykorzystania dronów przez terrorystów do ataku, ponieważ przechwyciły kilka w przeszłości. Poza tym można przypuszczać, że agencje wywiadowcze, nawet te w rywalizujących państwach, byłyby skłonne podzielić się pewnymi informacjami wywiadowczymi w interesie zwalczenia wspólnego wroga, takiego jak organizacja terrorystyczna. Państwa nie uciekałyby się od razu do wskazywania winnych – co działałoby na korzyść agresora – nie znając wszystkich faktów.

[135] R. McDermott, *Moscow Unveils Further Advances in Drone Technology*, Eurasia Daily Monitor, Volume: 16, Issue: 139.

Jeśli chodzi o skalę, jest możliwe, że wojna dronów między aktorami państwowymi i niepaństwowymi byłaby podobna do walk między siłami powietrznymi państw o utrzymanie dominacji na niebie. Terroryści mieliby możliwość walki z dominacją mocarstwa w powietrzu, a nawet wykorzystania sprzętu lotniczego. W ten sposób uzyskaliby możliwość osłabienia kluczowych przewag, którymi mocarstwa i inni aktorzy państwowi cieszyli się przez wiele lat w walce z terroryzmem.

DRUK 3D JAKO PRZYSZŁE ZAGROŻENIE TERRORYSTYCZNE

Druk 3D można opisać jako wirtualny projekt konkretnego przedmiotu, który następnie zostanie stworzony (lub wydrukowany). Jest to proces, za pomocą którego z pliku cyfrowego można tworzyć bryły 3D o dowolnym kształcie i geometrii. Istnieje kilka programów, które pozwalają opracować projekt do modelowania 3D. Przedmiot można replikować na podstawie istniejącego modelu lub można go zbudować od podstaw. Skaner 3D znajdujący się w drukarce 3D precyzyjnie kopiuje zeskanowany obiekt fizyczny i przesyła jego schematy w postaci pliku cyfrowego[136]. Istotnym elementem jest digitalizacja rzeczywistego przedmiotu. Aby uzyskać złożony plik cyfrowy, niezbędne jest użycie profesjonalnego urządzenia przemysłowego, które tworzy model 3D dzięki tysiącom poziomych linii. Drukarka 3D składa się z zestawu komponentów, które działają jednocześnie, aby wytworzyć pożądany wynik z wprowadzonego pliku cyfrowego[137]. Kiedy cały wielowarstwowy model zostanie przesłany do drukarki 3D, oprogramowanie tworzy dokładny obiekt, który łączy każdą warstwę, w konsekwencji dostarczając trójwymiarowy projekt gotowy do druku. Istnieje wiele różnych skanerów 3D, które wykorzystują różne technologie do skanowania – np. czas naświetlania, światło modulowane i wiele innych, które wciąż są ulepszane. Wszystko zależy od skali,

[136] A. Syed, P. Elias, B. Amit, B. Susmita, O. Lisa, C. Charitidis, *Additive manufacturing: scientific and technological challenges, market uptake and opportunities,* Materials today 2017, Vol. 1, s. 1-16.
[137] S. Mkhemer, 3D Printing Technology, Birzeit University, December 2014, s. 3-5.

ilości detali przedmiotu, materiałów użytych do jego wykonania czy wreszcie kompatybilności z innymi elementami, z którymi obiekt będzie używany[138].

Druk 3D jest szeroko rozwijany na całym świecie. Stwarza nowe możliwości dla firm, które chcą poprawić wydajność produkcji. Konwencjonalne tworzywa termoplastyczne, ceramikę, materiały na bazie grafenu i metal można teraz pozyskiwać za pomocą technologii druku 3D[139], który jest coraz częściej stosowany dla indywidualizacji masowej czy produkcji wszelkiego rodzaju projektów typu *open source* w rolnictwie, służbie zdrowia, a także w przemyśle samochodowym i lotniczym[140]. Jednak obecny rozwój tej technologii, a także możliwości wykorzystania w niej sztucznej inteligencji prowadzą do popularyzacji wielu zaawansowanych technologicznie systemów, które w rękach ekstremistów mogą być niebezpieczne.

Wykorzystanie druku 3D do produkcji broni ręcznej ma kluczowe znaczenie dla organizacji terrorystycznych, ponieważ państwa mają do dyspozycji inne możliwości prowadzenia podobnych operacji[141]. Jest prawdopodobne, że terroryści mogą zdobyć tę technologię do produkcji broni z zamiarem przeprowadzania ataków. Coraz popularniejsze wśród tych grup staje się samodzielne tworzenie broni zamiast inwestowania w zakup jej, czy też materiałów wybuchowych, na czarnym rynku. Przez drukowanie 3D uzbrojenie staje się łatwo dostępne, niemniej jednak broni wydrukowanej w 3D nie można załadować pociskiem, który nie jest do niej dopasowany – wymaga to sprawdzenia wytrzymałości materiałów. Poza tym w większości przypadków wydrukowana broń może zostać użyta tylko raz do wystrzelenia krótkiej serii lub nawet pojedynczego pocisku. Niemniej jednak fakt, że terroryści mogą drukować broń w każdym miejscu

[138] A. J. Almaliki, *The Processes and Technologies of 3D Printing*, International Journal of Advances in Computer Science and Technology, Volume 4 No.10, October 2015, s. 161-162.
[139] L. Ze-Xian, T. Yen, M. Ray, D. Mattia, I. Metcalfe, D. Patterson, *Perspective on 3D printing of separation membranes and comparison to related unconventional fabrication techniques*, Journal of Membrane Science 2016, Vol 523, No.1, s. 596-613.
[140] N. Shahrubudina, T.C. Leea, R. Ramlana, *An Overview on 3D Printing Technology: Technological, Materials, and Applications*, Procedia Manufacturing 35 (2019), s. 1286-1296.
[141] K. Brockmann, R. Kelley, *The Challenge of Emerging technologies to non-Proliferation Efforts controlling Additive Manufacturing and intangible Transfers of Technology,* Solna 2018, s. 36.

na świecie stanowi niezwykle duże zagrożenie dla bezpieczeństwa. Jakość druku 3D wzrasta, a dostęp do technologii zwiększa ryzyko oraz skuteczność terrorystów używających drukowanej broni[142]. Dostępność tej technologii może skutkować wzrostem liczby ataków terrorystycznych w wielu krajach. W Republice Francuskiej prawie 50% ataków przeprowadzonych przez islamskich terrorystów zostało dokonanych z użyciem broni palnej[143].

Druk 3D i ataki terrorystyczne

Jednym z najbardziej godnych uwagi przykładów wykorzystania druku 3D do celów terrorystycznych był atak na synagogę w Halle w Niemczech. Ekstremista, 28-letni obywatel Niemiec Stephan Balliet, zdecydował się przeprowadzić atak terrorystyczny podczas żydowskiego święta Jom Kippur 9 października 2019 roku. Próbował dostać się do synagogi, strzelając i używając materiałów wybuchowych domowej roboty. Kiedy nie mógł wyważyć drzwi, zaczął strzelać do przechodniów obok świątyni i zabił jedną kobietę. Inny przechodzący mężczyzna, który chciał pomóc rannej kobiecie, przeżył tylko dlatego, że broń ekstremisty się zacięła. Sfrustrowany niemożnością dostania się do synagogi, napastnik uciekł do Landsbergu – oddalonego o ok. 15 km od Halle – gdzie zabił jeszcze jedną osobę i ranił dwie. Terrorysta transmitował cały atak na żywo za pośrednictwem serwisu streamingowego Twitch, mając nadzieję, że zaprezentuje go szerokiej publiczności i zachęci innych myślących jak on do dokonywania podobnych czynów. Śledztwo policyjne wykazało, że napastnik był skrajnie prawicowym i antysemickim ekstremistą.

Ostatecznie, gdyby był lepiej przeszkolony, terrorysta mógł zabić ok. 50 osób. Rok później prokurator stwierdził, że napastnik miał przy sobie 8 sztuk broni palnej,

[142] 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: 28.10.2020.
[143] Fondation Pour L'Innovation Politique, *Les attentats islamistes dans le monde 1979-2019*, Paris 2019, s. 32.

kilka ładunków wybuchowych, hełm i kamizelkę. Terrorysta został oskarżony o 13 przestępstw, w tym zabójstwo, usiłowanie zabójstwa, uszkodzenie ciała i podżeganie do działań terrorystycznych.

Atak terrorystyczny w Halle jest szczególny ze względu na wykorzystanie technologii druku 3D, która umożliwia wykonanie broni domowej produkcji. Korzystając jedynie z bezpłatnych przewodników internetowych, dostępnych dla wszystkich, Stephan Balliet był w stanie wydrukować broń. Wydrukowane w 3D części broni użytej w ataku w Halle niekoniecznie były zaprojektowane do tego celu. Jednak wraz ze wzrostem jakości druku 3D i tym, jak coraz bardziej znana i dostępna staje się ta technika, skuteczność terrorystów produkujących broń prawdopodobnie wzrosną jeszcze bardziej. Może to być pierwszy krok w kierunku stworzenia wytrzymałej, drukowanej w 3D broni służącej do ataków terrorystycznych. Jeśli terroryści już wspierają produkcję swojej broni palnej komponentami 3D, to tylko kwestią czasu pozostaje, kiedy będą w stanie wykonać wytrzymałe pistolety, opierając się jedynie na technologii druku 3D.

Druk 3D w metalu to nowa technologia, która z czasem również stanie się bardziej powszechna. W 2013 roku firma z Teksasu wydrukowała metalową replikę pistoletu Colt M1911, który skutecznie wystrzelił 600 nabojów[144]. Również w Stanach Zjednoczonych sędzia federalny wydał firmie Defense Distributed zakaz projektowania planów do drukowania broni. Firma sprzedawała w sieci instrukcje drukowania części m.in. do AR-15.

Niemniej jednak, biorąc pod uwagę wzrost prawicowego terroryzmu, atak w Halle zostanie najprawdopodobniej zapamiętany jako historycznie istotny, ponieważ był pierwszym przypadkiem, kiedy terrorysta użył broni domowej produkcji, w tym komponentów wydrukowanych w 3D. Przypomina to działalność terrorystów Państwa

[144] C. Farivar, "Download this gun": 3D-printed semi-automatic fires over 600 rounds, https://arstechnica.com/tech-policy/2013/03/download-this-gun-3d-printed-semi-automatic-fires-over-600-rounds, dostęp: 1.12.2020.

Islamskiego w Europie Zachodniej, którzy sami wytwarzali broń, m.in. noże i materiały wybuchowe. Służbom bezpieczeństwa coraz trudniej jest też znaleźć sprawców, ze względu na brak nabywców przedmiotów zabronionych, które można by namierzyć – potencjalni nabywcy mogą samodzielnie „tworzyć" śmiercionośne przedmioty przy pomocy schematów w Internecie[145].

Powszechna dostępność druku 3D i prostota, z jaką można przesyłać pliki komputerowe, mogą finalnie wpłynąć na rozprzestrzenianie broni jądrowej, podobnie jak obecnie wpływają na broń konwencjonalną. Na przykład firma Raytheon drukuje komponenty broni kierowanej, która może służyć jako element systemu głowicy nuklearnej. To część technologii przyszłości, w której państwa wykorzystają druk 3D do rozwijania broni jądrowej[146].

Technologia może przynosić zarówno korzyści, jak i szkody. Druk 3D umożliwił już tworzenie różnego rodzaju przedmiotów, jak noże, pociski, pistolety, części składowe pojazdów wojskowych czy inne niebezpieczne przedmioty, które można wykorzystać przeciwko ludziom. Nie jest możliwe, żeby drukowanie 3D pozostało ograniczone tylko do określonych grup ludzi lub organizacji, jak to się dzieje w przypadku materiałów wybuchowych czy broni[147]. Głównym celem powinno być zapobieganie zdobywaniu broni przez terrorystów i przestępców bez ich wykrycia. Z tego powodu niezbędna jest weryfikacja osób kupujących materiały, z których można wydrukować broń. Co więcej, wyścig technologiczny jest procesem globalnym, w którym rządy, podobnie jak służby bezpieczeństwa, muszą się dostosować do bieżących wyzwań, w przeciwnym razie zostaną przytłoczone powszechnością i dostępnością takich drukarek.

---

[145] D. Koehler, *The Halle, Germany, Synagogue Attack and the Evolution of the Far-Right Terror Threat*, CTC Sentinerl, December 2019, Vol. 12, Issue 11, s. 18.
[146] A. Nelson, *The truth about 3-d printing and nuclear proliferation,* https://warontherocks.com/2015/12/the-truth-about-3-d-printing-and-nuclear-proliferation, dostęp: 10.11.2020.
[147] N. Shahrubudina, T.C. Leea, R. Ramlana, *An Overview on 3D Printing Technology: Technological, Materials, and Applications*, Procedia Manufacturing 35 (2019), s. 1287.

AUTONOMICZNE I PÓŁAUTONOMICZNE POJAZDY

Autonomiczny pojazd może być zdefiniowany jako „połączenie sprzętu i oprogramowania (zarówno zdalnego, jak i pokładowego), które realizuje funkcję prowadzenia pojazdu, z aktywnym monitorowaniem środowiska prowadzenia pojazdu przez człowieka lub bez niego"[148]. Autonomiczne pojazdy są przykładem SI, która nadal nie została w pełni wdrożona w życie codzienne ludzi. Technologia pojazdów autonomicznych była w ostatnich latach testowana, lecz w pełni samodzielne pojazdy nadal są postrzegane jako przyszłość transportu, choć prawdopodobnie nie jest to aż tak odległa perspektywa.

Powszechnie uważa się, że autonomiczne pojazdy przynoszą szereg korzyści, wśród których można wyróżnić pozytywny wpływ na środowisko naturalne poprzez zmniejszenie zużycia energii i tym samym zanieczyszczenia, zwiększenie mobilności osób niezdolnych do prowadzenia pojazdów (takich jak osoby niepełnosprawne, star-

[148] The U.S. Department of Transportation, 2016. *Federal Automated Vehicles Policy - Accelerating the Next Revolution in Roadway Safety*, [online] https://www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016, dostęp: 25.11.2020.

sze, niewidome lub zbyt młode, by prowadzić), co ostatecznie powinno zmniejszyć izolację społeczną, czy także zmniejszenie częstotliwości wypadków samochodowych[149]. Niemniej jednak, autonomiczne pojazdy, jak każdy inny przykład technologii SI, mają również swoje wady. Autonomiczne pojazdy mogą, oprócz rosnącego bezrobocia wśród kierowców autobusów, ciężarówek i taksówek, a także osób pracujących na stacjach paliw (aspekt wcześniej zasygnalizowany w tej publikacji), relatywnie zmniejszyć zyski wielu miast z parkingów i transportu publicznego, ostatecznie zmniejszając ich budżet[150].

Co więcej, możliwy jest scenariusz, w którym autonomiczne pojazdy mogą same stać się dla terrorystów bronią, a przynajmniej oferować nowe metody umożliwiające im przeprowadzanie ataków. Istotnie, w 2014 r. członkowie Strategic Issues Group, wchodząca w skład FBI Directorate of Intelligence, przewidzieli, że „autonomia [spowoduje, iż samochody] będą potencjalnie bardziej śmiertelną bronią, niż są obecnie"[151]. Jak wskazuje przykład uzbrajania bezzałogowych dronów, które stają się jednym z popularniejszych narzędzi stosowanych w asymetrycznych działaniach wojennych i mają wpływ na zmianę strategii organizacji terrorystycznych, również możliwość użycia autonomicznych pojazdów do przeprowadzenia ataku wymagają głębszej analizy. Zmiany przyjęte przez terrorystów w ich taktyce mogą mieć poważne skutki i nawet jeśli ryzyko, że użyją oni zaawansowanego technologicznie pojazdu do przeprowadzenia ataku wydaje się być obecnie raczej niskie, to w ciągu najbliższych lat może ono znacznie wzrosnąć. Dlatego też należy dokładnie zbadać możliwość używania przez terrorystów pojazdów w pełni autonomicznych lub półautonomicznych.

---

[149] Anderson J. M., et al., *Autonomous Vehicle Technology: A Guide for Policymakers,* Santa Monica, RAND, 2014.
[150] Anderson, J.M., et al., *Autonomous Vehicle Technology: A Guide for Policymakers* Santa Monica, RAND, 2014.
[151] BBC News, 2014. *FBI: Google's Driverless Cars Could Be Lethal Weapons*. [online] BBC News. https://www.bbc.com/news/technology-28344219, dostęp: 6.11.2020.

Pojazdy jako bomby samochodowe

Wykorzystanie pojazdów do przeprowadzania ataków bombowych przez terrorystów jest niezwykle szerokim tematem, często badanym przez analityków ds. terroryzmu i bezpieczeństwa. Jest to powszechna taktyka stosowana przez wiele organizacji terrorystycznych i powiązanych z nimi osób w ciągu ostatnich dziesięcioleci praktycznie na całym świecie. Przykładem może być podkładanie przez Irlandzką Republikańską Armię ładunków wybuchowych w pojazdach od lat 70. do 90. XX wieku, lub pierwszy atak na World Trade Center w 1993 roku. W ciągu ostatnich dwóch dekad pojazdy wypełnione materiałami wybuchowymi były jednak najczęściej detonowane na Bliskim Wschodzie, zwłaszcza w Iraku i Syrii. Wyjaśnienie Hugo Kaamana dotyczące użycia pojazdów przez terrorystów najlepiej opisuje ich wykorzystanie: „pojazd samochodowy może być albo zaparkowany, a następnie zdalnie zdetonowany, albo może być prowadzony przez zamachowca-samobójcę, który ostatecznie kontroluje mechanizm detonacji"[152].

Biorąc pod uwagę fakt, że terroryści często wykorzystywali nieautonomiczne samochody, argument, że rozszerzyliby swoją taktykę na w pełni lub częściowo autonomiczne pojazdy i używaliby ich jako systemów służących do dostarczania materiałów wybuchowych na miejsce zaplanowanego ataku, jest z pewnością zasadny. Według doniesień, członkowie organizacji terrorystycznych zaczęli już korzystać z automatyzacji, co ilustruje przykład ISIS opracowującego zdalnie sterowany samochód wypełniony ładunkami wybuchowymi[153]. W tym konkretnym przypadku terroryści umieścili nawet fałszywego kierowcę, swoistego manekina wypełnionego termostatami, aby uniknąć wykrycia przez skanery bezpieczeństwa.

[152] Kaaman, H., 2017. *The Evolution Of Suicide Car Bombs Examined*. [online] AOAV. <http://aoav.org.uk/2017/evolution-suicide-car-bombs/>, dostęp 18.11.2020.
[153] Ramsay, S., 2016. *Exclusive: Inside IS Terror Weapons Lab*. [online] Sky News. <https://news.sky.com/story/exclusive-inside-is-terror-weapons-lab-10333883>, dostęp: 11.11.2020.

Korzystanie z autonomicznych i półautonomicznych samochodów stanowiłoby ogromną korzyść dla terrorystów – nie musieliby oni prowadzić pojazdu, a następnie tracić życia w wyniku wybuchu, ponieważ samochód sam jechałby w wybrane miejsce lub był tam zdalnie prowadzony i zostałby zdetonowany z bezpiecznej dla terrorystów odległości. Szkody byłyby równie druzgocące, ale dodatkowo nie zmniejszyłyby się szeregi organizacji terrorystycznych, a niedoszli zamachowcy-samobójcy mogliby nadal realizować inne zadania. Nawet jeśli możliwości organizacji terrorystycznych w zakresie użycia pół- lub całkowicie autonomicznych pojazdów nie są w tej chwili doskonałe, nie można pominąć takiej możliwości w kontekście analizy przyszłych zagrożeń terrorystycznych.

Kierowanie pojazdów w stronę tłumów

Organizacje terrorystyczne również używają pojazdów do kierowania ich w tłumy i, używając ich jak tarana, przeprowadzania ataków w ten sposób. W 2010 r., w drugim wydaniu internetowego magazynu *Inspire* wydawanego przez Al-Kaidę na Półwyspie Arabskim (AQAP) materiału propagandowego, ukazał się artykuł zachęcający do używania ciężarówek jako broni do „zabijania wrogów Allaha"[154] w krajach, które wspierają „izraelską okupację Palestyny, amerykańską inwazję na Afganistan i Irak lub krajach, które odegrały znaczącą rolę w zniesławieniu Mahometa"[155]. W ostatnich latach miało miejsce wiele ataków z użyciem ciężarówek jako broni, czego tragicznym przykładem były ataki w Nicei we Francji i stolicy Niemiec, Berlinie – oba miały miejsce w 2016 roku. W pierwszym z wymienionych Tunezyjczyk o nazwisku Mohamed Lahouaiej Bouhlel celowo wjechał 20-tonową ciężarówką w tłum na Promenade des Anglais[156] zabijając 86 osób i raniąc wielu innych. Drugi również został popełniony przez

[154] CNN, 2010. *New Issue Of Magazine Offers Jihadists Terror Tips*. [online] Edition.cnn.com. <https://edition.cnn.com/2010/WORLD/meast/10/12/mideast.jihadi.magazine/index.html>, dostęp: 3.11.2020.
[155] CNN, 2010. *New Issue Of Magazine Offers Jihadists Terror Tips*. [online] Edition.cnn.com. <https://edition.cnn.com/2010/WORLD/meast/10/12/mideast.jihadi.magazine/index.html>, dostęp: 3.11.2020.
[156] Smith-Spark, L., 2016. *France Pays Tribute To Nice Attack Victims*. [online] CNN. <https://edition.cnn.com/2016/10/15/europe/france-nice-attack-memorial/index.html>, dostęp: 10.11.2020.

Tunezyjczyka, który wjechał ciężarówką na jarmark bożonarodzeniowy w Berlinie, zabijając 12 osób i raniąc ponad 50[157]. Wyżej wymienione to tylko dwa ze znacznie większej liczby zamachów tego rodzaju[158].

Odnosząc się do ataku w Nicei, John Carlin, zajmujący się w prokuraturze generalnej USA bezpieczeństwem narodowym kraju, powiedział: „jeśli próbują skłonić ludzi do wjechania ciężarówką w tłum, to nie trzeba mieć zbyt dużej wyobraźni, aby przewidzieć, że użyją [do tego celu] autonomicznego samochodu"[159]. Niestety, zdaje się on mieć rację. Jeśli terroryści uzyskają dostęp do autonomicznych lub półautonomicznych pojazdów, jest więcej niż pewne, że spróbują wykorzystać je w sposób, który służy ich walce. Pomimo głosów, że autonomiczne pojazdy są znacznie bezpieczniejsze i zaprogramowane tak, aby przestrzegać zasad i ograniczeń drogowych (ograniczenie prędkości, zachowanie stosownej odległości od innych pojazdów), co skutkuje m.in. zmniejszeniem liczby wypadków samochodowych, można oczekiwać, że terroryści będą ingerować w algorytmy pojazdów tak, aby złamać ich zaprogramowane instrukcje bezpieczeństwa, aby wjechać nimi na chodnik lub udać się w inne miejsca pełne ludzi, w celu wyrządzenia szkody jak największej liczbie z nich. Jest to ponury scenariusz, którego nie wolno lekceważyć biorąc pod uwagę szybkie dostosowywanie się terrorystów do nowo dostępnych technologii oraz ich niekończące się próby przechytrzania służb porządkowych i bezpieczeństwa poprzez stosowanie nowych metod przeprowadzania ataków.

[157] BBC News, 2016. *Berlin Lorry Attack: What We Know*. [online] BBC News. <https://www.bbc.com/news/world-europe-38377428>, dostęp: 15.11.2020.
[158] Więcej przykładów dostępne pod linkiem: https://edition.cnn.com/2017/05/03/world/terrorist-attacks-by-vehicle-fast-facts/index.html
[159] Industry Week, 2016. *Connected, Self-Driving Cars Pose Serious New Security Challenges*. [online] Industry Week. <https://www.industryweek.com/technology-and-iiot/emerging-technologies/article/22006985/connected-selfdriving-cars-pose-serious-new-security-challenges>, dostęp: 9.11.2020].

Przejmowanie pojazdów przy wykorzystaniu złośliwego oprogramowania

Jedną z metod pozwalających terrorystom na przejęcie kontroli nad autonomicznym lub półautonomicznym pojazdem, jest możliwość włamania się do oprogramowań odpowiadających za sterowani – innymi słowy, zhakowania go.

Rzeczywiście, w połowie 2017 r. jeden z ekspertów ds. informatycznych amerykańskiego think tanku RAND Corporation, Nidhi Kalra, powiedział podczas przesłuchania prowadzonego przez US Congress House Energy and Commerce Subcommittee on Digital Commerce and Consumer Protection, że hakowanie pojazdów – samo w sobie bardzo realne zagrożenie – stwarza szansę dla terrorystów[160]. Powołując się na publiczne ogłoszenie FBI, „luki mogą występować w funkcjach komunikacji bezprzewodowej pojazdu, w urządzeniu mobilnym – takim jak telefon komórkowy lub tablet podłączony do pojazdu przez USB, Bluetooth lub Wi-Fi – lub w urządzeniu zewnętrznym podłączonym przez port diagnostyczny pojazdu"[161].

Do tej pory przeprowadzono wiele „testów hakerskich", mających na celu udowodnienie, że nawet pojazdy nie w pełni autonomiczne, ale zaawansowane technologicznie, są podatne na ataki cybernetyczne. Przykładem może być eksperyment z włamaniem do samochodu przeprowadzony w 2015 roku, kiedy to hakerzy przejęli kontrolę nad systemem klimatyzacji, radiem, przednimi wycieraczkami, a także hamulcami i układem kierowniczym[162]. Podczas gdy przejęcie kontroli nad trzema pierwszymi elementami wyposażenia nie stanowi dużego zagrożenia dla kierowcy lub innych osób na drodze, przejęcie kontroli nad hamulcami i układem kierowniczym może stanowić zagrożenie dla życia.

---

[160] Jones, S., 2017. *'Autonomous Vehicles Provide An Avenue For Terrorism,' Congress Is Told*. [online] CNSNews.com. <https://www.cnsnews.com/news/article/susan-jones/autonomous-vehicles-provide-avenue-terrorism-congress-told>, dostęp: 15.11.2020.

[161] FBI Public Service Announcement, 2016. *Motor Vehicles Increasingly Vulnerable To Remote Exploits*. [online] Ic3.gov. <https://ic3.gov/Media/Y2016/PSA160317>, dostęp: 14.11.2020.

[162] Greenberg, A., 2015. *Hackers Remotely Kill A Jeep On The Highway—With Me In It*. [online] Wired. <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>, dostęp: 14.11.2020.

Chociaż wymagałoby to określonej wiedzy i szeregu kompetencji, nie można wykluczyć scenariusza, w którym członkowie organizacji terrorystycznej nabywają możliwość hakowania pojazdów częściowo lub całkowicie autonomicznych. Istnieje kilka możliwych scenariuszy, które można tu przytoczyć, ale udany cyberatak na pojazd umożliwiłby terrorystom na przykład przyspieszenie tego pojazdu i skierowanie go w stronę tłumu, albo zderzenie z innymi samochodami na drodze, przy czym oba te scenariusze mogłyby kosztować życie wielu ludzi. Jeszcze bardziej niepokojący jest scenariusz to ten, w którym terroryści przejmują kontrolę nad wieloma pojazdami w tym samym czasie, zyskując w ten sposób możliwość spowodowania wielu kolizji drogowych, ostatecznie doprowadzając do blokady dróg, a jednocześnie przeprowadzając atak przy użyciu bardziej tradycyjnych środków (tj. np. materiałów wybuchowych). Ze względu na zablokowane drogi, służby medyczne nie byłyby w stanie dotrzeć do rannych, co z kolei pogłębiłoby chaos i wywołałoby jeszcze większą panikę.

Niemniej jednak terroryści mogą dokonywać „cyberprzejęć" pojazdów również w innych celach, niż używając ich jako broni. Przykładowym scenariuszem jest włamanie się do komputera pojazdu, kradzież danych osobowych i groźba ich upublicznienia, przy czym byłyby to działania zrealizowane w celu otrzymania okupu potrzebnego do sfinansowania innych działań i planów.

DEEP FAKES

Termin „deep fake" jest używany w „odniesieniu do realistycznych zdjęć, audio, wideo i innych podróbek generowanych przy użyciu technologii sztucznej inteligencji"[163] i został po raz pierwszy użyty w 2017 roku. Najczęściej deep fake'i są tworzone 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 (zdjęcia, materiał wideo, nagrania audio), 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 prawdziwych od fałszywych.

.

[163] Harris, L., 2020. *Deep Fakes And National Security*. [online] Congressional Research Service. https://crsreports.congress.gov/product/pdf/IF/IF11333, dostęp: 2.11.2020.

Deep fake'i mają wiele pożytecznych zastosowań. Mogą one być wykorzystywane na przykład przez nauczycieli w procesie edukacji do prowadzenia „innowacyjnych lekcji, które są o wiele bardziej angażujące”[164] niż tradycyjne lekcje poprzez, na przykład, „przywrócenie do życia" postaci historycznych. W medycynie deep fake'i są przydatne do celów syntetyzowania „fałszywych obrazów medycznych w celu wyszkolenia algorytmów wykrywania chorób rzadkich"[165]. Zastosowanie znajdują też w dziedzinie kultury i rozrywki: jedno z muzeów na Florydzie stworzyło wystawę poświęconą Salvadorowi Dalí, w której przedstawiono „naturalnej wielkości rekonstrukcję Dalí za pomocą techniki montażu wideo wzbogaconego o uczenie maszynowe"[166].

Pomimo powyższych wskazań, deep fake'i mogą również stanowić szeroki zakres zagrożeń dla bezpieczeństwa krajowego i międzynarodowego. Autorzy badania przeprowadzonego w University College London w 2020 r. stwierdzili, że „fałszywe treści audio lub wideo zostały uznane przez ekspertów za najbardziej niepokojące wykorzystanie sztucznej inteligencji pod względem jej potencjalnych zastosowań w przestępczości lub terroryzmie [...]"[167].

Szkodiwe wykorzystanie deep fake'ów

Wykorzystywanie sztucznej inteligencji 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

[164] Jaiman, A., n.d. *Positive Use Cases Of Deepfakes*. [online] Toward Data Science. https://towardsdatascience.com/positive-use-cases-of-deepfakes-49f510056387, dostęp: 3.11.2020.
[165] Harris, L., 2020. *Deep Fakes And National Security*. [online] Congressional Research Service. https://crsreports.congress.gov/product/pdf/IF/IF11333, dostęp: 2.11.2020.
[166] Lee, D., 2019. *Deepfake Salvador Dalí Takes Selfies With Museum Visitors*. [online] The Verge. https://www.theverge.com/2019/5/10/18540953/salvador-dali-lives-deepfake-museum, dostęp: 4.11.2020.
[167] University College London, 2020. *'Deepfakes' Ranked As Most Serious AI Crime Threat*. [online] 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>

przekonujące podrobione treści"[168]. Chociaż z pewnością nie każdy byłby w stanie produkować deep fake'i o jakości wystarczającej, by oszukać innych, to jednak ich tworzenie nie wymaga od ludzi aż takiej 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 Nancy Pelosi, spikerkę amerykańskiej Izby Reprezentantów, jak gdyby była odurzona alkoholem[169]. Operacja taka może zostać podjęta w celu obniżenia zaufania zwykłych ludzi 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[170], co miałoby szkodliwe skutki dla ich krajów.

Również terroryści mogą używać deep fake'ów w celu wspierania swojej działalności i walki. Wśród możliwych scenariuszy istnieje ten, według którego członkowie organizacji terrorystycznej wykorzystują deep fake'i w celu podszycia się pod krewnych lub osoby nadzorujące czyjąś pracę, dążąc ostatecznie do wyłudzenia funduszy, które mogłyby zostać wykorzystane do finansowania ich działalności. Terroryści mogliby to zrobić replikując głos takich osób przy użyciu programu, który klonuje głosy (co cie-

[168] Harris, L., 2020. *Deep Fakes And National Security*. [online] Congressional Research Service. https://crsreports.congress.gov/product/pdf/IF/IF11333, dostęp: 2.11.2020.
[169] Zegart, A., 2019. *In The Deepfake Era, Counterterrorism Is Harder*. [online] The Atlantic. https://www.theatlantic.com/ideas/archive/2019/09/us-intelligence-needs-another-reinvention/597787/, dostęp: 17.11.2020.
[170] Harris, L., 2020. *Deep Fakes And National Security*. [online] Congressional Research Service. https://crsreports.congress.gov/product/pdf/IF/IF11333, dostęp: 2.11.2020.

kawe, taki program jest w stanie nie tylko „naśladować głos wejściowy, ale także zmienić go tak, aby odzwierciedlał inną płeć lub nawet inny akcent"[171]). W 2019 roku cyberprzestępcy zadziałali właśnie w opisany powyżej sposób: wykorzystali technologię SI do podszycia się pod szefa firmy i wyłudzili od jego pracownika przelew w wysokości 243 000 dolarów[172]. Opierając się na fakcie, że prosty ładunek wybuchowy, który miał zostać zdetonowany podczas mistrzostw świata w piłce nożnej w Niemczech w 2006 r., został stworzony z „zbiornika propanu, zegarka, baterii i plastikowej butli wypełnionej gazem"[173] 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 niezmierne duże.

Inną niebezpieczną alternatywą jest ta, w której terroryści generują realistycznie wyglądające treści (zdjęcia lub filmy), mające na celu zintensyfikowanie radykalizacji i rozszerzenia ich kampanii rekrutacyjnych. Takie fałszywe materiały mogłyby pokazywać na przykład amerykańskich, brytyjskich lub francuskich żołnierzy popełniających zbrodnie wojenne (tj. znęcanie się nad schwytanymi dżihadystami, 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 radykalizacji nowych przeciwników

[171] Future Work Institute, n.d. *Deepfake Video And Audio Recordings*. [online] Future Work Institute. https://futureworkinstitute.com/deepfake-video-and-audio-recordings/, dostęp: 7.11.2020.
[172] Stupp, C., 2019. *Fraudsters Used AI To Mimic CEO'S Voice In Unusual Cybercrime Case*. [online] WSJ. <https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402>, dostęp: 10.11.2020.
[173] Temple-Raston, D., 2014. *How Much Does A Terrorist Attack Cost? A Lot Less Than You'd Think*. [online] 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.

bądź wzmocnienia istniejących. Były wśród nich na przykład przypadki niewłaściwego traktowania więźniów poprzez poddawanie ich torturom lub przenoszenie ich z kraju do kraju bez ich zgody. Nawet 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 krajom zachodnim. Studium przypadku z wojny z terroryzmem wspierające tę hipotezę to skandal, do którego doszło w Abu Gharib – czyli w 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"[174]. Zdjęcia torturowanych podejrzanych zostały upublicznione w 2004 r., w następstwie czego „zakapturzony mężczyzna i pies gnębiący więźniów stały się ikonicznymi symbolami zachodniego wysiłku wojennego"[175], które z kolei zaczęły podsycać propagandę dżihadystów, przedstawiając torturowanych jako niesprawiedliwie skrzywdzonych przez zachodnich żołnierzy, ułatwiając tym samym wysiłki rekrutacyjne terrorystów. Dostępna obecnie technologia SI pozwoliłaby terrorystom nie tylko na tworzenie fałszywych zdjęć przedstawiających muzułmanów niewłaściwie traktowanych przez członków zachodnich sił zbrojnych, 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 (tzw. Samozwańczy terroryści – samotne wilki).

[174] Kennedy-Pipe, C. (2015). *IEDs, Martyrs, Civil Wars and Terrorists.* [w]: C. Kennedy-Pipe, G. Clubb and S. Mabon, ed., Terrorism and Political Violence. London: Sage, s.158.
[175] Kennedy-Pipe, C. (2015). *IEDs, Martyrs, Civil Wars and Terrorists.* [w]: C. Kennedy-Pipe, G. Clubb and S. Mabon, ed., Terrorism and Political Violence. London: Sage, s.158.

WYKORZYSTANIE PRZEZ TERRORYSTÓW NOWYCH TECHNOLOGII DO DEZINFORMACJI I PROPAGANDY

Bez cienia wątpliwości można powiedzieć, że organizacje terrorystyczne „kochają" wszelkie nowinki technologiczne – w szczególności te, które zapewniają im realizację jednego z ich głównych celów, jakim jest zyskanie rozgłosu. Zdobycie uwagi społeczności pozwala na osiągnięcie wyznaczonych przez organizację celów politycznych, ale również zastraszenie, pozyskanie nowych członków, czy wywieranie wpływu na stosunki międzynarodowe. W dalszym ciągu cele te realizowane są głównie za pomocą tych samych aktów – czyli masowego wywoływania strachu poprzez zastosowanie gróźb, a także coraz to bardziej wysublimowanych sposobów ataku.

Z pewnością można również stwierdzić, że bez adaptowania nowych zdobyczy technologicznych organizacje terrorystyczne wręcz nie mogłyby tego celu realizować. Chcąc, a raczej musząc, dostosować się do stale zmieniających się warunków komunikacyjnych czy trybu funkcjonowania mediów, terroryści dość swobodnie adoptują wszelkie nowości dostępne na rynku. Nie tylko tych, których zastosowanie nie da im „wypaść z obiegu" informacyjnego, ale również pozwoli na zwiększenie efektywności przy realizacji celów.

Jednym z podstawowych narzędzi, które dość szybko zostało zaadaptowane przez terrorystów była sieć internetowa oraz media społecznościowe. Przed erą mediów społecznościowych, organizacje terrorystyczne korzystały z dobrodziejstwa nadających całodobowo, ogólnokrajowych (lub międzynarodowych) stacji telewizyjnych. Co należy podkreślić, relację łączącą mass media oraz terrorystów nie można uznać za pasożytniczą, ale wręcz przeciwnie, za synergiczną – media otrzymywały szokujący materiał, który gwarantował im rekordy oglądalności, natomiast terroryści osiągali swój cel – docierali ze swoim przekazem do bardzo szerokiej publiczności, czyli zyskiwali, to, na czym najbardziej im zależy – rozgłos. Obopólnie korzystna relacja, posiadała jednak pewne ograniczenia – jak np. cenzurę krwawych nagrań, które zmniejszała oddziaływanie na poziom szoku i strachu (ale również poparcie u niektórych jednostek) – które zniknęły wraz z pojawieniem się mediów społecznościowych. Media masowe, w swoich relacjach, jednoznacznie prezentowały działania terrorystów w negatywnym świetle, jednak media społecznościowe dały również głos tej grupie użytkowników, która wyrażała poparcie dla tego typu działań. Co więcej, pojawiła się możliwość nadawania w czasie rzeczywistym i docierania do jeszcze większej publiczności nieograniczonej wiekiem.

Internet oraz media społecznościowe pozwoliły również na szeroką skalę realizacji dwóch rodzajów działań. Po pierwsze będzie to znaczne ułatwienie i przyspieszenie komunikacji we własnym gronie zwolenników, która umożliwia łatwiejszą koordynację działań pomiędzy poszczególnymi członkami grupy, niejednokrotnie rozsianymi na całym świecie. Drugim bardzo istotnym rodzajem komunikacji jest ta realizowana masowo – czyli docieranie do szerokiej publiki. Media społecznościowe oraz komunikatory zapewniły grupom ekstremistycznym nie tylko możliwość relacjonowania w czasie rzeczywistym zamachów, ale również prowadzenie długotrwałego oddziaływania w obszarze informacyjnym – czyli działań propagandowych. Patrząc na wymiar realizacji operacji w obszarze informacyjnym chociażby Państwa Islamskiego czy Hezbollahu,

możemy stwierdzić, że organizacje terrorystyczne prowadzą nie działania, a wręcz wojnę w cyberprzestrzeni. Koncentrują się przy tym nie tylko na aspektach zastraszania, ale również na pozyskiwaniu zwolenników, rekrutów gotowych przybyć na tereny kontrolowane, jak również podjąć działania w charakterze samotnych wilków.

Materiały propagandowe, przygotowywane i publikowane przez Państwo Islamskie również stanowią wyznacznik, w jaki sposób zdobycze technologiczne są wykorzystywane przez tę organizację. W zależności od poziomu jej rozwoju były one realizowane w mniej lub bardziej profesjonalny sposób. Co warto jednak podkreślić, wykorzystanie zaawansowanych środków realizacji nagrań pokazuje stopień, w jakim organizacja ta dostosowuje swoją medialną aktywność do wymagań odbiorców. Poprzez działania propagandowe organizacja realizowała przeróżne cele – począwszy od zastraszania, poprzez zachęcanie do wstąpienia w szeregi jej bojowników (w wypadku mężczyzn) oraz budowania społeczeństwa (w wypadku kobiet), aż po zachęcenie do podjęcia czynnych działań w miejscu zamieszkania – czyli do przeprowadzenia zamachów jako tzw. samotne wilki.

Pozyskiwanie zwolenników, jak i chętnych do militarnego i społecznego wsparcia organizacji, poprzez produkcję odpowiednio przygotowanych materiałów wideo czy prowadzenia bezpośredniej komunikacji z potencjalnymi rekrutami, przynosiło wymierne korzyści – przykłady zrekrutowanych kobiet i mężczyzn do wstąpienia w szeregi terrorystów, często bardzo nagłaśnianych poprzez media, można wręcz mnożyć[176]. W wypadku działań propagandowych sieć oraz media społecznościowe posłużyły do publikowania i przesyłania nie tylko filmów zachęcających do czynnego podjęcia działań, ale również materiałów instruktażowych – mających ułatwić planowanie ataku potencjalnemu bojownikowi. Do produkcji tego typu materiałów stosowano efekty graficzne jak animacje czy grafiki, a także wykorzystywano drony do realizacji ujęć z powietrza.

[176] Rekrutacja do Państwa Islamskiego odbywała się poprzez przeróżne czynniki, do których można zaliczyć m.in. oddziaływanie na chęci zdobycia stabilnego miejsca do życia, zbudowania życia rodzinnego opartego o wartości religijne, chęć zdobycia sławy czy walkę w imię Allaha.

Jak wskazują liczne doniesienia medialne, wykorzystane metody skutecznie pozwoliły na dotarcie do szerokiego grona osób. Jakość i forma przygotowania tego typu materiałów z pewnością sprzyjała lepszemu odbiorowi materiałów przez użytkowników sieci.

Kolejnym bardzo negatywnym przykładem zastosowania mediów społecznościowych przez terrorystów jest możliwość bezpośredniego promowania swoich działań w czasie rzeczywistym. Przykładem tak negatywnego wykorzystania mediów społecznościowych był zamach przeprowadzony w marcu 2019 roku w Christchurch w Nowej Zelandii, kiedy to prawicowy ekstremista przez niespełna 17 minut transmitował na żywo za pośrednictwem Facebooka przebieg ataku, w trakcie którego śmierć poniosło łącznie 51 osób. Atak ten wykazał bardzo niebezpieczne zastosowanie tej platformy. Pierwszy sygnał o szkodliwej zawartości serwis otrzymał dopiero po 29 minutach od jej rozpoczęcia, przez co, zanim została ona usunięta obejrzano ją 4 tysiące razy. O dużej popularności nagrania świadczy fakt, że przez pierwsze 24 godziny po zamachu próbowano je ponownie wgrać na platformę 1,5 mln razy (1,2 mln zostało zablokowane w momencie wgrywania)[177]. Pomimo że relacja została usunięta, jest ona wciąż ogólnodostępna w sieci za pośrednictwem innych serwisów.

Uwadze terrorystów nie umknął również gwałtowny rozwój kryptowalut, których przepływ jest znacznie trudniejszy do namierzenia niż w przypadku tradycyjnych środków finansowych. Na problem wykorzystania kryptowalut do pozyskiwania środków przez tego typu organizacje zwracał uwagę m.in. RAND Corporation, który wskazał na możliwości nie tylko pozyskiwania środków zewnętrznych od darczyńców na bieżące funkcjonowanie, ale również finansowania aktów terrorystycznych poprzez zakup niezbędnych materiałów[178]. Przykładem tego typu działań jest założona pod auspicjami

[177] Facebook statement "Update on New Zealand" https://about.fb.com/news/2019/03/update-on-new-zealand/, dostęp: 11.10.2020.
[178] C. Dion-Schwarz., D. Manheim, P. B. Johnston, *Terrorist Use of Cryptocurrencies. Technical and Organizational Barriers and Future Threats*, RAND Corporation 2019.

Hamasu organizacja „al-Nasr Brigades – Lawa al-Tawahid", której działania w obszarze pozyskiwania środków z wykorzystaniem technologii blockchain zostały zidentyfikowane w 2019 roku. Organizacja za pomocą Telegramu oraz Facebooka zachęcała do dokonywania darowizn w kryptowalutach na potrzeby jej działalności[179].

Dość szybko organizacje ekstremistyczne zdały sobie sprawę z możliwości wykorzystania sieci do prowadzenia działań ofensywnych. Zaskakującym przykładem działalności Hamasu w sieci było wykorzystanie mediów społecznościowych, aby za pomocą fikcyjnych profili wchodzić w interakcje z przedstawicielami izraelskiego wojska. Po zdobyciu zaufania wybranej ofiary, z fikcyjnego konta przesyłano link, za pomocą którego instalowano aplikację zawierającą złośliwe oprogramowanie, które umożliwiało przejmowanie urządzenia ofiary. Jak podkreślali przedstawiciele izraelskiego wojska, nie była to pierwsza sytuacja tego typu – wcześniej próbowano kontaktować się z żołnierzami np. za pomocą komunikatorów w celu pozyskania informacji o działaniach armii[180].

Platformy mediów społecznościowych, świadome swojej roli, jaką odgrywają w przekazywaniu dezinformacji i propagandy, podjęły liczne działania mające na celu wykrywania i usuwania szkodliwych treści. Pod koniec listopada 2019 roku, w ramach wspólnej pracy European Union Internet Referral Unit of Europol, Eurojust oraz platform internetowych udało się zamknąć znaczną liczbę stron i kont w mediach społecznościowych, wykorzystywanych do promocji działań Państwa Islamskiego[181]. O podobnym odkryciu opinia publiczna mogła się dowiedzieć we wrześniu 2020 roku, kiedy to

[179] Azani E., Barak M., Landau E., Liv N., *Identifying Money Transfers and Terror Finance Infrastructure*, International Institute for Counter-Terrorism, January 2020.
[180] A. Ahronheim, *IDF stops Hamas 'honeypots' from trapping soldiers*, https://www.jpost.com/israel-news/idf-foils-hamas-operation-targeting-soldiers-operation-rebound-617744, dostęp: 12.10.2019; A. Ahronheim, *Hamas using WhatsApp to collect intelligence on IDF movements,* https://www.jpost.com/israel-news/hamas-using-whatsapp-to-collect-intelligence-on-idf-movement-595701, access: 12.10.2019.
[181] A. Kozłowski, *Europol uderza w serwery ISIS. Cios w propagandę Państwa Islamskiego*, CyberDefence24.pl https://cyberdefence24.pl/europol-uderza-w-serwery-isis-cios-w-propagande-panstwa-islamskiego, dostęp: 11.10.2019.

brytyjski nadawca BBC poinformował, że Institute for Strategic Dialogue jeszcze w październiku 2019 roku wykrył gigantyczne repozytorium danych należących do ISIS. Pomimo że o znalezisku zostały poinformowane władze Wielkiej Brytanii i Stanów Zjednoczonych, repozytorium stale powiększało się na przestrzeni kolejnych miesięcy[182].

Internet oraz media społecznościowe powstały w górnolotnym celu – łączenia ze sobą ludzi. Dość szybko mogliśmy się jednak przekonać, że pomimo swoich niezliczonych zalet, stały się one również obszarem działań przestępców i terrorystów. Jak pokazują liczne przykłady, działalność w obszarze informacyjnym, poprzez oddziaływanie na opinię i nastroje społeczne, przekłada się także na działania w świecie „offline" przejawiające się, jako naruszenia bezpieczeństwa i porządku publicznego[183]. Pomimo licznych inicjatyw mających zwalczać szkodliwą działalność w sieci, warto wyraźnie podkreślić, że wdrażane rozwiązania wciąż pozostają o krok za działalnością, nie tylko organizacji terrorystycznych, ale również zwykłych przestępców.

[182] S. Silva, *Islamic State: Giant library of group's online propaganda discovered*, BBC https://www.bbc.com/news/technology-54011034, dostęp: 11.10.2019; Click reveals ISD discovery of huge pro-ISIS online cache, ISD https://www.isdglobal.org/isd-in-the-news/click-reveals-isd-discovery-of-huge-pro-isis-cache/, dostęp: 11.10.2019.

[183] Jednym z takich przykładów były zamieszki w 2020 roku w Stanach Zjednoczonych wywołane śmiercią George Floyda, które podsycane były poprzez szkodliwą działalność podmiotów zewnętrznych w mediach społecznościowych.

ANTYTERRORYZM W MEDIACH SPOŁECZNOŚCIOWYCH I SPOŁECZEŃSTWIE

Z uwagi na międzynarodowe zagrożenia terrorystyczne i rosnącą liczbą organizacji terrorystycznych istnieje potrzeba udoskonalania krajowych strategii w celu utrzymania wysokiego poziomu bezpieczeństwa. Każdy kraj wykorzystuje różne środki w celu ochrony własnych obywateli, ale jednym z najważniejszych elementów każdego systemu bezpieczeństwa jest technologia. Wysoko zaawansowane technologie stały się nieodłączną częścią działań na rzecz zapewnienia bezpieczeństwa własnego państwa i społeczeństwa. Na przykład, technologie rozpoznawania twarzy, które są zintegrowane z kamerami, zapewniają szybszą identyfikację sprawców, zwłaszcza jeśli znajdują się one na obszarach o dużej aktywności przestępczej lub też w przypadku ataku terrorystycznego. Ich instalacja w miejscach, gdzie na co dzień przebywa dużo ludzi, takich jak lotniska czy dworce kolejowe, już teraz pokazuje korzyści płynące z wykorzystania technologii w zapewnianiu bezpieczeństwa ludziom. Ulepszenie dzięki wykorzystaniu możliwości sztucznej inteligencji tylko poprawi ich skuteczność, między innymi dzięki szybszej identyfikacji, szybszemu sortowaniu danych i lepszej koordynacji między wieloma elementami sieci bezpieczeństwa.

Stopień, w jakim państwa są w stanie wdrożyć wysoko zaawansowane technologie w celu wzmocnienia swojego bezpieczeństwa zależy od dostępnych funduszy oraz procesu decyzyjnego. Potrzebny czas na rozwój, dostępność i finansowanie technologii SI również wpłyną na jej wdrożenie w sektorze bezpieczeństwa. Niemniej jednak, koordynacja między władzami lokalnymi i agencjami wywiadowczymi będzie także stanowić filar strategii bezpieczeństwa. Innym kluczowym filarem tych strategii jest inwigilacja, a sztuczna inteligencja może znacznie pomóc siłom bezpieczeństwa w zarządzaniu i gromadzeniu informacji na temat kluczowych zagrożeń, a także w śledzeniu podejrzanych osób oraz nadzorowaniu obszarów wysokiego zagrożenia. Niemniej jednak sztuczna inteligencja nie jest „magicznym rozwiązaniem" w radzeniu sobie z zagrożeniami dla bezpieczeństwa. Dlatego też odpowiedzialność za zapewnienie ludziom życia w bezpieczeństwie spoczywa także na samych obywatelach i na całym społeczeństwie.

Liczba ludzi, którzy posiadają konta w popularnych serwisach internetowych, rośnie każdego dnia. Z tego powodu konieczne jest wykorzystanie tej szansy i użycie globalnych usług komunikacji jako narzędzia do informowania ludzi o zagrożeniach bezpieczeństwa i, co może ważniejsze, do edukowania ich, jak rozpoznawać te zagrożenia i oraz zradykalizowane jednostki[184]. Obywatele mogą informować służby bezpieczeństwa za pomocą specjalnych formularzy na stronie internetowej oferowanej przez policję[185]. Ten rodzaj komunikacji znacznie zwiększa liczbę osób walczących z terroryzmem – od niewielkiej grupy wyszkolonych oficerów i funkcjonariuszy kontrterrorystycznych po zwykłych obywateli kraju, którzy mogą dzielić się swoimi opiniami i poglądami przez Internet, pod warunkiem, że ludzie nie będą nadużywać infolinii z po-

[184] The National News, *Convicted ISIS supporter carried out deadly terrorist attack in Vienna.* [online] Available at: https://www.thenationalnews.com/world/europe/convicted-isis-supporter-carried-out-deadly-terrorist-attack-in-vienna-1.1104434, dostęp: 16.11.2020.
[185] Polizei Wien, [online] Available at: https://twitter.com/LPDWien/status/1323364631734341633, dostęp: 16.11.2020.

wodu błędnych interpretacji lub innych pomyłek, co mogłoby prowadzić do nadwyrężenia zasobów władz. Nie można oczekiwać, że użycie broni przez oddziały kontrterrorystyczne pozwoli skutecznie i całkowicie zwalczać terroryzm. Bardziej kompleksowe podejście, które obejmuje zachęcanie obywateli do wspólnego działania we współpracy z władzami, pomoże zapewnić większe bezpieczeństwo społeczeństwa. Współpraca między cywilami a sektorem bezpieczeństwa może znacznie przyczynić się do zapobiegania wielu atakom terrorystycznym. Odnosi się to również do wykorzystywania mediów społecznościowych jako środka przyspieszającego wyśledzenie potencjalnych terrorystów, w przypadkach gdy byliby oni zgłaszani online, a władze szybko podejmowałyby działania, co znacznie skracałoby czas reakcji i umożliwiało podjęcie działań wyprzedzających.

9 grudnia 2020 roku Komisja Europejska przedstawiła komunikat prasowy, w którym zapowiada poprawę zdolności antyterrorystycznych UE. Głównym celem tego zobowiązania jest zwiększenie częstotliwości oraz jakości wymiany informacji wywiadowczych między państwami członkowskimi a Centrum Sytuacyjnym (EU INTCEN) w celu identyfikacji przyszłych zagrożeń w trakcie inwestowania w nowe technologie (np. sztuczną inteligencję), a także w celu przeciwdziałania radykalizacji postaw w internecie oraz w więzieniach poprzez programy edukacyjne i usuwanie treści terrorystycznych. Stwierdzono również, że nowe „Zobowiązanie UE do bezpieczeństwa i odporności miejskiej" będzie koncentrować się na zapewnieniu środków na zabezpieczenia gęsto zaludnionych obszarów oraz tych o charakterze symbolicznym, przy jednoczesnym oddzielnym wzmocnieniu mandatu Europolu i policyjnych programów wymiany informacji[186].

[186] European Commission, *Security Union: A Counter-Terrorism Agenda and stronger Europol to boost the EU's resilience*, Press release, 9 December 2020, Brussels.

KONKLUZJE

Współcześnie działalność terrorystyczna charakteryzuje się wieloma atakami przeprowadzanymi jednocześnie w różnych częściach świata. Nie jest to stała i powtarzalna taktyka, tylko raczej chaotyczne zamachy, które mają prowadzić do destabilizacji i niepokoju. Jeśli wziąć pod uwagę ostatnie ataki w Europie, to dokonano ich przy użyciu noży lub broni maszynowej, natomiast na Bliskim Wschodzie terroryści częściej wykorzystują materiały wybuchowe. W związku z powyższym warto zastanowić się, jak bardzo wymagające będzie przeciwdziałanie terrorystom, jeśli będą regularnie korzystać z zaawansowanego technologicznie oprogramowania i sprzętu, skoro tak trudno jest powstrzymać ich teraz, wiedząc jakich narzędzi użyją. Z czasem nowe systemy będą dostępne dla coraz większej liczby użytkowników, także dla członków organizacji terrorystycznych. Uzyskanie dronów zdalnie sterowanych przez sztuczną inteligencję lub zablokowanie systemów internetowych infrastruktury krytycznej państwa będzie tylko kolejnym etapem w ewolucji przeprowadzania zamachów. Już teraz wiele grup terrorystycznych korzysta z wysokorozwiniętej technologii, którą przejęły lub otrzymały.

Na podstawie przeprowadzonych analiz należy wskazać, że występuje coraz więcej wyzwań i zagrożeń w zmaganiach z terrorystami. Jest to efekt politycznego i społecznego zaangażowania grup terrorystycznych, które dodatkowo otrzymują wsparcie od niektórych państw lub instytucji. Powstaje zatem wielopłaszczyznowe zagrożenie, które często obejmuje zwalczanie nie samej organizacji terrorystycznej, ale całego państwa, ideologii lub religii. Największym niebezpieczeństwem nie jest współcześnie sam terroryzm – jako forma prowadzenia walki – ale cała hybryda zagrożeń pod postacią wielowymiarowych i niekonwencjonalnych działań realizowanych przez organizacje terrorystyczne przeciwko państwom.

W dobie wyścigu zbrojeń, USA, Chiny i Rosja zamierzają wykorzystywać sztuczną inteligencję nie tylko wewnętrznie w ramach postępu technologicznego państwa i wsparcia obywateli, ale także na rzecz rozwijania systemu uzbrojenia. Jeśli jedno państwo wzmacnia swój potencjał militarny, to automatycznie inni aktorzy na arenie międzynarodowej będą dążyć do ulepszenia swoich struktur bojowo-obronnych. Tym samym globalna rozgrywka ulega intensyfikacji. Jednak tym razem wdrażana jest sztuczna inteligencja, która bez wątpienia znacząco wpłynie na całokształt dotychczasowych relacji oraz sposobów wykorzystywania zdolności militarnych.

W związku z powyższym, trzeba z uwagą śledzić dalszy rozwój zaawansowanych systemów informatycznych oraz procesów mających na celu wykorzystanie sztucznej inteligencji do nadzorowania ataków podczas misji wojskowych. Scenariusz regularnego stosowania nowoczesnych broni niesie ze sobą dużo więcej konsekwencji. Wiele skoordynowanych ataków przeprowadzanych w różnych częściach państwa może prowadzić do jego całkowitego paraliżu. Dlatego też kluczowym elementem rozwijania każdego zaawansowanego systemu militarnego jest kwestia określenia, przeciw komu zostanie on wykorzystany oraz kto będzie mógł w przyszłości mieć do niego dostęp. W obecnej perspektywie rozważane są dwa scenariusze. Terroryści mogą zacząć dokonywać coraz większej liczby zamachów w odpowiedzi na użycie przeciw nim rozwiniętej technologii albo sami zaczną regularnie korzystać z zaawansowanych broni przeciw poszczególnym państwom i organizacjom.

Przedłożone opracowanie powinno przybliżyć problematykę współczesnych zagrożeń o charakterze technologiczno-terrorystycznym, a także zwrócić uwagę na kluczowe kwestie w procesie rozwijania sztucznej inteligencji przez światowe mocarstwa. Jednocześnie należy podkreślić, że dynamika środowiska bezpieczeństwa oraz szybki postęp technologiczny uniemożliwiają wzięcie pod uwagę wszystkich zmiennych, tak ważnych dla weryfikacji współczesnych zagrożeń.

REKOMENDACJE

1. Ze względu na międzynarodowe zagrożenia terrorystyczne i możliwość pozyskania przez terrorystów zaawansowanych technologii, konieczne jest rozpoczęcie globalnej debaty o przyszłych wyzwaniach dla bezpieczeństwa. Politycy, na czele z organizacjami międzynarodowymi takimi jak Unia Europejska, Organizacja Traktatu Północnoatlantyckiego, Organizacja Narodów Zjednoczonych, Liga Arabska czy Unia Afrykańska, powinni współpracować, aby zapobiegać szkodliwemu wykorzystywaniu nowych technologii przez podmioty niepaństwowe, a także kontrolować ich rozwój w sektorze wojskowym i cywilnym państw rozwijających SI.

2. Naukowcy muszą stale współpracować, aby na bieżąco weryfikować i wskazywać najbardziej podatne obszary, w których nowe technologie, zwłaszcza sztuczna inteligencja, mogą być szkodliwie wykorzystywane.

3. Inżynierowie, informatycy, fizycy i operatorzy wojskowi specjalizujący się w sztucznej inteligencji będą odpowiedzialni za rozwój nowych technologii dla swoich krajów i muszą mieć świadomość, że mogą stworzyć maszyny, które posłużą terrorystom do przeprowadzenia ataków. Zapewnianie restrykcyjnego i stopniowego wdrażania nowych technologii jest powszechną, globalną odpowiedzialnością.

4. Biorąc pod uwagę, że rywalizacja w rozwijaniu SI już się rozpoczęła, eksperci z różnych dziedzin powinni zintensyfikować dyskusje na temat jej wykorzystania. Niezbędnym jest niezwłoczne przedstawienie nowej, międzynarodowej polityki dotyczącej rozwoju sztucznej inteligencji, szczególnie dla państw, które już wdrażają lub chcą ją w przyszłości wykorzystywać.

5. Międzynarodowa debata powinna uwzględniać opinie sektora prywatnego, ponieważ widoczny jest wzrost zaangażowania inwestorów prywatnych. Wiele z niepaństwowych organizacji rozwija zaawansowane technologie i sztuczną inteligencję, dzięki czemu ich wiedza jest równie cenna. W związku z powyższym trzeba dążyć do zacieśnienia relacji na linii władze państwowe – prywatni inwestorzy, gdyż taka relacja będzie prowadzić do unikalnych oraz wartościowych rozwiązań i porozumień.

6. Rozwój i testowanie technologii muszą odbywać się w bezpiecznym środowisku. Eksperymenty z nową bronią (wyposażoną w SI) nie powinny być podejmowane podczas konfliktów zbrojnych lub walk przeciwko organizacjom terrorystycznym, jak to miało miejsce podczas wojny w Syrii. Wówczas niektóre mocarstwa testowały na polu bitwy swoją najnowszą broń, aby sprawdzić jej skuteczność.

7. Dane badawczo-rozwojowe nad najnowszymi technologiami muszą być chronione przy wykorzystaniu najlepszych zabezpieczeń w dziedzinie cyberbezpieczeństwa. Biorąc pod uwagę, że nie można przecenić znaczenia rozwoju takich technologii, wielu aktorów uciekałoby się do cyberataków, i nie tylko, aby je ukraść. Dane dotyczące rozwoju sztucznej inteligencji będą narażone na złośliwe oprogramowanie z zamiarem ich kradzieży i wykorzystania do własnych celów przez podmioty państwowe i niepaństwowe. W związku z tym, organizacje i państwa zaangażowane w rozwój nowych technologii muszą wzmocnić szkolenie personelu informatycznego, a także ulepszyć swoje oprogramowania, aby były odporne na włamania, uniemożliwiając hakerom uzyskanie łatwego dostępu do wrażliwych informacji. Sztuczna inteligencja może okazać się również potężnym narzędziem nie tylko w zakresie cyberbezpieczeństwa, ale też do przeprowadzania cyberataków.

8. Stopniowa integracja ze sztuczną inteligencją, korzystając z możliwości wykorzystania jej w codziennym życiu, ułatwi społeczeństwu zaakceptowanie tej technologii. Jednocześnie

edukacja stanowi główną rolę w uświadamianiu społeczności o zaletach i wadach użytkowania rozwiniętych technologii, takich jak np. drony[187].

9. Zrozumienie potęgi sztucznej inteligencji może prowadzić do formalnych uzgodnień między państwami co do sposobu jej wykorzystania, jak to ma miejsce w przypadku broni atomowej. Jednakże dotychczasowe militarne wykorzystanie sztucznej inteligencji ukazało wiele możliwości jej zastosowania na polu bitwy, co może prowadzić do priorytetyzowania egoistycznych interesów przez poszczególnych aktorów. Trzeba podkreślić, że jeszcze nie do końca określony potencjał sztucznej inteligencji może doprowadzić do wybuchu nowych konfliktów, jak również być elementem nowej zimnej wojny pomiędzy światowymi mocarstwami.

10. Militaryzacja SI prowadzi do tego, że supermocarstwa będą odmawiać sobie nawzajem bardziej liberalnego wykorzystania tej technologii. Ponadto jednym z wielu międzynarodowych wyzwań związanych z regulacją takich technologii jest to, że państwa mogą odmówić międzynarodowej współpracy z powodu własnych interesów, co będzie prowadzić do braku międzypaństwowych dyskusji na rzecz ustanowienia regulacji o wykorzystaniu sztucznej inteligencji. Niezbędna jest zatem jak najszybsza międzynarodowa regulacja procesów rozwoju technologii SI przez poszczególne państwa.

11. Należy opracowywać krótkoterminowe i długoterminowe strategie, mając na uwadze, że sztuczna inteligencja i inne zaawansowane technologie staną się częścią nowego międzynarodowego środowiska bezpieczeństwa. Ze względu na spodziewaną eskalację rywalizacji między głównymi mocarstwami skupionymi na wyścigu na rzecz rozwoju sztucznej inteligencji, obecnie, bardziej niż kiedykolwiek, ważne jest ustanowienie nowych zasad prawa międzynarodowego w oparciu o organizacje ponadpaństwowe. W przypadku złamania

[187] Unia Europejska 1 stycznia 2021 roku ujednolici przepisy dotyczące dronów na całym kontynencie. Nowe przepisy zastępują obowiązujące przepisy każdego państwa UE i mają zastosowanie do wszystkich cywilnych operatorów dronów. Pojawia się jednak kwestia wykorzystywania dronów na innych kontynentach, a także dronów wojskowych.

ustalonych regulacji przez któreś z państw lub podmiotów niepaństwowych, niezwłocznie wyciągnięte muszą zostać konsekwencje, łącznie z sankcjami, przez wszystkich innych sygnatariuszy. Ponadto zaleca się utworzenie międzynarodowej organizacji zajmującej się nadzorowaniem rozwoju sztucznej inteligencji, aby uniknąć wymknięcia się spod kontroli prowadzonych badań i testów.

12. Powszechne wykorzystanie bezzałogowych statków powietrznych na polu bitwy prowadzi do cyfryzacji dotychczasowych wojen. Ponadto UAVs można wykorzystać do transportu materiałów wybuchowych, broni, narkotyków czy niebezpiecznych chemikaliów. Dlatego też szczególną uwagę należy zwrócić na podwójne zastosowanie różnych zaawansowanych technologicznie narzędzi, które mogą służyć społeczeństwom, ale być również wykorzystane przez terrorystów. Trzeba wziąć pod uwagę, że sztuczna inteligencja będzie prowadzić do dalszej automatyzacji oraz rozpowszechnienia wykorzystania dronów, także tych, przy użyciu których można wyrządzić krzywdę.

13. Każdy zakup, nabycie lub użytkowanie dronów bojowych musi być rejestrowane w celu uzyskania informacji o użytkowniku danej maszyny. Jest to procedura podobna do tej służącej weryfikacji państw posiadających określoną liczbę systemów rakietowych lub osób fizycznych, które zakupiły broń. W związku z tym zarówno użytkownicy, jak i dostawcy muszą udostępnić swoje dane na rzecz rejestracji w systemach krajowych i międzynarodowych, aby móc korzystać z poszczególnych elementów uzbrojenia.

14. Należy się spodziewać, że druk 3D stanie się jednym z kluczowych zagrożeń dla bezpieczeństwa państw. Możliwość wykonania własnej broni w domu może prowadzić do częstszych starć między przestępcami/terrorystami i policją. Z tego powodu należy wzmocnić nowe przepisy dotyczące udostępniania w Internecie schematów broni, a także ich nielimitowanej sprzedaży. Służby bezpieczeństwa muszą skoncentrować się na monitorowaniu ludzi, którzy szukają projektów broni drukowanej w 3D lub dzielą się swoją wiedzą na temat tworzenia takich broni w mediach społecznościowych. Jedną z form regulowania

dystrybucji planów jest wydawanie certyfikatów zatwierdzonych przez władze państwowe, które pozwalają zaufanym firmom sprzedawać swoje plany osobom sprawdzonym. Dodatkowym pomysłem na rzecz ograniczenia zagrożenia jest utworzenie ogólnokrajowej bazy danych, która będzie zawierać dane o poszczególnych osobach, a także posłuży za element weryfikacji, jeśli zakupu spróbuje dokonać przestępca lub osoba nieuprawniona.

15. Międzynarodowa współpraca w walce z terroryzmem musi być kontynuowana. Jednak obecne wysiłki na Bliskim Wschodzie oraz Afryce powinny być realizowane nie tylko w celu utrzymania pokoju. Misjom organizowanym przez państwa koalicji NATO, UE i ONZ powinny towarzyszyć starania o odbudowę poszczególnych państw, wspierane przez społeczność międzynarodową, z zastrzeżeniem, iż władza musi należeć do rządów pokrzywdzonych państw. Oprócz tego, kraje, które decydują się na udział w międzynarodowych konfliktach, powinny wziąć pod uwagę moralny obowiązek wspierania wysiłków na rzecz odbudowy poszczególnych państw, ponieważ ich zaangażowanie wojskowe na obcym terytorium powoduje często eskalacje konfliktów w regionach już i tak rozdartych konfliktami, co było szczególnie widoczne w Iraku, Libii i Syrii. Poszczególne państwa po interwencji (militarnej/stabilizacyjnej) muszą opuścić kraje poszkodowane, aby nie zaostrzać konfliktu. Ponadto niestabilnym rządom powinno się oferować szkolenie sił zbrojnych oraz służb bezpieczeństwa w celu walki z terroryzmem.

16. Terroryzm jest bardzo często sponsorowany lub wspierany, w tym finansowo, przez różne państwa. Dlatego należy zwiększyć sankcje międzynarodowe na kraje, które jawnie lub niejawnie wspierają działalność terrorystyczną. Warto również rozważyć powołanie komitetów obserwacyjnych, które będą nadzorować eksport broni w regionach narażonych na konflikty, co powinno być jawnie prezentowane na posiedzeniach plenarnych organizacji międzynarodowych, jak np. ONZ.

17. Państwa, które zbyt długo utrzymują obecność wojskową w poszczególnych krajach, co prowadzi bardzo często do wykorzystania zasobów naturalnych „państw gospodarzy", powinny zostać ukarane międzynarodowymi sankcjami z tytułu ich szkodliwej działalności. Co ważne, jest to niejednokrotnie przyczyna i podstawa reakcji społeczności lokalnych, które bronią swoich zasobów, co często jest to postrzegane jako terroryzm. Dlatego taż należy przyjrzeć się współczesnym misjom wojskowym, gdyż takie działania prowadzą do zaostrzenia konfliktu.

18. Jest tylko kwestią czasu, kiedy zaawansowane technologie, takie jak roje dronów, będą powszechnie wykorzystywane przez siły zbrojne. Decydenci, a także społeczeństwo obywatelskie, mają zatem czas na opracowanie metod i narzędzi w celu uregulowania lub zwalczania ich nieuchronnego wykorzystania. Wielu badaczy zbyt mocno koncentruje się na przyszłych możliwościach, a nie na obecnych zagrożeniach. Ważne jest, aby znaleźć równowagę i zdefiniować krótko- i długoterminowe cele. Już wcześniej udowodniono dużą zdolność do adaptacji przez organizacje terrorystyczne i dlatego konieczne jest zapobieganie i przeciwdziałanie ich wysiłkom, które na pewno będą obejmować pozyskanie zaawansowanej broni.

19. Odnosząc się do reagowania na obecne i przyszłe zagrożenia, społeczność międzynarodowa musi dążyć do ustanowienia nowego status quo, poprzez ustalenie globalnych standardów obejmujących rozwój i wdrażanie sztucznej inteligencji, w ten sposób minimalizując nieuregulowane i bezprawne wykorzystanie zaawansowanej technologii. Utrzymanie światowego balansu umożliwi opracowanie kompleksowej strategii mającej na celu zabezpieczenie wykorzystania zaawansowanych technologii w przyszłości. Będzie to jednocześnie szansa do doskonalenia systemów krajowych oraz międzynarodowych, a także pozwoli na właściwe przygotowania względem pojawiających się wyzwań w związku z globalnym wyścigiem technologicznym.

BIBLIOGRAFIA

1. Abdulla, R. A., *Islam, Jihad, and Terrorism in Post-9/11 Arabic Discussion Boards,* „Journal of Computer-Mediated Communication", 12(3), article 15, s. 1-16.
2. Agence France-Presse, 2020. *At least 110 dead in Nigeria after suspected Boko Haram attack.* [online] Available at: <https://www.theguardian.com/world/2020/nov/29/nigeria-attack-boko-haram-farm-workers-killed>
3. Al Jazeera, 2018. *US hits Iran IRGC with sanctions over support of Yemen's Houthis,* [online] Available at: <https://www.aljazeera.com/news/2018/05/23/us-hits-iran-irgc-with-sanctions-over-support-of-yemens-houthis> [Accessed 12.11.2020].
4. Allen, G. and Chan, T., 2017. *Artificial Intelligence And National Security*. [online] Belfer Center for Science and International Affairs, s.1. Available at: <https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf> [Accessed 8 October 2020].
5. Almaliki A. J., *The Processes and Technologies of 3D Printing*, International Journal of Advances in Computer Science and Technology, Volume 4 No.10, October 2015, ss. 161-162.
6. Anderson J. M., et al., *Autonomous Vehicle Technology: A Guide for Policymakers,* Santa Monica, RAND, 2014.
7. Armed Forces Journal, 2009. *The War of New Words: Why Military History Trumps Buzzwords*, Armed Forces Journal, [online] Available at: <http://www.armedforcesjournal.com/essay-the-war-of-new-words> [Accessed 24.10.2020].
8. Azani, E., *The Hybrid Terrorist Organization: Hezbollah as a Case Study*, in Studies in Conflict & Terrorism, 36:11, 2013, ss. 899-916.
9. Bachmann, S., *Hybrid Threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats: mapping the new frontier of global risk and security management*, Amicus Curiae 2011 (88), ss. 24-25.
10. Bachmann, S., *Hybrid wars: the 21st-century's new threats to global peace and security*, Scientia Militaria, South African Journal of Military Studies, Vol 43, No. 1, 2015, s. 82.

11. Bajoria, J., *Lashkar-e-Taiba (Army of the Pure) (aka Lashkar e-Tayyiba, Lashkar e-Toiba; Lashkar-i-Taiba)*, Council on Foreign Relations, New York 2010.
12. Banerjee, I. and Sheenan, M., 2020. *America'S Got AI Talent: US' Big Lead In AI Research Is Built On Importing Researchers*. [online] macropolo.org. Available at: <https://macropolo.org/americas-got-ai-talent-us-big-lead-in-ai-research-is-built-on-importing-researchers/?rp=e> [Accessed 25 October 2020].
13. BBC News, 2014. *FBI: Google's Driverless Cars Could Be Lethal Weapons*. [online] BBC News. Available at: <https://www.bbc.com/news/technology-28344219> [Accessed 6 November 2020].
14. BBC News, 2016. *Berlin Lorry Attack: What We Know*. [online] BBC News. Available at: <https://www.bbc.com/news/world-europe-38377428> [Accessed 15 November 2020].
15. BBC, 2017. *Anti-drone protest at RAF Waddington,* [online] Available at: <https://www.bbc.com/news/uk-england-lincolnshire-41536818> [Accessed 20.10.2020].
16. Bird, E., Fox-Skelly, J., Jenner, N., Larbey, R., Weitkamp, E. and Winfield, A. *The Ethics Of Artificial Intelligence: Issues And Initiatives*. Brussels 2020.
17. Borkowski, R., *Terroryzm ponowoczesny*, Wydawnictwo Adam Marszałek, Toruń 2006, s. 40.
18. Brockmann, K., Kelley, R., *The Challenge of Emerging technologies to non-Proliferation Efforts controlling Additive Manufacturing and intangible Transfers of Technology,* Solna 2018, s. 36.
19. Builtin.com. n.d. *What Is Artificial Intelligence? How Does AI Work?*. [online] Available at: <https://builtin.com/artificial-intelligence> [Accessed 1 November 2020].
20. Bukowski, S., *Terroryzm europejski*, Słupsk 2010, s. 21.
21. Bunker, R., 2016. *Daesh/IS Armored Vehicle Borne Improvised Explosive Devices (AVBIEDs): Insurgent Use and Terrorism Potentials,* Claremont Colleges, [online] Available at: <https://core.ac.uk/download/pdf/148362649.pdf> [Accessed 7 November 2020].

22. Савчук, Т., 2020. *Пентагон занепокоєний використанням Росією штучного інтелекту у військовій сфері. Ось чому* [online] Available at: <https://www.radiosvoboda.org/a/pentagon-zanepokoyenyy-vykorystannyam-rosiyeyu-shtuxhnogo-intelektu-u-viyskoviy-sferi/30841807.html
23. Cafarella, J., *Jabat al-Nusra in Syria: An Islamic Emirate for Al-Qaeda,* Middle East Security Report 25, 2014.
24. Center for Data Innovation, 2019. *Who Is Winning The AI Race: China, The EU Or The United States?.* [online] Who Is Winning the AI Race: China, the EU or the United States?. Available at: https://s3.amazonaws.com/www2.datainnovation.org/2019-china-eu-us-ai.pdf [Accessed 2 October 2020].
25. Center on Sanctions & Illicit Finance, *'Al-Qaeda's Branch in Syria: Financial Assessment*, Foundation For Defense of Democracies, Washington 2017.
26. Cesarz, Z. Stadmulller, E., *Problemy polityczne współczesnego świata*, Wrocław 2002, s. 351.
27. CNN, 2010. *New Issue Of Magazine Offers Jihadists Terror Tips*. [online] Edition.cnn.com. Available at: <https://edition.cnn.com/2010/WORLD/meast/10/12/mideast.jihadi.magazine/index.html> [Accessed 3 November 2020].
28. CNN, 2010. *New Issue Of Magazine Offers Jihadists Terror Tips*. [online] Edition.cnn.com. Available at: <https://edition.cnn.com/2010/WORLD/meast/10/12/mideast.jihadi.magazine/index.html> [Accessed 3 November 2020].
29. Congressional Research Service, *Artificial Intelligence And National Security*, CRS, Washington 2020.
30. Congressional Research Service, *Hamas: Background and Issues for Congress*, CRS, Washington 2010.
31. Congressional Research Service, *The Islamic State and U.S. Policy,* CRS, Washington, 2018.
32. Council on Foreign Relations, *Palestinian Islamic Jihad.* [online] Available at: <https://www.cfr.org/backgrounder/palestinian-islamic-jihad> [Accessed 2 November 2020]

33. Counter Extremism Project, *Kata'ib Hezbollah,* [online] Available at: <https://www.counterextremism.com/threat/kata%E2%80%99ib-hezbollah> [Accessed 2 November 2020].
34. Counter Extremist Project, *Taliban.* [online] Available at: <https://www.counterextremism.com/threat/taliban> [Accessed 2 November 2020].
35. Daalder, M., 2019. *German attack raises questions about 3D printed guns,* [online] Available at: <https://www.newsroom.co.nz/germany-shooting-raises-questions-about-3d-printed-guns> [Accessed 26.10.2020].
36. Daily Military Defense, *Hypervelocity weapons systems are tested in support of the Advanced Battle Management System*. [online] Available at: <https://www.youtube.com/watch?v=XgwZmkT8VX0&feature=emb_logo> [Accessed 16.09.2020].
37. Daley, S., 2020. *32 Examples Of AI In Healthcare That Will Make You Feel Better About The Future*. [online] Built In. Available at: <https://builtin.com/artificial-intelligence/artificial-intelligence-healthcare> [Accessed 22 October 2020].
38. Defense Advanced Research Projects Agency, 2018. *ACTUV "Sea Hunter" Prototype Transitions to Office of Naval Research for Further Development.* [online] Available at: <https://www.darpa.mil/news-events/2018-01-30a> [Accessed 18 October 2020].
39. Dengg, A., Schurian, M. N., *On the Concept of Hybrid Threats*, s. 26, [in:] Networked Insecurity – Hybrid Threats in the 21st Century, Vienna 2016.
40. Dignum, V., 2018. *Ethics in artificial intelligence: introduction to the special issue*. Ethics and Information Technology, 20, ss. 1-3.
41. Directive (Eu) 2017/541 of the European Parliament and of the Council of 15 March 2017 *on combating terrorism* and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, 31.3.2017.
42. Dziubek T., *Obronność państwa a zagrożenia asymetryczne*, [in:] *Nowe zagrożenia bezpieczeństwa. Wyzwania XXI wieku*, (red.) K. Hennig, Wyższa Szkoła Humanistyczno-Ekonomiczna, Kraków 2015, s. 17.
43. European Commission, n.d. 2020. *Germany AI Strategy Report*. [online] European Commission. Available at: <https://knowledge4policy.ec.europa.eu/ai-watch/germany-ai-strategy-report_en> [Accessed 13 November 2020].

44. European Parliament, *The Financing of the 'Islamic State' in Iraq and Syria (ISIS),* European Parliament's Committee on Foreign Affairs, Belgium 2017.

45. Facebook statement "Update on New Zealand", [online] Available at: <https://about.fb.com/news/2019/03/update-on-new-zealand/> [Accessed 11.10.2020].

46. Farivar, C., 2013. *"Download this gun": 3D-printed semi-automatic fires over 600 rounds,* [online] Available at: <https://arstechnica.com/tech-policy/2013/03/download-this-gun-3d-printed-semi-automatic-fires-over-600-rounds> [Accessed 1.12.2020].

47. FATF, *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)*, Paris 2015.

48. FBI Public Service Announcement, 2016. *Motor Vehicles Increasingly Vulnerable To Remote Exploits*. [online] Ic3.gov. Available at: <https://ic3.gov/Media/Y2016/PSA160317> [Accessed 14 November 2020].

49. Fiott, D., Parkes, R., *Protecting Europe. The EU's response to hybrid threats*, European Union Institute for Security Studies, Paris 2019, s. 5.

50. Fondation Pour L'Innovation Politique, *Les attentats islamistes dans le monde 1979-2019*, Paris 2019, s. 32.

51. Foreign Policy Research Institute, 2013. *The Three Versions of Al Qaeda: A Primer*. [online] Available at: <https://www.fpri.org/article/2013/12/the-three-versions-of-al-qaeda-a-primer/> [Accessed 19.11.2020].

52. Foundation for Defense of Democracies, *Kataib Hezbollah: Background and Analysis*, 2018.

53. Freier, N. P., *Known Unknowns: Unconventional "Strategic Shocks",* Defense Strategy Development, Carlisle Barracks, PA: U.S. Army War College Strategic Studies Institute, 2008.

54. Future Work Institute, n.d. *Deepfake Video And Audio Recordings*. [online] Future Work Institute. Available at: <https://futureworkinstitute.com/deepfake-video-and-audio-recordings/> [Accessed 7 November 2020].

55. Gergin, N., Duru, H., Çetin, H. C., *Profile and Life Span of the PKK Guerillas*, Studies in Conflict & Terrorism, 38:3, 2015, ss.219-232.

56. Gibbons-Neff, T., 2016. *ISIS used an armed drone to kill two Kurdish fighters and wound French troops, report says,* [online] Available at: <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> [Accessed 21.09.2020].

57. Global Conflict Tracker, 2020. *Boko Haram in Nigeria.* [online] Available at: <https://www.cfr.org/global-conflict-tracker/conflict/boko-haram-nigeria> [Accessed 1.12.2020].

58. Greenberg, A., 2015. *Hackers Remotely Kill A Jeep On The Highway—With Me In It*. [online] Wired. Available at: <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/> [Accessed 14 November 2020].

59. Greenhouse, S., 2016. *Op-Ed: Autonomous Vehicles Could Cost America 5 Million Jobs. What Should We Do About It?*. [online] Los Angeles Times. Available at: <https://www.latimes.com/opinion/op-ed/la-oe-greenhouse-driverless-job-loss-20160922-snap-story.html> [Accessed 12 October 2020].

60. Gruszczak A., *Hybrydowść współczesnych wojen – analiza krytyczna*, [w:] *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, (red.) W. Sokała, B. Zapała, Biuro Bezpieczeństwa Narodowego, Warszawa 2011, s. 11.

61. H. Liu, L. Van Rompaey, M. Maas, *Beyond Killer Robots: Networked Artificial Intelligence Systems Disrupting the Battlefield?,* Journal of international humanitarian legal studies 10 (2019), s. 77-88.

62. Harris, L., 2020. *Deep Fakes And National Security*. [online] Congressional Research Service. Available at: <https://crsreports.congress.gov/product/pdf/IF/IF11333> [Accessed 2 November 2020].

63. Hoorickx, E., *Countering "Hybrid Threats": Belgium and the Euro-Atlantic Strategy,* Security & Strategy No 131 October 2017, ss. 6-7.

64. Industry Week, 2016. *Connected, Self-Driving Cars Pose Serious New Security Challenges*. [online] Industry Week. Available at: <https://www.industryweek.com/technology-and-iiot/emerging-technologies/article/22006985/connected-selfdriving-cars-pose-serious-new-security-challenges> [Accessed 9 November 2020].

65. Institute for Economics &Peace, *Global Terrorism Index 2015 – Measuring and understanding the impact of terrorism,* Sydney 2015.
66. Institute for Economics &Peace, *Global Terrorism Index 2017 - Measuring the impact of terrorism,* Sydney 2017.
67. Institute for Economics &Peace, *Global Terrorism Index 2020 - Measuring the impact of terrorism,* Sydney 2020.
68. Iulian R. I., *International terrorism in the 21st century – 16 years after 9/11 2001*, CBU International conference on innovations in science and education March 22-24, Prague 2017, Czech Republic.
69. IZ., 2019, *Путин сравнил преимущества искусственного интеллекта и ядерного оружия.* [online] Available at: <https://iz.ru/928464/2019-10-03/putin-sravnil-preimushchestva-iskusstvennogo-intellekta-i-iadernogo-oruzhiia> [Accessed 12.11.2020].
70. Jaiman, A., n.d. *Positive Use Cases Of Deepfakes*. [online] Toward Data Science. Available at: <https://towardsdatascience.com/positive-use-cases-of-deepfakes-49f510056387> [Accessed 3 November 2020].
71. Jasper S., Moreland, S., *ISIS: An Adaptive Hybrid Threat in Transition,* Small Wars Journal, October 2016, s. 2.
72. Johnson, K., 2019. *Defense Innovation Board unveils AI ethics principles for the Pentagon,* [online] Available at: <https://venturebeat.com/2019/10/31/defense-innovation-board-unveils-ai-ethics-principles-for-the-pentagon> [Accessed 17 September 2020].
73. Jones, S., 2017. *'Autonomous Vehicles Provide An Avenue For Terrorism,' Congress Is Told*. [online] CNSNews.com. Available at: <https://www.cnsnews.com/news/article/susan-jones/autonomous-vehicles-provide-avenue-terrorism-congress-told> [Accessed 15 November 2020].
74. Jongman, A. J., Schmid, A. P., *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature*, Transaction Publishers, New Brunswick 1988.
75. Kaaman, H., 2017. *The Evolution Of Suicide Car Bombs Examined*. [online] AOAV. Available at: <http://aoav.org.uk/2017/evolution-suicide-car-bombs/> [Accessed 18 November 2020].

76. Kaâniche, M., (ed.), *Applying Resilience to Hybrid Threats,* IEEE Security and Privacy Magazine 17(5), September 2019, s. 78.

77. Kennedy-Pipe, C. (2015). *IEDs, Martyrs, Civil Wars and Terrorists.* [in]: C. Kennedy-Pipe, G. Clubb and S. Mabon, ed., Terrorism and Political Violence. London: Sage, s.158.

78. Kerdemelidis, M., Reid, M., *Wellbeing recovery after mass shootings: information for the response to the Christchurch mosque attacks 2019*, „Canterbury District Health Board", 28.05.2019, ss. 2–5.

79. Koehler, D., *The Halle, Germany, Synagogue Attack and the Evolution of the Far-Right Terror Threat*, CTC Sentinerl, December 2019, Vol. 12, Issue 11, s. 18.

80. Koh, D., 2019. *Ping An Good Doctor Launches Commercial Operation Of One-Minute Clinics In China.* [online] Available at: <https://www.mobihealthnews.com/news/asia-pacific/ping-good-doctor-launches-commercial-operation-one-minute-clinics-china> [Accessed 8 October 2020].

81. Коновалова, Н. 2019. *Беспилотная «Ласточка». На железнодорожном салоне в Щербинке показали уникальную технологию.* [online] Available at: <https://spbvedomosti.ru/news/financy/bespilotnaya-lastochka-na-zheleznodorozhnom-salone-v-shcherbinke-pokazali-unikalnuyu-tekhnologiyu/> [Accessed 20.10.2020].

82. Kozłowski, A., *Europol uderza w serwery ISIS. Cios w propagandę Państwa Islamskiego*. [online] Available at: <https://cyberdefence24.pl/europol-uderza-w-serwery-isis-cios-w-propagande-panstwa-islamskiego> [Accessed11.10.2019].

83. Kubaczyk T., *Wojna hybrydowa – (czy) nowy typ konfliktu zbrojnego we współczesnym świecie*, [w:] *Konflikt hybrydowy na Ukrainie. Aspekty teoretyczne i praktyczne*, (red.) B. Pacek, J. A. Grochocka, Piotrków Trybunalski 2017, s. 24.

84. Kudzko, A., 2018. *Future Now: How AI Is Already Changing The Global And Military Landscape - GLOBSEC*. [online] GLOBSEC. Available at: <https://www.globsec.org/2018/02/06/future-now-ai-already-changing-global-military-landscape/> [Accessed 8 November 2020].

85. Kumar, N., 2019. *Saudi Arabia Drone Attack: Sign of Changing Character of Hybrid War,* [online] Available at: <https://www.vifindia.org/article/2019/october/01/saudi-arabia-drone-attack-sign-of-changing-character-of-hybrid-war> [Accessed 22.09.2020].

86. Lasconjarias, G., Larsen J. A., *(ed.), NATO's Response to Hybrid Threats,* Rome 2015, s. 101.

87. Law., R. D., *Terrorism: A History*, Cambridge 2009, ss. 155–157.

88. Lee, D., 2019. *Deepfake Salvador Dalí Takes Selfies With Museum Visitors*. [online] The Verge. Available at: <https://www.theverge.com/2019/5/10/18540953/salvador-dali-lives-deepfake-museum> [Accessed 4 November 2020].

89. Lopez, C., 2020. *Where It Counts, U.S. Leads In Artificial Intelligence.* [online] defense.gov. Available at: <https://www.defense.gov/Explore/News/Article/article/2269200/where-it-counts-us-leads-in-artificial-intelligence/> [Accessed 25 October 2020].

90. M. Hoenig, *Hezbollah and the Use of Drones as a Weapon of Terrorism.* [online] Available at: <https://fas.org/pir-pubs/hezbollah-use-drones-weapon-terrorism> [Accessed 14.10.2020].

91. Maas J., *Hybrid Threat and CSDP*, ss. 125-130, [in:] J. Rehrl (Ed.), Handbook on CSDP - The Common Security and Defence Policy of the European Union, Vienna 2019.

92. Malakoutikhah, Z., *Iran: Sponsoring or Combating Terrorism?,* Studies in Conflict & Terrorism, 43, (2020), ss. 913-939.

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

94. McKinsey & Company, 2017. *Artificial Intelligence And Southeast Asia's Future*. [online] s. 4. Available at: <https://www.mckinsey.com/~/media/mckinsey/featured%20insights/artificial%20intelligence/ai%20and%20se%20asia%20future/artificial-intelligence-and-southeast-asias-future.ashx> [Accessed 22 October 2020].

95. McLeary, P., 2018. *Pentagon'S Big AI Program, Maven, Already Hunts Data In Middle East, Africa*. [online] Available at: <https://breakingdefense.com/2018/05/pentagons-big-ai-program-maven-already-hunts-data-in-middle-east-africa/> [Accessed 11 November 2020].

96. Middle East Institute, *Hezbollah's Evolution: From Lebanese Militia to Regional Player*, Washington 2017.
97. Mitchell, J., 2017. *BIDMC Researchers Use Artificial Intelligence To Identify Bacteria Quickly And Accurately*. [online] Bidmc.org. Available at: <https://www.bidmc.org/about-bidmc/news/bidmc-researchers-use-artificial-intelligence-to-identify-bacteria-quickly-and-accurately> [Accessed 4 November 2020].
98. Mkhemer, S., *3D Printing Technology,* Birzeit University, December 2014, ss. 3-5.
99. Министерство цифрового развития связи и массовых коммуникаций Российской Федерации, 2020. *Цифровая экономика РФ*. [online] Available at: <https://digital.gov.ru/ru/activity/directions/858> [Accessed 25 November 2020].
100. Morton, M., 2018. *Inside The Chilling World Of Artificially Intelligent Drones,* [online] Available at: <https://www.theamericanconservative.com/articles/inside-the-chilling-proliferation-of-artificially-intelligent-drones> [Accessed 20.09.2020].
101. Moy, G., Shekh, S., Oxenham, M. and Ellis-Steinborner, S., 2020. *Recent Advances In Artificial Intelligence And Their Impact On Defence*. [online] Available at: <https://www.dst.defence.gov.au/sites/default/files/publications/documents/DST-Group-TR-3716_0.pdf> [Accessed 16 October 2020].
102. N. Guibert, 2016. *Irak : Paris confirme qu'un drone piégé a blessé deux membres des forces spéciales françaises à Erbil,* [online] Available at: <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> [Accessed 21.09.2020].
103. NATO Energy Security Centre of Excellence, *Hybrid Threats: Overcoming Ambiguity, Building Resilience,* No 11 2017, s. 6.
104. Nelson, A., 2015. *<The truth about 3-d printing and nuclear proliferation>* [online] Available at: <https://warontherocks.com/2015/12/the-truth-about-3-d-printing-and-nuclear-proliferation> [Accessed 10.11.2020].
105. Palestinian public opinion and terrorism: A two-way street?, *Journal of Policing, Intelligence and Counter Terrorism,* 10, (2015), ss. 71-87.
106. Parachini, J. V., Wilson, s. A., 2020. *Drone-Era Warfare Shows the Operational Limits of Air Defense Systems,* [online] Available at:

<https://www.rand.org/blog/2020/07/drone-era-warfare-shows-the-operational-limits-of-air.html> [Accessed 21.09.2020].

107. Piazza, J. A., Guler, A., *The Online Caliphate: Internet Usage and ISIS Support in the Arab World*, Terrorism and Political Violence, May 2019.
Cohen-Almagor, R., *Jihad Online: How Do Terrorists Use the Internet?,* Advances in Intelligent Systems and Computing, Hull 2017.
Salama, B., *The Resilience of the Islamic State,* Institut für Friedenssicherung und Konflikt management, Vienna 2016.

108. Polizei Wien, [online] Available at: <https://twitter.com/LPDWien/status/1323364631734341633> [Accessed 16.11.2020].

109. Pope, C., 2020. *Advanced Battle Management System field test brings Joint Force together across all domains during second onramp.* [online] Available at: <https://www.af.mil/News/Article-Display/Article/2336618/advanced-battle-management-system-field-test-brings-joint-force-together-across> [Accessed 16.09.2020].

110. Ramsay, S., 2016. *Exclusive: Inside IS Terror Weapons Lab*. [online] Sky News. Available at: <https://news.sky.com/story/exclusive-inside-is-terror-weapons-lab-10333883> [Accessed 11 November 2020].

111. Raugh, D., *Is the Hybrid Threat a True Threat?,* Journal of Strategic Security 9(2), June 2016, ss. 1-13.

112. RBC. *Путин назвал срок спуска на воду подлодки с ядерным «Посейдоном»*. [online] Available at: <https://www.rbc.ru/politics/20/02/2019/5c6d2c779a7947c9343f1028> [Accessed 13.11.2020].

113. Renstrom, J., 2018. *The UK Wants To Be The World Leader In Ethical AI*. [online] Slate. Available at: <https://slate.com/technology/2018/08/the-u-k-wants-to-be-the-world-leader-in-ethical-a-i.html> [Accessed 6 November 2020].

114. Rogoway, T., 2017. *ISIS Drone Dropping Bomblet On Abrams Tank Is A Sign Of What's To Come,* [online] Available at: <https://www.thedrive.com/the-war-zone/7155/isis-drone-dropping-bomblet-on-abrams-tank-is-a-sign-of-whats-to-come> [Accessed 21.09.2020].

115. Rotman, D., 2013. *How Technology Is Destroying Jobs*. [online] MIT Technology Review. Available at: <https://www.technologyreview.com/2013/06/12/178008/how-technology-is-destroying-jobs/> [Accessed 24 October 2020].

116. Saker, R., 2020. *The Impact Of Artificial Intelligence In Retail*. [online] My Total Retail. Available at: <https://www.mytotalretail.com/article/the-impact-of-artificial-intelligence-in-retail/> [Accessed 25 October 2020].

117. Sayler, K., 2020. *Artificial Intelligence And National Security*. [online] Available at: <https://fas.org/sgp/crs/natsec/R45178.pdf> [Accessed 11 November 2020].

118. Semple, M., Rhetoric, *Ideology and Organizational Structure of the Taliban Movement,* United States Institute of Peace, Washington 2014.

119. Shahrubudina, N., Leea, T.C. Ramlana, R., *An Overview on 3D Printing Technology: Technological, Materials, and Applications*, Procedia Manufacturing 35 (2019), s. 1287.

120. Shu, C., 2019. *Leaked Chinese Government Documents Detail How Tech Is Used To Escalate The Persecution Of Uighurs.* [online] Available at: < https://techcrunch.com/2019/11/24/leaked-chinese-government-documents-detail-how-tech-is-used-to-escalate-the-persecution-of-uighurs/> [Accessed 7 October 2020].

121. Sikorski, C., Schmuck, D., Matthes, Binder, J. A., *"Muslims are not Terrorists": Islamic State Coverage, Journalistic Differentiation Between Terrorism and Islam, Fear Reactions, and Attitudes Toward Muslims,* „Mass Communication and Society", 2017, vol. 20, Issue 6: „Media, Terrorism and Society", ss. 825–848.

122. Silva S., *Islamic State: Giant library of group's online propaganda discovered.* [online] Available at: <https://www.bbc.com/news/technology-54011034> [Accessed 11.10.2019];
ISD, *Click reveals ISD discovery of huge pro-ISIS online cache.* [online] Available at: <https://www.isdglobal.org/isd-in-the-news/click-reveals-isd-discovery-of-huge-pro-isis-cache/> [Accessed 11.10.2019].

123. Smith-Spark, L., 2016. *France Pays Tribute To Nice Attack Victims*. [online] CNN. Available at: <https://edition.cnn.com/2016/10/15/europe/france-nice-attack-memorial/index.html> [Accessed 10 November 2020].

124. Srivastava, S., 2020. *State Of Artificial Intelligence In US: Becoming Technology Superpower*. [online] Analytics Insight. Available at: <https://www.analyticsinsight.net/state-of-artificial-intelligence-in-us-becoming-technology-superpower/> [Accessed 25 October 2020].

125. Stanford University, *Mapping Militant Organizations.* [online] Available at: <https://web.stanford.edu/group/mappingmilitants/cgi-bin/pages/definitions> [Accessed 2 November 2020].

126. Stupp, C., 2019. *Fraudsters Used AI To Mimic CEO'S Voice In Unusual Cybercrime Case*. [online] WSJ. Available at: <https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402> [Accessed 10 November 2020].

127. Sukhankin, S., 2019. *Russia Adopts National Strategy for Development of Artificial Intelligence*. Eurasia Daily Monitor 16(163). [online] Available at: <https://jamestown.org/program/russia-adopts-national-strategy-for-development-of-artificial-intelligence/> [Accessed 18 October 2020].

128. *Summary Of The 2018 National Defense Strategy Of The United States Of America*. 2018. s.3.

129. Syed, A., Elias, P., Amit, B., Susmita, B., Lisa, O., Charitidis, C., *Additive manufacturing: scientific and technological challenges, market uptake and opportunities,* Materials today 2017, Vol. 1, ss. 1-16.

130. Taillat, S., *Un mode de guerre hybride dissymétrique ? Le cyberespace*, Stratégique, No 111, Paris 2016, ss. 89, 95.

131. Taken from the Department of Défense's Chief Information Officer website. Available at: <https://dodcio.defense.gov/About-DoD-CIO/Organization/JAIC/> [Accessed 22 October 2020].

132. Tankel, S., *Laskar-e-Taiba: From 9/11 to Mumbai,* ICSR, London 2009 s. 5.

133. Techjury.Net, 2019. *Infographic: How AI Is Being Deployed Across Industries*. [online] Robotics Business Review. Available at: <https://www.roboticsbusinessreview.com/ai/infographic-how-ai-is-being-deployed-across-industries/> [Accessed 28 October 2020].

134. Temple-Raston, D., 2014. *How Much Does A Terrorist Attack Cost? A Lot Less Than You'd Think*. [online] NPR. Available at: <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> [Accessed 5 November 2020].

135. Tenenbaum, E. *La manœuvre hybride dans l'art opératif, Stratégique*, No 111, Paris 2016, s. 56.

136. The Declaration is available at: <https://www.state.gov/declaration-of-the-united-states-of-america-and-the-united-kingdom-of-great-britain-and-northern-ireland-on-cooperation-in-artificial-intelligence-research-and-development-a-shared-vision-for-driving/> [Accessed 20 October 2020].

137. The National News, *Convicted ISIS supporter carried out deadly terrorist attack in Vienna.* [online] Available at: <https://www.thenationalnews.com/world/europe/convicted-isis-supporter-carried-out-deadly-terrorist-attack-in-vienna-1.1104434> [Accessed 16.11.2020].

138. *The Next Revolution in Roadway Safety,* [online] Available at: <https://www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016> [Accessed 25.11.2020].

139. The U.S. Department of Transportation, 2016. Federal Automated Vehicles Policy – Accelerating the Next Revolution in Roadway Safety, [online] Available at: <https://www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016> [Accessed 25.11.2020].

140. The Verge, 2017. Putin Says The Nation That Leads In AI 'Will Be The Ruler Of The World'. [online] Available at: <https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world> [Accessed 5 October 2020].

141. The Wall Street Journal, 2015. *5 Things to Know About the Houthis of Yemen*. [online] Available at: <https://www.wsj.com/articles/BL-263B-3613> [Accessed 11.11.2020].

142. The White House Office of Science and Technology Policy, 2020. *American Artificial Intelligence Initiative: Year One Annual Reports*. s. iii.

143. Tim. S., 2020. *"Is al-Qaeda's leader dead? Report claims terror chief Ayman al-Zawahiri has died in Afghanistan from 'asthma-related breathing issues"*, [online]

Available at: <https://www.dailymail.co.uk/news/article-8970231/Al-Qaedas-leader-Ayman-al-Zawahiri-died-reports-claim.html> [Accessed 20.11.2020].

144. U.S. Dept of Defense, 2020. *DOD Adopts Ethical Principles for Artificial Intelligence,* [online] Available at: <https://www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/> [Accessed 12.10.2020].

145. United Against Nuclear Iran, *Kata'ib Hezbollah*, [online] Available at: <https://www.unitedagainstnuclearіran.com/report/kataib-hezbollah> [Accessed 2 November 2020].

146. United Nations Office on Drugs and Crime, *Education for justice university module series counter-terrorism – Module 1 introduction to international terrorism*, UN, Vienna 2018, s. 1.

147. United Nations, General Assembly, *Agenda Item 108 – Question of Palestine (Resumed from the 2268th meeting),* Wednesday, 13 November 1974, at 10.30 a.m. New York, A/PV.2282 and Corr.1.

148. University College London, 2020. *'Deepfakes' Ranked As Most Serious AI Crime Threat*. [online] Available at: <https://www.ucl.ac.uk/news/2020/aug/deepfakes-ranked-most-serious-ai-crime-threat> [Accessed 4 November 2020].

149. University of California, 2016. *Big Data, Analytics & Artificial Intelligence. The Future Of Health Care Is Here*. [online] San Francisco. Available at: <https://www.gehealthcare.com/static/pulse/uploads/2016/12/GE-Healthcare-White-Paper_FINAL.pdf> [Accessed 9 November 2020].

150. Uslu, E., *Turkey's Kurdish Problem: Steps Toward a Solution,* Studies in Conflict & Terrorism, 30:2, 2007, ss. 157-172.

151. Van der Veer, R., 2020. *Terrorism in the age of technology*, [online] Available at: <https://www.clingendael.org/pub/2019/strategic-monitor-2019-2020/terrorism-in-the-age-of-technology> [Accessed 18 September 2020].

152. Ware, J., 2019. *Terrorist groups, artificial intelligence, and killer drones,* [online] Available at: <https://warontherocks.com/2019/09/terrorist-groups-artificial-intelligence-and-killer-drones> [Accessed 21.09.2020].

153. Webster, G., Creemers, R., Triolo, P. and Kania, E., 2017. All Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017). [online] Available at: <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/> [Accessed 1 October 2020].

154. Wiegand, K. E., *Reformation of a Terrorist Group: Hezbollah as a Lebanese Political Party*, Studies in Conflict & Terrorism, 32 (2009), ss. 669-680.

155. Zabłocki, E., *Kategorie, zagrożenia: system bezpieczeństwa narodowego,* Warszawa 2013, ss. 51–52.

156. Zegart, A., 2019. *In The Deepfake Era, Counterterrorism Is Harder*. [online] The Atlantic. Available at: <https://www.theatlantic.com/ideas/archive/2019/09/us-intelligence-needs-another-reinvention/597787/> [Accessed 17 November 2020].

157. Ze-Xian, L., Yen, T., Ray, M., Mattia, M., Metcalfe, I. Patterson, D., *Perspective on 3D printing of separation membranes and comparison to related unconventional fabrication techniques*, Journal of Membrane Science 2016, Vol 523, No.1, ss. 596-613.

AUTORZY

Aleksander Ksawery Olech

Dyrektor Programu Bezpieczeństwa Europejskiego w Instytucie Nowej Europy. Specjalista z zakresu bezpieczeństwa i relacji międzynarodowych. Doktorant nauk o bezpieczeństwie na Akademii Sztuki Wojennej. Doświadczenie badawcze zdobywał m.in. na Université Jean Moulin III w Lyonie, Instytucie Stosunków Międzynarodowych w Pradze oraz Instytucie Wspierania Pokoju i Zarządzania Konfliktami w Wiedniu. Stypendysta OSCE & UNODA Peace and Security oraz Fundacji im. Kazimierza Pułaskiego. Jego główne zainteresowania badawcze to terroryzm, międzynarodowa współpraca na rzecz bezpieczeństwa w Europie Wschodniej oraz rola NATO i UE w środowisku zagrożeń hybrydowych.

Alan Lis

Dyrektor ds. Analiz i Koordynacji Projektów w Instytucie Nowej Europy. Absolwent dwóch brytyjskich uczelni: Uniwersytetu w Yorku (studia licencjackie) i Uniwersytetu w Warwick (studia magisterskie). W ramach wymiany studenckiej spędził rok na Uniwersytecie w Bergen w Norwegii. Doświadczenie zawodowe zdobył m.in. w Departamencie Studiów Strategicznych KPRM i redakcji Euractiv.pl. Zainteresowania badawcze koncentruje na kwestiach bezpieczeństwa międzynarodowego, terroryzmu i zagrożeń hybrydowych.

Program Rozwoju Organizacji Obywatelskich na lata 2018–2030 PROO

NIW

Sfinansowano przez Narodowy Instytut Wolności – Centrum Rozwoju Społeczeństwa Obywatelskiego ze środków Programu Rozwoju Organizacji Obywatelskich na lata 2018-2030.

INSTYTUT NOWEJ EUROPY

FUNDACJA INSTYTUT NOWEJ EUROPY (INE)

Organizacja pozarządowa prowadząca działalność analityczną i badawczą w obszarze gospodarki, polityki i systemu prawnego w kontekście krajowym oraz międzynarodowym. Nasza działalność ma na celu merytoryczne wspieranie procesów podejmowania strategicznych dla państwa decyzji poprzez przygotowywanie propozycji rozwiązań w formie postulatów do realizacji, a także konkretnych rozwiązań legislacyjnych i uczestniczenie w procesie wcielania ich w życie.

JEŻELI DOCENIASZ NASZĄ PRACĘ,
DOŁĄCZ DO GRONA NASZYCH DARCZYŃCÓW!

Z otrzymanych funduszy sfinansujemy powstanie kolejnych publikacji. Bezpośrednia wpłata na konto Instytutu Nowej Europy:

Tytułem: „darowizna na cele statutowe”

95 2530 0008 2090 1053 7214 0001

www.ine.org.pl kontakt@ine.org.pl