BezpieczenstwoNarodowe.pl

1/2025

Adres redakcji:

ABO sp. z o.o.
ul. Chałubińskiego 9/2
02-004 Warszawa
e-mail: redakcja@bezpieczenstwonarodowe.pl

Wydano w wersji cyfrowej.

Spis treści

Contents

Słowo wstępne

Oddajemy w ręce Czytelników pierwszy numer kwartalnika naukowego *BezpieczenstwoNarodowe.pl* – czasopisma, które powstało jako odpowiedź na rosnącą potrzebę pogłębionej, interdyscyplinarnej i rzetelnej debaty nad bezpieczeństwem we współczesnym, dynamicznie zmieniającym się środowisku międzynarodowym. Inauguracyjne wydanie stanowi nie tylko symboliczny początek nowego projektu wydawniczego, lecz także wyraz ambicji stworzenia trwałej platformy wymiany myśli pomiędzy środowiskiem akademickim, ekspertami praktykami oraz decydentami odpowiedzialnymi za kształtowanie polityki bezpieczeństwa państwa.

Bezpieczeństwo narodowe – rozumiane dziś znacznie szerzej niż wyłącznie w kategoriach militarnych – obejmuje złożoną sieć wzajemnie powiązanych wymiarów: polityczny, militarny, ekonomiczny, energetyczny, infrastrukturalny, informacyjny i cybernetyczny. Współczesne zagrożenia coraz częściej mają charakter hybrydowy, wielodomenowy i transgraniczny, co wymaga odejścia od uproszczonych analiz na rzecz podejścia systemowego, uwzględniającego zarówno poziom krajowy, jak i międzynarodowy. Czasopismo *BezpieczenstwoNarodowe.pl* powstaje z przekonania, że tylko taka perspektywa pozwala właściwie diagnozować wyzwania oraz formułować adekwatne rekomendacje dla praktyki bezpieczeństwa.

Szczególne znaczenie dla powołania niniejszego kwartalnika miały doświadczenia ostatnich lat, zwłaszcza wojna rosyjsko-ukraińska, która w sposób jednoznaczny unaoczniła skalę zagrożeń dla państw Europy Środkowo-Wschodniej, w tym Polski. Konflikt ten potwierdził, że bezpieczeństwo infrastruktury krytycznej, odporność energetyczna, cyberbezpieczeństwo oraz zdolność do reagowania na zagrożenia informacyjne stały się kluczowymi elementami bezpieczeństwa narodowego i sojuszniczego. Państwa wschodniej flanki NATO funkcjonują dziś w warunkach permanentnej presji strategicznej, co wymaga nie tylko wzmocnienia zdolności obronnych, lecz także pogłębionej refleksji naukowej.

Pierwszy numer *BezpieczenstwoNarodowe.pl* odzwierciedla te wyzwania zarówno tematycznie, jak i metodologicznie. Znalazły się w nim artykuły poświęcone ochronie infrastruktury krytycznej w kontekście planowanej rozbudowy energetyki jądrowej w Polsce, nowoczesnym metodom szkolenia strzeleckiego dla szkół mundurowych z wykorzystaniem

technologii immersyjnych oraz cyberbezpieczeństwu wschodniej flanki NATO w obliczu wojny rosyjsko-ukraińskiej. Dobór tematów nie jest przypadkowy – pokazuje bowiem, że bezpieczeństwo narodowe należy analizować jednocześnie w wymiarze strategicznym, operacyjnym i technologicznym.

Pragniemy podkreślić, że czasopismo ma charakter otwarty na różnorodność podejść badawczych i szkół teoretycznych. Zależy nam na publikowaniu tekstów opartych na solidnych podstawach metodologicznych, ale jednocześnie zachowujących wrażliwość na praktyczne implikacje prowadzonych analiz. *BezpieczenstwoNarodowe.pl* aspiruje do roli forum, na którym spotykają się nauka i praktyka – gdzie wyniki badań naukowych mogą inspirować realne działania w obszarze bezpieczeństwa.

Nie byłoby możliwe przygotowanie tego numeru bez zaangażowania Autorów, Recenzentów oraz Rady Naukowej kwartalnika, której przewodniczy dr hab. Witold Mazurek. Ich wkład merytoryczny, doświadczenie i otwartość na dialog stanowią fundament jakości naukowej pisma. Wyrazy podziękowania kieruję również do zespołu redakcyjnego, w szczególności Sekretarza Redakcji, za profesjonalizm i determinację w realizacji tego projektu.

Oddając do Państwa rąk pierwsze wydanie kwartalnika, mamy świadomość odpowiedzialności, jaka wiąże się z tworzeniem nowego czasopisma naukowego. Traktujemy je jako długofalowe przedsięwzięcie, którego celem jest systematyczne budowanie dorobku naukowego oraz wzmacnianie kultury strategicznego myślenia o bezpieczeństwie narodowym.

Na zakończenie, w imieniu Redakcji *BezpieczenstwoNarodowe.pl*, pragnę złożyć Czytelnikom, Autorom i Współpracownikom serdeczne życzenia spokojnych, refleksyjnych Świąt Bożego Narodzenia oraz pomyślności, zdrowia i sukcesów naukowych w nadchodzącym Nowym Roku. Niech będzie to czas sprzyjający pogłębionej refleksji, twórczej pracy i odpowiedzialnemu myśleniu o bezpieczeństwie państwa i wspólnocie międzynarodowej.

Mirosław Podgórski

Redaktor Naczelny

BezpieczenstwoNarodowe.pl

Witold Mazurek
Uniwersytet Ignatianum w Krakowie
https://orcid.org/0000-0002-9440-7324

Wyzwania i problemy stojące przed systemem ochrony infrastruktury krytycznej w kontekście planowanej rozbudowy sektora energetyki jądrowej w Polsce

Streszczenie

Infrastruktura krytyczna stanowi fundament funkcjonowania współczesnych państw, a jej odporność przesądza o stabilności politycznej, gospodarczej i społecznej. Szczególne miejsce wśród sektorów infrastruktury krytycznej zajmuje energetyka, w tym planowane w Polsce elektrownie jądrowe. Celem artykułu jest identyfikacja kluczowych wyzwań w ochronie infrastruktury krytycznej w Polsce z perspektywy budowy elektrowni jądrowych oraz ocena adekwatności obecnych rozwiązań systemowych. W pierwszej części przedstawiono ewolucję pojęcia infrastruktury krytycznej oraz jej miejsce w krajowych i unijnych regulacjach prawnych. Następnie przeanalizowano główne kategorie zagrożeń – naturalne, technologiczne, terrorystyczne, cybernetyczne i hybrydowe – ze szczególnym uwzględnieniem ich wpływu na sektor energetyczny. W dalszej części omówiono specyfikę bezpieczeństwa obiektów jądrowych oraz zaprezentowano postulaty w zakresie wzmocnienia systemu ochrony, w tym powołania wyspecjalizowanej służby odpowiedzialnej za ochronę infrastruktury krytycznej. Artykuł kończą rekomendacje dotyczące budowy zintegrowanego modelu bezpieczeństwa elektrowni jądrowych w Polsce.

Słowa kluczowe: infrastruktura krytyczna, bezpieczeństwo jądrowe, elektrownia jądrowa, cyberbezpieczeństwo, zagrożenia hybrydowe

New challenges in critical infrastructure protection: the perspective of planned nuclear power plants in Poland

Abstract

Critical infrastructure constitutes the backbone of modern states, and its resilience determines political, economic and social stability. The energy sector, including planned nuclear power plants in Poland, has a special place among critical infrastructure sectors. The aim of the article is to identify key challenges in critical infrastructure protection in Poland from the perspective of the construction of nuclear power plants and to assess the adequacy of the current systemic solutions. The first part presents the evolution of the concept of critical infrastructure and its place in national and EU legal regulations. The paper then analyses the main categories of threats – natural, technological, terrorist, cyber and hybrid – with particular emphasis on their impact on the energy sector. The next part discusses the specific nature of nuclear facilities' security and presents proposals for strengthening the protection system, including the establishment of a specialised service responsible for critical infrastructure protection. The article concludes with recommendations for building an integrated model of nuclear power plants' security in Poland.

Keywords: critical infrastructure, nuclear security, nuclear power plant, cybersecurity, hybrid threats

Wprowadzenie

Infrastruktura krytyczna jest jednym z centralnych pojęć współczesnych studiów nad bezpieczeństwem narodowym. Obejmuje ona systemy, obiekty i usługi, których zakłócenie lub zniszczenie prowadziłoby do poważnych konsekwencji dla funkcjonowania państwa i jakości życia obywateli[1]. W warunkach narastającej złożoności środowiska bezpieczeństwa – na które składają się zmiany klimatyczne, postępująca cyfryzacja, rywalizacja mocarstw i rozwój zagrożeń hybrydowych – ochrona infrastruktury krytycznej staje się jednym z kluczowych zadań państwa.

Szczególne znaczenie ma sektor energetyczny, zapewniający funkcjonowanie wszystkich pozostałych sektorów infrastruktury krytycznej. W tym kontekście elektrownie jądrowe są postrzegane jako obiekty o strategicznej wadze: z jednej strony oferują stabilne i niskoemisyjne źródło energii, z drugiej – koncentrują w sobie ryzyka o potencjalnie katastrofalnych konsekwencjach[2]. Dla Polski, która znajduje się na etapie przygotowań do budowy pierwszych bloków jądrowych, zagadnienie bezpieczeństwa tych obiektów ma wymiar nie tylko techniczny, ale przede wszystkim systemowy i strategiczny.

Celem artykułu jest analiza wyzwań stojących przed systemem ochrony infrastruktury krytycznej w Polsce w perspektywie planowanych elektrowni jądrowych. Postawiono następujące pytania badawcze:

1. Jak kształtowały się pojęcie i regulacje infrastruktury krytycznej w Polsce i UE?
2. Jakie są główne kategorie zagrożeń dla infrastruktury krytycznej, w szczególności dla energetyki jądrowej?
3. Na ile obecny model ochrony infrastruktury krytycznej w Polsce jest adekwatny do wyzwań związanych z budową i eksploatacją elektrowni jądrowych?
4. Jakie zmiany instytucjonalne i organizacyjne są pożądane, aby zwiększyć odporność systemu?

Struktura artykułu obejmuje część teoretyczno-prawną, charakterystykę zagrożeń, analizę specyfiki bezpieczeństwa jądrowego oraz postulaty dotyczące modelu ochrony elektrowni jądrowych w Polsce.

1. Infrastruktura krytyczna – ewolucja pojęcia i ujęcie systemowe

1.1. Definicje i podstawowe cechy

W polskim porządku prawnym pojęcie infrastruktury krytycznej zostało zdefiniowane w ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[3]. Zgodnie z art. 3 pkt 2, infrastrukturę krytyczną stanowią systemy oraz wchodzące w ich skład obiekty, urządzenia i instalacje kluczowe dla bezpieczeństwa państwa i obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej i podmiotów gospodarczych. Kluczowy jest tu akcent na systemowość i funkcjonalne powiązania – infrastruktura krytyczna

nie jest prostą sumą pojedynczych obiektów, lecz złożoną siecią elementów wzajemnie się warunkujących.

W literaturze podkreśla się dualny charakter infrastruktury krytycznej: obejmuje ona zarówno infrastrukturę materialną (hardware), jak sieci energetyczne, wodociągi, gazociągi, obiekty transportowe, jak i infrastrukturę niematerialną (software) – systemy teleinformatyczne, procedury zarządzania, wiedzę ekspercką oraz kulturę organizacyjną[4]. Z tej perspektywy infrastruktura krytyczna pełni funkcję „kręgosłupa" państwa – jej odporność decyduje o zdolności systemu polityczno-gospodarczego do przetrwania w sytuacjach kryzysowych.

Do podstawowych cech infrastruktury krytycznej zalicza się:
– **systemowość** – silne powiązania między sektorami, generujące efekt kaskadowy;
– **strategiczność** – kluczowe znaczenie dla ciągłości funkcjonowania państwa;
– **wrażliwość na zagrożenia** – zarówno naturalne, jak i antropogeniczne;
– **interdyscyplinarność ochrony** – konieczność współdziałania administracji, służb, sektora prywatnego i nauki;
– **dynamiczność** – zmienność katalogu sektorów i priorytetów wraz z rozwojem technologii i zagrożeń[5].

1.2. Infrastruktura krytyczna w regulacjach Unii Europejskiej

Na poziomie Unii Europejskiej pojęcie infrastruktury krytycznej zyskało znaczenie wraz z przyjęciem dyrektywy 2008/114/WE dotyczącej identyfikacji i wyznaczania europejskiej infrastruktury krytycznej[6]. Skoncentrowano się wówczas na sektorach energii i transportu, których zakłócenie mogłoby mieć ponadnarodowe skutki. Kolejnym krokiem była dyrektywa CER z 2022 r., odnosząca się do odporności podmiotów krytycznych, oraz dyrektywa NIS2, która rozszerzyła wymagania w zakresie cyberbezpieczeństwa.

Implementacja tych regulacji doprowadziła do dostosowania polskiego systemu prawnego, m.in. poprzez wprowadzenie pojęcia europejskiej infrastruktury krytycznej oraz aktualizację Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK)[7]. Program ten nie tylko identyfikuje sektory IK, ale również definiuje zasady współpracy i podziału odpowiedzialności między państwem a operatorami.

2. Elektrownie jądrowe jako element infrastruktury krytycznej

2.1. Znaczenie dla bezpieczeństwa energetycznego

Elektrownie jądrowe są zaliczane do sektora energetycznego, który ma fundamentalne znaczenie dla funkcjonowania wszystkich pozostałych sektorów infrastruktury krytycznej. Z punktu widzenia bezpieczeństwa energetycznego wyróżnia je kilka cech:

1. **Stabilność dostaw** – w odróżnieniu od części źródeł odnawialnych, energia jądrowa nie jest bezpośrednio zależna od warunków pogodowych.
2. **Niskoemisyjność** – wytwarzanie energii elektrycznej w reaktorach jądrowych wiąże się z bardzo niską emisją CO_2, co czyni je ważnym narzędziem realizacji polityki klimatycznej[8].
3. **Redukcja zależności importowej** – rozwój energetyki jądrowej może ograniczać zależność od importu paliw kopalnych, co ma istotny wymiar geopolityczny.

Jednocześnie elektrownie jądrowe generują specyficzne ryzyka, związane m.in. z potencjalnymi awariami reaktora, skażeniem radiologicznym oraz możliwością wykorzystania materiałów jądrowych do celów przestępczych lub terrorystycznych[9].

2.2. Specyfika bezpieczeństwa jądrowego

Bezpieczeństwo jądrowe opiera się na zasadzie „obrony w głąb" (defence-in-depth), która zakłada tworzenie wielopoziomowych barier technicznych, organizacyjnych i proceduralnych, mających zapobiegać awariom i ograniczać ich skutki[10]. Obejmuje to:

– projektowanie reaktorów o wysokich parametrach bezpieczeństwa;
– redundantne systemy chłodzenia i zasilania;
– wzmocnione konstrukcje budynków reaktora;
– rozwinięte procedury reagowania awaryjnego;
– ścisły nadzór regulacyjny.

Doświadczenia Czarnobyla i Fukushimy pokazały, że kluczowe znaczenie mają nie tylko rozwiązania techniczne, lecz także kultura bezpieczeństwa, jakość regulacji i zdolność państwa do zarządzania kryzysem[11].

3. Kategorie zagrożeń dla infrastruktury krytycznej i elektrowni jądrowych

3.1. Zagrożenia naturalne i technologiczne

Infrastruktura krytyczna jest narażona na szerokie spektrum zagrożeń naturalnych: powodzie, huragany, ekstremalne temperatury, susze czy osuwiska[12]. W przypadku elektrowni jądrowych szczególnie istotne są:

– dostępność wody do chłodzenia,
– ryzyko powodzi i podtopień,
– ekstremalne zjawiska meteorologiczne (silny wiatr, burze, lód)[13].

Zagrożenia technologiczne obejmują awarie urządzeń, wady materiałowe, błędy projektowe oraz niewystarczającą modernizację. Niedoinwestowanie infrastruktury, opóźnienia w wymianie zużytych elementów oraz braki w konserwacji zwiększają podatność systemów na zakłócenia[14].

3.2. Terroryzm i sabotaż

Ze względu na potencjalnie katastrofalne skutki awarii, elektrownie jądrowe stanowią atrakcyjny cel dla terrorystów. Możliwe scenariusze obejmują zarówno ataki zewnętrzne (np. przy użyciu broni palnej, materiałów wybuchowych, bezzałogowych statków powietrznych), jak i działanie wewnętrzne (insider threat)[15].

Sabotaż wewnętrzny jest szczególnie groźny, ponieważ sprawca dysponuje wiedzą o procedurach i słabych punktach systemu[16]. Dlatego tak duży nacisk kładzie się na weryfikację personelu, systemy kontroli dostępu, podział obowiązków oraz rozwijanie kultury bezpieczeństwa jądrowego.

3.3. Cyberzagrożenia

Postępująca cyfryzacja systemów sterowania procesami (SCADA, ICS) przyniosła wzrost efektywności, lecz jednocześnie otworzyła nowy wektor zagrożeń. Przykłady udanych cyberataków na systemy energetyczne, w tym ataki na ukraińskie sieci elektroenergetyczne oraz incydent Colonial Pipeline, pokazują realność ryzyka paraliżu infrastruktury poprzez złośliwe oprogramowanie (w tym ransomware)[17].

W kontekście elektrowni jądrowych kluczowe jest fizyczne i logiczne separowanie systemów sterowania od sieci zewnętrznych, stosowanie dedykowanych rozwiązań bezpieczeństwa (IDS/IPS, monitorowanie integralności danych), ciągły audyt bezpieczeństwa oraz rozwój kompetencji personelu technicznego[18].

3.4. Zagrożenia hybrydowe

Zagrożenia hybrydowe łączą środki militarne i pozamilitarne: cyberataki, sabotaż, operacje informacyjne, szantaż energetyczny, wsparcie grup ekstremistycznych. Celem jest nie tylko fizyczne uszkodzenie infrastruktury, ale także podważenie zaufania społecznego do instytucji państwa, wywołanie chaosu i polaryzacji[19].

Połączenie cyberataku na systemy energetyczne z fizycznym sabotażem i kampanią dezinformacyjną wokół rzekomego zagrożenia radiologicznego mogłoby doprowadzić do masowej paniki, ucieczek ludności i poważnego kryzysu politycznego[20]. W tym sensie elektrownie jądrowe stają się nie tylko obiektem inżynieryjnym, ale także symbolem, wokół którego mogą być prowadzone operacje psychologiczne.

4. Polski system ochrony infrastruktury krytycznej w kontekście energetyki jądrowej

4.1. Ramy instytucjonalno-prawne

Polski system ochrony infrastruktury krytycznej opiera się na współpracy administracji publicznej (w tym Rządowego Centrum Bezpieczeństwa), operatorów poszczególnych sektorów oraz służb odpowiedzialnych za bezpieczeństwo wewnętrzne i obronę narodową[21]. Podstawę prawną stanowią m.in.:

– ustawa o zarządzaniu kryzysowym,
– akty sektorowe (Prawo energetyczne, Prawo atomowe, ustawy o transporcie, łączności),
– Narodowy Program Ochrony Infrastruktury Krytycznej,
– strategie bezpieczeństwa narodowego i cyberbezpieczeństwa.

Dotychczas model ten rozwijano w warunkach braku elektrowni jądrowych. Planowana budowa takich obiektów wymaga jednak wzmocnienia komponentu związanego z bezpieczeństwem jądrowym i radiologicznym, zarówno na poziomie regulacyjnym (rola Państwowej Agencji Atomistyki), jak i operacyjnym[22].

4.2. Ograniczenia obecnego modelu

W literaturze i raportach wskazuje się na kilka słabości obecnego systemu ochrony IK w Polsce[23]:

– rozproszenie kompetencji i brak jednego podmiotu odpowiedzialnego za całościową koordynację ochrony IK;
– zróżnicowany poziom dojrzałości systemów bezpieczeństwa między sektorami i

operatorami;
– ograniczone zasoby kadrowe i finansowe dedykowane ochronie IK;
– niewystarczające uwzględnienie scenariuszy hybrydowych i wielodomenowych.

W przypadku sektora energetyki jądrowej oznacza to ryzyko niedostosowania systemu do specyfiki zagrożeń radiologicznych i jądrowych oraz potencjalnych konsekwencji transgranicznych.

5. Koncepcja wyspecjalizowanej służby ochrony infrastruktury krytycznej

Jedną z propozycji pojawiających się w debacie jest powołanie wyspecjalizowanej służby ochrony infrastruktury krytycznej (SOIK), w ramach której funkcjonowałaby sprofilowana Służba Ochrony Elektrowni Atomowych (SOEA) [24].

Do kluczowych zadań takiej służby należałoby:

– planowanie i realizacja ochrony fizycznej obiektów IK,
– zapewnienie ciągłej ochrony cybernetycznej (we współpracy z CSIRT-ami sektorowymi),
– prowadzenie analiz zagrożeń i ocen ryzyka,
– koordynacja reagowania kryzysowego w obiektach IK,
– współpraca z policją, służbami specjalnymi i siłami zbrojnymi.

Model ten, inspirowany rozwiązaniami funkcjonującymi w wybranych państwach NATO, umożliwiałby kumulację specjalistycznych kompetencji oraz budowę jednolitych standardów bezpieczeństwa w skali krajowej[25].

6. Wnioski i rekomendacje

Analiza pokazuje, że:

1. Infrastruktura krytyczna, w tym sektor energetyki jądrowej, stanowi centralny element bezpieczeństwa narodowego i wymaga podejścia systemowego, uwzględniającego sprzężenia między sektorami.
2. Katalog zagrożeń dla infrastruktury krytycznej uległ znacznemu poszerzeniu – od klasycznych zagrożeń naturalnych i technicznych po cyberataki i złożone działania hybrydowe.

3. Planowana budowa elektrowni jądrowych w Polsce stanowi szansę na wzmocnienie bezpieczeństwa energetycznego, ale równocześnie wymaga głębokiej przebudowy systemu ochrony infrastruktury krytycznej.
4. Obecny model ochrony IK, oparty na rozproszonej odpowiedzialności, powinien zostać uzupełniony o wyspecjalizowane struktury dedykowane ochronie obiektów o szczególnym znaczeniu, zwłaszcza elektrowni jądrowych.
5. Kluczowe znaczenie ma inwestowanie nie tylko w technologie i infrastrukturę fizyczną, lecz także w kulturę bezpieczeństwa, szkolenia personelu, zdolności analityczne oraz współpracę międzynarodową.

Rekomenduje się w szczególności:

– stworzenie wyspecjalizowanej Służby Ochrony Infrastruktury Krytycznej;
– wzmocnienie roli organów odpowiedzialnych za bezpieczeństwo jądrowe i radiologiczne;
– rozwijanie scenariuszy ćwiczeń obejmujących jednoczesne wystąpienie zdarzeń fizycznych, cybernetycznych i informacyjnych;
– systematyczne korzystanie z dobrych praktyk MAEA, UE i NATO w zakresie bezpieczeństwa jądrowego i ochrony IK;
– włączenie zagadnień związanych z odpornością infrastruktury krytycznej do szerszej debaty publicznej nad bezpieczeństwem państwa.

Bibliografia

1. Kitler W., *Bezpieczeństwo narodowe RP. Podstawowe kategorie, uwarunkowania, system*, AON, Warszawa 2011.
2. Jędrzejczyk K., *Bezpieczeństwo energetyczne państwa. Ujęcie teoretyczne i praktyczne*, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego, Warszawa 2017.
3. Gryz J., Kitler W., *System reagowania kryzysowego*, Toruń 2007.
4. Cieślarczyk M., *Teoria i praktyka bezpieczeństwa narodowego w ujęciu systemowym*, AON, Warszawa 2011.
5. Mazurek W., *Brudny terroryzm. Zagrożenia terrorystyczne w energetyce jądrowej*, Wydawnictwo WAM, Kraków 2017.
6. Küfeoğlu S., Akgün A.T., *Cyber Resilience in Critical Infrastructure*, CRC Press, Boca Raton 2023.
7. Lannoy A., *Reliability of Nuclear Power Plants*, Wiley-ISTE, London 2022.
8. *Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej*, Rządowe Centrum Bezpieczeństwa, Warszawa 2023.
9. *Safety of Nuclear Power Plants: Design. Specific Safety Requirements No. SSR-2/1 (Rev. 1)*, IAEA, Vienna 2016.
10. *Report Fukushima: Ten Years On*, OECD/NEA, Paris 2021.
11. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z późn. zm.).
12. *Konwencja o wczesnym powiadamianiu o awarii jądrowej*, Wiedeń, 26 września 1986 r., Dz.U. 1988, nr 31, poz. 216.
13. *Konwencja o pomocy w przypadku awarii jądrowej lub zagrożenia radiologicznego*, Wiedeń, 26 września 1986 r.
14. *NIK o bezpieczeństwie obiektów infrastruktury krytycznej*, Najwyższa Izba Kontroli, dostęp: 06.02.2025.
15. *IAEA Safety Standards*, Międzynarodowa Agencja Energii Atomowej, dostęp: 29.09.2025.
16. *Ransomware – jedno z najpoważniejszych zagrożeń w cyberprzestrzeni*, gov.pl, dostęp: 30.09.2025.
17. *Raport Cyberbezpieczeństwo w energetyce*, 2024, dostęp: 29.02.2024.

Jacek Doskocz
LeoXR sp. z o.o. w Radomiu
https://orcid.org/0000-0002-5299-2465
Rafał Radowiecki
LeoXR sp. z o.o. w Radomiu
https://orcid.org/0009-0005-3177-3991
Henryk Wojtaszek
Wyższa Szkoła Kształcenia Zawodowego we Wrocławiu
https://orcid.org/0000-0002-3082-1219
Mateusz Ziętarski
Pomorska Szkoła Wyższa w Starogardzie Gdańskim
https://orcid.org/0000-0003-2960-7669
Agnieszka Doskocz
LeoXR sp. z o.o. w Radomiu
https://orcid.org/0009-0003-0453-6857

Przegląd nowoczesnych metod szkolenia i treningu strzelania dla szkół mundurowych uwzględniając trendy technologiczne i badania naukowe

Streszczenie

W ostatnich latach rozwój technologii cyfrowych i immersyjnych znacząco wpłynął na metody szkolenia strzeleckiego w szkołach mundurowych. Niniejszy artykuł stanowi kompleksowy przegląd nowoczesnych systemów edukacji i treningu z broni palnej, ze szczególnym uwzględnieniem wirtualnej rzeczywistości (VR), wirtualnych strzelnic (VR CAVE) oraz laserowych trenażerów (tarcze z fotokomórkami). Analizowane są również aktualne badania naukowe potwierdzające skuteczność tych innowacyjnych metod, w tym ich wpływ na szybkość przyswajania umiejętności, poprawę precyzji, retencję wiedzy oraz przygotowanie funkcjonariuszy do realnych sytuacji. Ponadto artykuł omawia aspekty bezpieczeństwa, koszt-efektywności oraz adaptacyjności treningów w kontekście współczesnych wyzwań w szkoleniu służb mundurowych. Przedstawione w publikacji wnioski

mogą wspierać rozwój nowatorskich programów edukacyjnych, optymalizujących proces przygotowania przyszłych funkcjonariuszy do wykonywania zadań w dynamicznym i wymagającym środowisku operacyjnym przy korzystaniu z oprogramowania VR jest DroneHunting.EU.

Słowa kluczowe: trening strzelania, nauka strzelania, strzelanie VR, technologie VR w obronności

Review of Modern Methods of Shooting Training and Practice for Uniformed Schools, Considering Technological Trends and Scientific Research

Abstract

In recent years, the development of digital and immersive technologies has significantly influenced shooting training methods in uniformed schools. This article provides a comprehensive review of modern firearm education and training systems, with particular emphasis on virtual reality (VR), virtual shooting ranges (VR CAVE), and laser training systems (targets with photodetectors). It also analyzes current scientific research confirming the effectiveness of these innovative methods, including their impact on skill acquisition speed, accuracy improvement, knowledge retention, and officers' preparedness for real-life scenarios. Furthermore, the article discusses safety, cost-effectiveness, and adaptability aspects of training in the context of contemporary challenges faced by uniformed services. The conclusions presented here may support the development of innovative educational programs that optimize the preparation of future officers for operations in dynamic and demanding environments, using VR-based software such as DroneHunting.EU.

Keywords: shooting training, learning to shoot, VR shooting, VR technologies in defense

Wprowadzenie

Szkolenie strzeleckie jest fundamentalnym elementem przygotowania funkcjonariuszy służb mundurowych, niezbędnym do zapewnienia skutecznej i bezpiecznej reakcji w sytuacjach kryzysowych. Tradycyjne metody szkolenia, opierające się głównie na strzelaniu ostrą amunicją na poligonach, są często czasochłonne, kosztowne i wymagają skomplikowanej logistyki.[1,2,3,4] Ograniczony dostęp do strzelnic i wysokie koszty amunicji narzuciły konieczność poszukiwania alternatywnych, zaawansowanych technologicznie rozwiązań[4,5].

W odpowiedzi na te wyzwania, technologia wirtualnej (VR) i rozszerzonej rzeczywistości (XR) oferuje znaczący potencjał transformacji szkolenia, umożliwiając przeprowadzanie immersyjnych symulacji w dowolnym miejscu i czasie[1,2,6]. Nowoczesne systemy symulacyjne pozwalają na wielokrotne powtarzanie scenariuszy, ograniczając ryzyko dla uczestników i środowiska[2,7], jednocześnie umożliwiając bezpieczne popełnianie błędów, z których funkcjonariusze mogą się uczyć.

Niniejszy artykuł dokonuje przeglądu trzech kluczowych, nowoczesnych metod treningu strzeleckiego stosowanych i badanych w kontekście szkolenia służb mundurowych.

2. Metody szkolenia i treningu bazujące na nowoczesnych technologiach

2.1 Metoda bazująca na technologii wirtualnej rzeczywistości (Gogle VR)

Wirtualna Rzeczywistość (VR) z wykorzystaniem gogli typu HMD (Head-Mounted Display) zapewnia pełną immersję, co jest kluczowe dla skuteczności symulacji. Rosnąca dostępność i przystępność cenowa konsumenckich zestawów VR o wysokiej rozdzielczości (np. platforma Meta Quest) przyczyniła się do wzrostu zainteresowania immersyjnym treningiem i symulacją w środowiskach policyjnych i akademickich [5,6]. Przykładem tego typu rozwiązaniem na jest DroneHunting.eu. VR jest powszechnie wykorzystywana w szkoleniu funkcjonariuszy, w tym do treningu strzeleckiego [10]. Tego rodzaju symulacje pozwalają na:

- **Wpływ na psychofizjologię i gotowość poznawczą:** Kluczowym elementem jest opanowanie specyficznych reakcji psychofizjologicznych związanych z kontrolowanym oddychaniem podczas strzelania [11]. VR umożliwia odtwarzanie realistycznych scenariuszy, które wywołują ostrą reakcję stresową, porównywalną do

tej w warunkach rzeczywistych[12,13,14]. Badania wykazały, że VR może być wykorzystywana do treningu z uwzględnieniem oddychania, co poprawiło kontrolę oddechu u 8 z 9 uczestników treningu w wirtualnym środowisku akcji[16,17]. Systemy, takie jak BioPhyS, wykorzystują dane neurofizjologiczne (EEG) i sercowo-naczyniowe (HRV) do tworzenia psychofizjologicznego modelu szkolenia, który służy do projektowania adaptacyjnych systemów treningowych (tzw. adaptacja biocybernetyczna) [18,19,20,21]. Taka integracja umożliwia trenowanie **gotowości poznawczej** (ang. *cognitive readiness*).

- **Trening decyzyjności i redukcja uprzedzeń:** Wiele symulacji VR koncentruje się na podejmowaniu decyzji użycia siły (*shoot/don't shoot*), deeskalacji i niwelowaniu uprzedzeń [10,24]. VR jest przydatnym narzędziem do badania uprzedzeń rasowych w decyzjach o użyciu siły śmiertelnej i w scenariuszach strzeleckich. Wykazano, że trening w VR może poprawiać umiejętności deeskalacji oraz zmniejszać uprzedzenia wobec osób z problemami psychicznymi [27]. Uczestnicy cywilni, którzy ukończyli szkolenie w VR, wykazali wyższy poziom wiedzy, motywacji i poczucia własnej skuteczności w scenariuszu aktywnego strzelca[28,29]. Szkolenia oparte na VR mogą zwiększyć wrażliwość funkcjonariuszy na własne zachowanie.
- **Wierność (Fidelity) i Imersja:** VR może zapewnić imersyjne środowiska szkoleniowe, które można prowadzić w dowolnym miejscu i czasie[1,5,6]. Immersyjna VR (HMD) może powodować **ostrą reakcję stresową** porównywalną do realistycznego treningu scenariuszowego[15,31]. Zastosowanie pełnych awatarów w wieloosobowej wirtualnej rzeczywistości może zwiększać poczucie zagrożenia i realizm[32,35]. Badania sugerują również, że fizyczne rekwizyty, takie jak **dotykowy pas taktyczny** (ang. *Tangible Tactical Belt*) z replikami broni i kajdanek, wzmacniają realizm haptyczny i immersję[34,35].
- **Elastyczność i bezpieczeństwo:** VR pozwala na prowadzenie powtarzalnego treningu, który byłby trudny lub niemożliwy do zaaranżowania w rzeczywistym świecie ze względu na niepraktyczność inscenizacji [36]. Jest to bezpieczniejsze niż konwencjonalne ćwiczenia, umożliwiając bezpieczną interakcję z niebezpiecznymi narzędziami, takimi jak materiały wybuchowe, lub bezpieczne włączanie do symulacji osób należących do grup wrażliwych, takich jak dzieci [37,38].

2.2 Metoda bazująca na wyświetlaczu multimedialnym (Projekcyjna strzelnica wirtualna)

Ta metoda, znana również jako projekcyjna strzelnica wirtualna lub uproszczona wersja CAVE, wykorzystuje wyświetlacz multimedialny lub projekcję na jednej ścianie. Symulator broni palnej wysyła znacznik laserowy na ekran [39,40]. Specjalna kamera, wykorzystująca przetwarzanie obrazu, wykrywa współrzędne (x, y) trafienia wiązki laserowej [40,41].

Kluczowe zalety i zastosowania tej metody w szkoleniu:

- **Przetwarzanie Obrazu i Precyzja:** Systemy te osiągają wysoką precyzję detekcji uderzenia. Przykładowy prototyp laserowy (PLP) osiągnął dokładność 95,4% z latencją poniżej 80 ms, wykorzystując przetwarzanie obrazu, w tym normalizację radiową i filtr Gaussian defocus, w celu zminimalizowania zakłóceń szumem i poprawy spójności w różnych warunkach oświetleniowych [40,41,42].
- **Adaptacyjność i Mobilność:** Metody oparte na przetwarzaniu obrazu do detekcji uderzenia laserem mogą być projektowane jako systemy przenośne i bezprzewodowe, co pozwala na ich użycie w różnych warunkach terenowych i oświetleniowych, bez konieczności stosowania kabli zasilających czy transmisyjnych (np. system PLP) [40,41,43,44].
- **Realizm interakcyjny:** Chociaż nie zapewnia pełnej immersji VR-HMD, systemy te mogą być integrowane z replikami broni palnej, które posiadają systemy elektromechanicznego odrzutu, zwiększając realizm doświadczenia strzeleckiego [5, 45].

2.3 Metoda bazująca na tarczach z fotokomórką (Laserowe Trenażery Strzeleckie - LMTS)

Laserowe Trenażery Strzeleckie (LMTS, ang. *Laser Marksmanship Training System*) to urządzenia oparte na laserze, wykorzystywane do szkolenia strzeleckiego z użyciem zmodyfikowanej broni służbowej [46,47]. Systemy te pozwalają na zaoszczędzenie czasu i amunicji [46,48]. Wykazano ich potencjał w przewidywaniu wyników strzelania ostrą amunicją zarówno z karabinów, jak i pistoletów [48,49,50].

- **Wzmacnianie Podstaw:** LMTS wspiera realistyczny i kompleksowy Program Szkolenia Strzeleckiego (POI), umacniając podstawowe zasady strzelania, ponieważ żołnierze używają swojej faktycznej broni [47].
- **Ograniczenia Balistyczne:** Laserowe systemy treningowe (np. MARS) opierały się na technologii podczerwieni laserowej, która **nie uwzględniała balistycznej trajektorii**

pocisku (sześciu stopni swobody). Jest to istotne ograniczenie, gdyż strzelcy muszą rozumieć krzywą balistyczną i odpowiednio korygować celowanie w zależności od odległości do celu. Nowoczesne systemy VR pokonują tę lukę, implementując algorytm trajektorii pocisku w sześciu stopniach swobody (6-DOF) [51,52,53].

3. Trendy technologiczne i badawcze

3.1 Adaptacyjność i sztuczna inteligencja (AI)

Integracja Sztucznej Inteligencji (AI) jest kluczowym trendem w rozwoju symulatorów wojskowych i policyjnych, umożliwiając tworzenie dynamicznych i realistycznych scenariuszy [54,55,56].

- **Adaptacja Biocybernetyczna:** Systemy VR, takie jak BioPhyS, wykorzystują dane fizjologiczne (EEG, HRV) do ciągłego monitorowania stanu psychofizjologicznego funkcjonariuszy podczas strzelania [18,19]. AI może wykorzystywać te dane w czasie rzeczywistym, aby dynamicznie dostosowywać trudność symulacji (np. prędkość celów, intensywność deszczu) w celu **maksymalizacji pożądanego stanu psychofizjologicznego** (np. skupienia i spokoju), co jest określane jako adaptacja biocybernetyczna [6,20,22,57].
- **AI-Driven Scenarios:** Symulatory oparte na AI mogą **dostosowywać scenariusze w czasie rzeczywistym** w zależności od działań szkolonego, co czyni doświadczenie bardziej spersonalizowanym i nieprzewidywalnym [55,56,58]. AI może również dynamicznie generować materiały szkoleniowe, dostosowując się do indywidualnego poziomu trudności [36,59].

3.2 Wierny realizm (Balistyka i Sprzężenie Zwrotne)

Aby zapewnić, że umiejętności nabyte w symulacji przekładają się na rzeczywiste warunki (*skill transfer*), niezbędna jest wysoka wierność (ang. *fidelity*) [6,52,60].

- **Modelowanie:** Zaawansowane symulatory VR, implementują algorytm trajektorii pocisku w sześciu stopniach swobody (6-DOF). Ten zaawansowany silnik balistyczny uwzględnia wpływ grawitacji, oporu powietrza, wiatru i znoszenia. Badania wykazały, że szkolenie z użyciem takich systemów znacząco poprawiło celność strzelania (K-2C1) ostrą amunicją w porównaniu z grupami kontrolnymi [51,52,53].

- **Sprzężenie zwrotne haptyczne:** W celu zwiększenia realizmu, repliki broni powinny mieć mechanizmy odrzutu (np. sprężone powietrze) [61,62]. Dodatkowo, fizyczne rekwizyty, takie jak **dotykowy pas taktyczny** [34], oraz możliwość symulacji multisensorycznych bodźców stresowych (np. pogodowych) zwiększają realizm i immersję [63,64,65].

3.3 Bezpieczeństwo i koszt-efektywność

Nowoczesne symulatory są cenione za **bezpieczeństwo** i **oszczędność** [2, 4] .

- **Bezpieczeństwo:** VR/XR pozwala na bezpieczny trening w sytuacjach wysokiego ryzyka (np. aktywny strzelec, incydenty użycia siły) w kontrolowanym środowisku, bez narażania uczestników na niebezpieczeństwo [2,7, 37, 38].
- **Koszt-efektywność:** Trening VR pozwala na oszczędność kosztów logistycznych, czasu i amunicji w porównaniu z tradycyjnym treningiem [2,3,4,5,25,66]. Choć początkowy koszt opracowania systemów może być wysoki, długoterminowe oszczędności są znaczące [25,40]. Badania wskazują, że strzelanie ostrą amunicją jest drogie, ryzykowne i ograniczone przez czas, przestrzeń i klimat, natomiast VR eliminuje te ograniczenia [3,4].

4. Wnioski

Nowoczesne metody szkolenia strzeleckiego, bazujące na zaawansowanych technologiach, stanowią istotną ewolucję w przygotowaniu funkcjonariuszy służb mundurowych.

Laserowe Trenażery Strzeleckie (LMTS) i projekcyjne strzelnice wirtualne stanowią koszt-efektywną i mobilną opcję do treningu podstawowych technik i świadomości sytuacyjnej, oferując natychmiastową informację zwrotną o trafieniu [40,41,44]. Mają one jednak historyczne ograniczenie w wiernym odtwarzaniu balistyki na dłuższych dystansach, co jest kluczowe dla zaawansowanego strzelania [52].

Technologie Wirtualnej Rzeczywistości (VR) (Gogle VR), szczególnie te zintegrowane z modelowaniem 6-DOF, stanowią najbardziej **kompleksowe i zaawansowane** narzędzie. Integracja AI i danych psychofizjologicznych (np. EEG, HRV) umożliwia trening gotowości

poznawczej i kontroli emocjonalnej w sytuacjach wysokiego stresu, co jest niemożliwe do osiągnięcia za pomocą prostszych metod [18,20,22].

W kierunku przyszłego rozwoju, kluczowe jest dążenie do pełnej wierności (fidelity), w tym modelowania balistycznego (6-DOF) w VR, co jest niezbędne, aby trening wirtualny przekładał się na poprawę celności w strzelaniu ostrą amunicją [51,52].

5. Podsumowanie: Dominująca rola i skuteczność technologii VR

Technologie Wirtualnej Rzeczywistości (VR) mają największe znaczenie i skuteczność w nowoczesnym szkoleniu strzeleckim dla służb mundurowych, ponieważ tylko VR łączy kluczowe zalety techniczne, psychologiczne i logistyczne.

1. **Imersja i Realizm Scenariuszowy:** VR z wykorzystaniem HMD oferuje pełną imersję, która umożliwia symulację realnych, złożonych i ryzykownych scenariuszy, takich jak incydenty z aktywnym strzelcem czy użyciem siły (*shoot/don't shoot*), które są zbyt niebezpieczne lub kosztowne do powtórzenia w realu [1,2,4, 10, 37,38]. Pełne awatary ciała w immersyjnym VR zwiększają poczucie zagrożenia, co przekłada się na bardziej realistyczną reakcję psychiczną [32,33].
2. **Trening Decyzyjności i Redukcja Stresu:** Badania potwierdzają, że VR jest kluczowa dla treningu poznawczego i decyzyjności w sytuacjach stresowych [10, 24]. Systemy VR umożliwiają stosowanie adaptacji biocybernetycznej, która, poprzez monitorowanie EEG i HRV, pomaga funkcjonariuszom trenować **gotowość poznawczą** i utrzymywać kontrolę fizjologiczną (np. kontrolę oddechu) pod presją – co jest bezpośrednio powiązane z wydajnością strzelecką w krytycznych sytuacjach [18,20,22]. Trening VR może prowadzić do ostrej reakcji stresowej, która jest podobna do tej obserwowanej w realnym treningu scenariuszowym, co jest dowodem na **wysoką wierność psychologiczną** symulacji [15,31].
3. **Wierność Balistyczna i Transfer Umiejętności:** Podczas gdy tradycyjne trenażery laserowe mają ograniczenie w symulowaniu balistyki pocisku, nowoczesne symulatory VR integrują algorytmy sześciu stopni swobody (6-DOF). Badania wykazały, że ten typ szkolenia w VR znacząco poprawił **celność strzelania ostrą amunicją** (live-fire accuracy)[51,52], co jest najważniejszym dowodem na transfer umiejętności do

rzeczywistości. Co więcej, VR jest skutecznym medium do szkolenia taktycznej kontroli wzroku, świadomości sytuacyjnej i umiejętności deeskalacji [27,67].

4. **Skalowalność i Ekonomia:** Dzięki przystępnym cenowo goglom VR i możliwości dostarczania treningu *„anywhere, anytime”*, VR eliminuje wąskie gardła związane z dostępem do kosztownych fizycznych obiektów i amunicji, co czyni ją **najbardziej skalowalną i elastyczną** metodą [2,5,36].

Mimo że tradycyjne strzelnice projekcyjne są ekonomiczne i mobilne [40], a LMTS wspiera podstawy strzeleckie, to VR jest jedyną technologią, która w pełni integruje zaawansowane modelowanie balistyczne z intensywnym treningiem decyzyjnym i psychofizjologicznym, co czyni ją **niezbędną i najskuteczniejszą** w kontekście przygotowania funkcjonariuszy i żołnierzy do współczesnych wyzwań operacyjnych [5,20,5, 52]. Jednym z wartościowych i przyszłościowych jest system DroneHunting.EU w technologii wirtualnej rzeczywistośći.

Bibliografia

1. Agha, Riaz A., and Alexander J. Fowler. "The Role and Validity of Surgical Simulation." *International Surgery* 2 (2015).
2. Andersen, J. P., P. M. Di Nota, B. Beston, E. C. Boychuk, H. Gustafsberg, S. Poplawski, *et al*. "Reducing lethal force errors by modulating police physiology." *J. Occup. Environ. Med.* 60 (2018): 867–874.
3. Biggs, A. T., J. R. Brockmole, and J. K. Witt. "Armed and attentive: holding a weapon can bias attentional priorities in scene viewing." *Atten. Percept. Psychophys.* 75 (2013): 1715–1724.
4. Biggs, A. T., J. A. Hamilton, A. G. Thompson, and R. Markwald. "Talk is cheap: Self-reported versus actual marksmanship proficiency among military and community samples." *Am. J. Psychol.* 137, no. 1 (2024): 1–17.
5. Bhagat, Kaushal Kumar, Wei-Kai Liou, and Chun-Yen Chang. "A cost-effective interactive 3D virtual reality system applied to military live firing training." *Virtual Reality* 20, no. 2 (2016): 127–140.
6. Binsch, Olaf, Nanco Oudejans, Milan N. A. Van Der Kuil, Annemarie Landman, Math M. J. Smeets, Mathie P. G. Leers, and Annika S. Smit. "The Effect of Virtual Reality Simulation on Police Officers' Performance and Recovery from a Real-Life Surveillance Task." *Multimedia Tools and Applications* 82, no. 11 (2023): 17471–17492.
7. Buga, Alex, Xavier El-Shazly, Christopher D. Crabtree, Justen T. Stoner, Lucas Arce, Drew D. Decker, Bradley T. Robinson, Madison L. Kackley, Teryn N. Sapper, John Paul V. Anders, William J. Kraemer, and Jeff S. Volek. "Age and weekly physical activity are correlated with ballistic VR decision making and reaction time shooting performance at rest." (2025).
8. Buga, A., *et al*. "The VirTra V-100 is a test-retest reliable shooting simulator for measuring accuracy/precision, decision-making, and reaction time in civilians, police/SWAT, and military personnel." *J. Strength Cond. Res.* 38, no. 10 (2024): 1714–1723.
9. Caserman, Polona, Philip Schmidt, Thorsten Göbel, Jonas Zinnäcker, André Kecke, and Stefan Göbel. "Impact of Full-Body Avatars in Immersive Multiplayer Virtual Reality Training for Police Forces." *IEEE Transactions on Games* 14, no. 4 (2022): 706–714.

10. Caserman, Polona, Philipp Niklas Müller, Thorsten Göbel, Pascal Tonecker, Savas Yildirim, André Kecke, Dennis Purdack, and Stefan Göbel. "Virtual Reality Simulator for Police Training with AI-Supported Cover Detection." In *Serious Games*, edited by Mads Haahr, Alberto Rojas-Salazar, and Stefan Göbel, 181–193. Vol. 14309. Cham: Springer Nature Switzerland, 2023.
11. Cole, Karie R., and Richard K. Shields. "Age and Cognitive Stress Influences Motor Skill Acquisition, Consolidation, and Dual-Task Effect in Humans." *J Mot Behav.* 51, no. 6 (2019): 622–639.
12. de Armas, C., R. Tori, and A. V. Netto. "Use of virtual reality simulators for training programs in the areas of security and defense: A systematic review." *Multimed. Tools Appl.* 79 (2020): 3495–3515.
13. De Vries, Peter W., Bas Böing, Els Mulder, and Jean-Louis Van Gelder. "Sugarcoating a Bitter Pill - VR Against Police Ethnic Profiling." In *Persuasive Technology*, edited by Alexander Meschtscherjakov, Cees Midden, and Jaap Ham, 22–35. Vol. 13832. Cham: Springer Nature Switzerland, 2023.
14. Garcia, E. T., S. G. Ware, L. J. Baker, Bartak R, and Brawner K. "Measuring Presence and Performance in a Virtual Reality Police Use of Force Training Simulation Prototype." *32nd International Florida Artificial Intelligence Research Society Conference, FLAIRS 2019* (2019): 276–281.
15. García Torres, José Antonio, Daniel Guzmán Pérez, Jhon Fredy Rincón Morantes, Daniel Felipe Molina Martínez, Cristian Camilo García Rodríguez, and Jhonnatan Eduardo Zamudio Palacios. "Image Processing for Laser Impact Detection in Shooting Simulators." *TecnoLógicas* 28, no. 62 (2025).
16. Gamito, Pedro, Jorge Oliveira, Jorge Silva, Joana Rosa, Maria L.R.Mendes, Ricardo Dias, Fábio Dias, Shivani A. Mansuklal, Joana Cartaxo, Hélder António, and Ágata Salvador. "Stress Inoculation in Police Officers Using Virtual Reality: A Controlled Study." *Cyberpsychology, Behavior, and Social Networking* 27, no. 4 (2024): 253–260.
17. Gaire, U. S. "Application of artificial intelligence in the military: An overview." *Unity Journal* 4, no. 1 (2023): 161–174.
18. Guo, Jia-Hui, Xiao-Na Zhou, Hu-Ye Zhou, Chen-Wei Huang, Yi-Lin Wu, Hong Zheng, Yun-Zi Liu, and Chun-Lei Jiang. "Enhancing shooting performance and cognitive engagement in virtual reality environments through brief meditation training." (2025).

19. Harris, D. J., K. J. Hardcastle, M. R. Wilson, and S. J. Vine. "Assessing the Learning and Transfer of Gaze Behaviours in Immersive Virtual Reality." *Virtual Reality* 25, no. 4 (2021): 961–973.
20. Harris, D. J., T. Arthur, J. Kearse, M. Olonilua, E. K. Hassan, T. C. De Burgh, M. R. Wilson, and S. J. Vine. "Exploring the role of virtual reality in military decision training." *Frontiers in Virtual Reality* 4 (2023).
21. Hussen, Noha, Rahma Mohamed, Islam Hany Hassan, Yousef Hossam, Mohamed Ashraf, and Maged Sadek. "A Review of Real-time Military Training Simulator Based on Improving War Scenario Using AI Tools." *Advanced Sciences and Technology Journal* 2, no. 2 (2025): 1020.
22. Kent, Julie A., and Charles E. Hughes. "Law Enforcement Training Using Simulation for Locally Customized Encounters." *Frontiers in Virtual Reality* 3 (2022): 960146.
23. Kleygrewe, Lisanne, R. I. Vana Hutter, Matthijs Koedijk, and Raôul R. D. Oudejans. "Virtual Reality Training for Police Officers: A Comparison of Training Responses in VR and Real-Life Training." *Police Practice and Research* 25, no. 1 (2024): 18–37.
24. Lavoie, Jennifer, Natalie Álvarez, Victoria Baker, and Jacqueline Kohl. "Training Police to De-Escalate Mental Health Crisis Situations: Comparing Virtual Reality and Live-Action Scenario-Based Approaches." *Policing: A Journal of Policy and Practice* 17 (2023): paad069.
25. Leite Jr., A. J. M., G. A. M. Gomes, N. A. Chicca Jr., A. D. D. Santos, C. A. Vidal, J. B. Cavalcante-Neto, M. Gattass, and Automacao de Engenharia; Squartz Technologies NVIDIA; Absolut Technologies; BARCO; Grande. "System Model for Shooting Training Based on Interactive Video, Three-Dimensional Computer Graphics and Laser Ray Capture." *2012 14th Symposium on Virtual and Augmented Reality, SVR 2012* (2012): 254–260.
26. Liao, Yi-Cheng, Hao-Chiang Koong Lin, Po-Chun Kuo, and Kuan-Yu Lin. "The Effects of Virtual Reality System Applied to Shooting Training Course for Senior High School Students." In *Proceedings of the 27th International Conference on Computers in Education*, 531–536 (2019).
27. Lovreglio, Ruggiero, Daphney-Chloe Ngassa, Anass Rahouti, Daniel Paes, Zhenan Feng, and Alastair Shipman. "Prototyping and Testing a Virtual Reality Counterterrorism Serious Game for Active Shooting." *International Journal of Disaster Risk Reduction* 82 (2022): 103283.

28. Martaindale, M. Hunter, William L. Sandel, Aaron Duron, and Matthew J. McAllister. "Can a Virtual Reality Training Scenario Elicit Similar Stress Response as a Realistic Scenario-Based Training Scenario?" *Police Quarterly* 27, no. 1 (2024): 109–129.
29. Michela, Abele, Jacobien M. van Peer, Jan C. Brammer, Anique Nies, Marieke MJW van Rooij, Robert Oostenveld, Wendy Dorrestijn, Annika S. Smit, Karin Roelofs, and Floris Klumpers. "Deep-Breathing Biofeedback Trainability in a Virtual-Reality Action Game: A Single-Case Design Study with Police Trainers." *Frontiers in Psychology* 13 (2022): 806163.
30. Muñoz, John E., Luis Quintero, Chad L. Stephens, and Alan T. Pope. "A Psychophysiological Model of Firearms Training in Police Officers: A Virtual Reality Experiment for Biocybernetic Adaptation." *Frontiers in Psychology* 11 (2020): 683.
31. Murtinger, Markus, Jakob C. Uhl, Quynh Nguyen, and Georg Regal. "Tangible Tactical Belt: Haptic Realism for Virtual Reality Police Training." In *2023 IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering (MetroXRAINE)*, 599–604 (2023).
32. Nawrat, Aleksander, Karol Jędrasiak, Artur Ryt, and Dawid Sobel. "Multimedia Firearms Training System." *International Journal of Computer and Information Engineering* 10, no. 11 (2016).
33. Nguyen, Q., E. Jaspaert, M. Murtinger, H. Schrom-Feiertag, S. Egger-Lampl, M. Tscheligi, Ardito C, Lanzilotti R, Malizia A, Malizia A, Petrie H, Piccinno A, Desolda G, and Inkpen K. "Stress Out: Translating Real-World Stressors into Audio-Visual Stress Cues in VR for Police Training." *18th IFIP TC 13 International Conference on Human-Computer Interaction, INTERACT 2021* 12933 (2021): 551–561.
34. Olma, Joshua, Christof Sutter, and Sven Sülzenbrück. "Blended police firearms training improves performance in shoot/don't shoot scenarios: a systematic replication with police cadets." *Front. Psychol.* 15 (2024): 1495812.
35. Olma, Joshua, Christof Sutter, and Sven Sülzenbrück. "When failure is not an option: a police firearms training concept for improving decision-making in shoot/don't shoot scenarios." *Front. Psychol.* 15 (2024): 1335892.
36. Podoletz, Lena, Mark McGill, David McIlhatton, Jill Marshall, Niamh Healy, and Leonie Maria Tanczer. "A Critical Review of Virtual and Extended Reality Immersive Police Training: Application Areas, Benefits & Vulnerabilities." In *30th ACM Symposium on Virtual Reality Software and Technology (VRST '24)*, October 09–11, 2024, Trier, Germany. New York, NY, USA: ACM, 2024.

37. Pope, A. T., C. L. Stephens, and K. Gilleade. "Biocybernetic adaptation as biofeedback training method." In *Advances in Physiological Computing*, edited by K. Gilleade, 91–115. Berlin: Springer, 2014.
38. Paululat, Meret. "The Impact of Racist Stereotypes on Dutch Police Officers' Behaviour in Stop-and-Search Scenarios: A Randomized Study with Deepfake Technology in Virtual Reality." B.S. Thesis, University of Twente, 2023.
39. Smith, M. D., and J. D. Hagman. "Predicting Rifle and Pistol Marksmanship Performance with the Laser Marksmanship Training System (Tech. Rep 1106)." Alexandria, VA: U.S. Army Research Institute for the Behavioral and Social Sciences, 2000.
40. Smith, M.D., and J. D. Hagman. "Predicting Rifle and Pistol Marksmanship Qualification (Research Report 1804)." Alexandria, VA: U.S. Army Research Institute for the Behavioral and Social Sciences, 2003.
41. Sudiarno, Adithya, Ratna Sari Dewi, Retno Widyaningrum, Reza Aulia Akbar, Yupit Sudianto, Wahyu Andy Prastyabudi, and Ahmadi. "Analysis of Human Performance and Potential Application of Virtual Reality (VR) Shooting Games as a Shooting Training Simulator for Military Personnel." *International Journal of Technology* 15, no. 1 (2024): 87–98.
42. Tawa, John, Yuanguo Lang, and Audrey St John. "Measuring Visual Attention with 360 Degree Video Stimuli in Virtually Immersive Environments: A Case Study of Police Officers' Decisions to Shoot." Available at SSRN 4063506 (2022).
43. Tawa, John, Yuanguo Lang, and M. M. Jernigan. "Cognitive and affective precursors to decisions to use lethal force against black suspects: a virtual reality application." *Race Just.* (2022).
44. Temby, P., C. Ryder, A. Vozzo, and G. Galanis. "Sharp Shooting in Fuzzy Fields: Effects of Image Clarity in Virtual Environments." *Proceedings of the Simulation, Technology and Training (SimTecT) Conference*, Sydney, Australia, 2005.
45. Uhl, Jacob C., Huu Quynh Huong Nguyen, Yannick Hill, Markus Murtinger, and Manfred Tscheligi. "xHits: An Automatic Team Performance Metric for VR Police Training." *2023 IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering. Proceedings* (2023).
46. Uhl, Jakob Carl, Georg Regal, Michael Gafert, Markus Murtinger, and Manfred Tscheligi. "Stress Embodied: Developing Multi-sensory Experiences for VR Police Training." In *Human-Computer Interaction – INTERACT 2023*, edited by José

Abdelnour Nocera, Marta Kristín Lárusdóttir, Helen Petrie, Antonio Piccinno, and Marco Winckler, 573–583. Cham: Springer Nature Switzerland, 2023.

47. Vickers, J. N., and W. Lewinski. "Performing under pressure: gaze control, decision making and shooting performance of elite and rookie police officers." *Hum. Mov. Sci.* 31 (2012): 101–117.
48. Voigt, Laura, and Marie Ottilie Frenkel. "How Officers Perform and Grow under Stress: Police Training in Virtual Reality." In *Police Conflict Management, Volume II*, edited by Mario S. Staller, Swen Koerner, and Benni Zaiser, 187–211. Cham: Springer International Publishing, 2023.
49. Wang, W., H. Liu, W. Lin, Y. Chen, and J.-A. Yang. "Investigation on Works and Military Applications of Artificial Intelligence." *IEEE Access* 8 (2020): 131614–131625.
50. Zaremba, Arnold, Jakub Tytuła, and Szymon Nitkiewicz. "The Analysis of the Possibilities of Using a Virtual Reality System in Fitness Training." *Technical Sciences* 26 (2023): 97–110.
51. Zechner, Olivia, Lisanne Kleygrewe, Emma Jaspaert, Helmut Schrom-Feiertag, RI Vana Hutter, and Manfred Tscheligi. "Enhancing Operational Police Training in High Stress Situations with Virtual Reality: Experiences, Tools and Guidelines." *Multimodal Technologies and Interaction* 7, no. 2 (2023): 14.
52. Zhang, Mingbao, Xiang Li, Zezheng Yu, Zhuo Chen, Yan Sun, and Yidi Li. "Virtual Range Training Based on Virtual Reality." In *4th International Conference on Contemporary Education, Social Sciences and Humanities (ICCESSH 2019)*, 2019.
53. Zhang, M., X. Li, Z. Yu, Z. Chen, Y. Sun, and Y. Li. "Virtual range training based on virtual reality." In *Proceedings of the 4th International Conference on Contemporary Education, Social Sciences and Humanities (ICCESSH 2019)*, 2019.
54. Lee, Byounghwak, Taek Yong Hwang, Seungju Hyun, and Hyunyup Lee. "Improvement of K-2 rifle's live-fire accuracy using virtual reality shooting training system." *Virtual Reality* 29 (2025): 23.

Mirosław Podgórski

Szkoła Główna Mikołaja Kopernika w Warszawie

https://orcid.org/0009-0008-8653-0681

Cyberbezpieczeństwo wschodniej flanki NATO w obliczu wojny rosyjsko-ukraińskiej

Streszczenie

Wojna rosyjsko-ukraińska stanowi punkt zwrotny w postrzeganiu cyberprzestrzeni jako jednego z kluczowych wymiarów współczesnych konfliktów zbrojnych. Działania prowadzone przez Federację Rosyjską wobec Ukrainy od 2014 roku, a w szczególności po rozpoczęciu pełnoskalowej inwazji w 2022 roku, potwierdziły, że cyberataki są integralnym elementem strategii hybrydowej, uzupełniając działania militarne, informacyjne i gospodarcze. Państwa wschodniej flanki NATO, skupione m.in. w formacie Bukaresztańskiej Dziewiątki, znalazły się w sytuacji szczególnej podatności na zagrożenia cybernetyczne, wynikającej z ich położenia geopolitycznego, roli infrastruktury krytycznej oraz zaangażowania w system bezpieczeństwa euroatlantyckiego.

Celem artykułu jest kompleksowa analiza znaczenia cyberbezpieczeństwa dla wschodniej flanki NATO w kontekście wojny rosyjsko-ukraińskiej oraz ocena zdolności państw regionu do przeciwdziałania zagrożeniom w cyberprzestrzeni. W pracy zastosowano podejście analityczno-syntetyczne, odwołujące się do paradygmatu realizmu oraz koncepcji bezpieczeństwa wielowymiarowego. Artykuł ukazuje rolę NATO i Unii Europejskiej w budowaniu odporności cybernetycznej, analizuje potencjał państw Bukaresztańskiej Dziewiątki oraz identyfikuje kluczowe wyzwania i kierunki dalszego rozwoju cyberochrony w Europie Środkowo-Wschodniej.

Słowa kluczowe: cyberbezpieczeństwo, NATO, wschodnia flanka, wojna rosyjsko-ukraińska, Bukaresztańska Dziewiątka.

Cybersecurity of NATO's eastern flank during the Russia-Ukraine war

Abstract

The Russian–Ukrainian war constitutes a turning point in the perception of cyberspace as one of the key dimensions of contemporary armed conflicts. Actions undertaken by the Russian Federation against Ukraine since 2014, and in particular following the launch of the full-scale invasion in 2022, have confirmed that cyberattacks are an integral element of hybrid strategy, complementing military, informational, and economic activities. States on NATO's eastern flank, including those cooperating within the Bucharest Nine format, have found themselves in a situation of particular vulnerability to cyber threats, resulting from their geopolitical location, the role of critical infrastructure, and their involvement in the Euro-Atlantic security system.

The aim of this article is to provide a comprehensive analysis of the significance of cybersecurity for NATO's eastern flank in the context of the Russian–Ukrainian war and to assess the capacity of the states in the region to counter threats in cyberspace. The study employs an analytical–synthetic approach, drawing on the paradigm of realism and the concept of multidimensional security. The article examines the role of NATO and the European Union in building cyber resilience, analyzes the potential of the Bucharest Nine states, and identifies key challenges as well as directions for the further development of cyber protection in Central and Eastern Europe.

Keywords: cybersecurity, NATO, eastern flank, Russian–Ukrainian war, Bucharest Nine.

Wprowadzenie

Postępująca cyfryzacja państw, społeczeństw i gospodarek sprawiła, że cyberprzestrzeń stała się jednym z kluczowych obszarów funkcjonowania współczesnego świata [1, 13, 15]. Równocześnie stała się ona nową domeną rywalizacji strategicznej, w której państwa wykorzystują narzędzia cybernetyczne do realizacji swoich interesów politycznych, militarnych i gospodarczych [3, 14, 16]. W tym kontekście cyberbezpieczeństwo przestało być wyłącznie problemem technicznym, a stało się jednym z fundamentalnych elementów bezpieczeństwa narodowego i międzynarodowego [4, 5].

Wojna rosyjsko-ukraińska unaoczniła skalę i charakter zagrożeń cybernetycznych, z jakimi mogą mierzyć się państwa zaangażowane w konflikt lub znajdujące się w jego bezpośrednim otoczeniu strategicznym [2, 28, 29]. Cyberataki stały się narzędziem destabilizacji państwa, osłabiania jego zdolności obronnych oraz oddziaływania na społeczeństwo i sojuszników [6, 7]. Państwa wschodniej flanki NATO, w tym Polska, Rumunia oraz państwa bałtyckie, znalazły się w sytuacji szczególnego ryzyka, co wymusiło intensyfikację działań na rzecz wzmocnienia odporności cybernetycznej [10, 11].

Celem niniejszego artykułu jest odpowiedź na pytanie, w jaki sposób wojna rosyjsko-ukraińska wpłynęła na postrzeganie i rozwój cyberbezpieczeństwa wschodniej flanki NATO oraz jakie znaczenie mają działania podejmowane przez NATO, Unię Europejską i państwa Bukaresztańskiej Dziewiątki dla stabilności bezpieczeństwa regionalnego 1, 12].

1. Cyberprzestrzeń jako domena współczesnych konfliktów zbrojnych

W literaturze przedmiotu cyberprzestrzeń coraz częściej traktowana jest jako pełnoprawna domena działań militarnych, porównywalna z lądem, morzem, powietrzem i przestrzenią kosmiczną [3, 7]. Rozwój technologii informacyjnych umożliwił prowadzenie operacji cybernetycznych o charakterze ofensywnym i defensywnym, których skutki mogą mieć bezpośredni wpływ na funkcjonowanie państwa oraz bezpieczeństwo międzynarodowe [14, 15].

Cyberoperacje charakteryzują się relatywnie niskim kosztem, możliwością zachowania anonimowości oraz działaniem poniżej progu wojny kinetycznej [16, 28]. Z tego względu stały się one szczególnie atrakcyjnym narzędziem dla państw dążących do realizacji celów strategicznych bez ryzyka bezpośredniej eskalacji militarnej [25, 26]. Koncepcje cyberodstraszania wskazują, że zdolność do obrony oraz do zadawania strat w cyberprzestrzeni stanowi istotny element równowagi strategicznej [15, 28].

Działania Federacji Rosyjskiej wobec Ukrainy od 2014 roku stanowią jeden z najbardziej kompleksowych przykładów zastosowania cybernarzędzi w konflikcie zbrojnym [2, 3]. Ataki na infrastrukturę energetyczną, administrację publiczną oraz sektor finansowy Ukrainy miały na celu osłabienie zdolności państwa do funkcjonowania oraz wywołanie chaosu społecznego [6, 11].

Po 2022 roku cyberataki stały się integralnym elementem działań wojennych, uzupełniając operacje kinetyczne [1, 28]. Kampanie dezinformacyjne, ataki typu DDoS oraz złośliwe oprogramowanie destrukcyjne były wykorzystywane równolegle z ofensywą militarną 14, 29]. Doświadczenia Ukrainy stanowią istotne źródło wiedzy dla państw wschodniej flanki NATO, pokazując możliwe scenariusze zagrożeń [5, 12].

2. Cyberbezpieczeństwo jako element bezpieczeństwa wschodniej flanki NATO

Państwa wschodniej flanki NATO charakteryzują się szczególną wrażliwością na zagrożenia cybernetyczne ze względu na swoje położenie geopolityczne, strukturę infrastruktury krytycznej oraz rolę w systemie bezpieczeństwa euroatlantyckiego [1, 5]. Cyberataki mogą prowadzić do paraliżu systemów energetycznych, transportowych i komunikacyjnych, co bezpośrednio wpływa na zdolności obronne Sojuszu [6, 27].

Uznanie cyberprzestrzeni za domenę operacyjną NATO stanowiło przełom w podejściu do planowania obronnego [7, 10]. Oznacza to, że cyberataki mogą być traktowane jako przesłanka do uruchomienia mechanizmów kolektywnej obrony, w tym art. 5 Traktatu Waszyngtońskiego [1, 7].

Państwa Bukaresztańskiej Dziewiątki odgrywają kluczową rolę w kształtowaniu bezpieczeństwa wschodniej flanki NATO [12, 20]. W ostatnich latach państwa te zintensyfikowały działania na rzecz rozwoju krajowych systemów cyberbezpieczeństwa, tworząc wyspecjalizowane instytucje, strategie oraz mechanizmy reagowania na incydenty [4,

11]. Szczególną rolę odgrywają państwa bałtyckie, które dzięki wcześniejszym doświadczeniom z cyberatakami stały się liderami w zakresie cyberodporności [2, 6]. Polska i Rumunia pełnią funkcję państw wiodących w regionie, zarówno pod względem potencjału instytucjonalnego, jak i znaczenia politycznego w ramach NATO [1, 5].

3. Rola NATO i Unii Europejskiej w budowaniu odporności cybernetycznej

NATO i Unia Europejska odgrywają komplementarne role w zakresie cyberbezpieczeństwa [7, 27]. NATO koncentruje się na wymiarze militarnym i strategicznym, rozwijając zdolności cyberobrony oraz mechanizmy odstraszania [1, 3]. Unia Europejska natomiast skupia się na harmonizacji regulacji prawnych, ochronie infrastruktury krytycznej oraz wsparciu państw członkowskich w budowaniu odporności systemowej [8, 9].

Współpraca NATO–UE w obszarze cyberbezpieczeństwa nabrała szczególnego znaczenia po 2022 roku, kiedy zagrożenia cybernetyczne zaczęły być postrzegane jako jedno z kluczowych wyzwań dla bezpieczeństwa całej Europy [27, 28].

Do głównych wyzwań stojących przed państwami wschodniej flanki NATO należą niedobory wysoko wykwalifikowanych specjalistów, szybkie tempo rozwoju technologii oraz rosnąca skala zagrożeń hybrydowych [13, 29]. Istotnym problemem pozostaje również konieczność integracji systemów cywilnych i wojskowych w zakresie cyberochrony [4, 17].

Perspektywy rozwoju cyberbezpieczeństwa w regionie są ściśle związane z dalszym pogłębianiem współpracy regionalnej, w tym w ramach Bukaresztańskiej Dziewiątki, oraz zacieśnianiem relacji z NATO i Unią Europejską [12, 27].

4. Cyberodstraszanie i odporność cyfrowa jako nowe filary bezpieczeństwa regionalnego

Rozwój cyberprzestrzeni jako domeny działań strategicznych doprowadził do wykształcenia nowych koncepcji bezpieczeństwa, wśród których szczególne znaczenie zyskały cyberodstraszanie oraz odporność cyfrowa [15, 28]. Cyberodstraszanie opiera się na założeniu, że potencjalny agresor powstrzyma się od działań w cyberprzestrzeni, jeżeli spodziewane koszty polityczne, militarne lub gospodarcze przewyższą możliwe korzyści [3, 7]. W odróżnieniu od klasycznego odstraszania nuklearnego lub konwencjonalnego,

cyberodstraszanie cechuje się wysokim poziomem niejednoznaczności, trudnością w atrybucji ataków oraz relatywnie niskim progiem eskalacji [14, 16].

Państwa wschodniej flanki NATO, analizując doświadczenia Ukrainy, coraz wyraźniej dostrzegają, że skuteczne cyberodstraszanie nie może opierać się wyłącznie na zdolnościach ofensywnych [2, 28]. Kluczowe znaczenie ma zdolność do szybkiego wykrywania incydentów, minimalizowania ich skutków oraz zapewnienia ciągłości funkcjonowania państwa i infrastruktury krytycznej [6, 9]. Odporność cyfrowa staje się zatem komplementarnym elementem odstraszania, wzmacniając wiarygodność całego systemu bezpieczeństwa regionalnego [1, 27].

5. Infrastruktura krytyczna jako główny cel cyberataków

Jednym z najważniejszych wniosków płynących z analizy wojny rosyjsko-ukraińskiej jest rola infrastruktury krytycznej jako głównego celu cyberataków [6, 11]. Systemy energetyczne, telekomunikacyjne, transportowe oraz finansowe stanowią fundament funkcjonowania nowoczesnych państw, a ich zakłócenie może prowadzić do paraliżu administracji publicznej i destabilizacji społecznej [8, 29].

Państwa wschodniej flanki NATO, ze względu na swoje położenie geopolityczne oraz funkcję zaplecza logistycznego Sojuszu, są szczególnie narażone na tego rodzaju zagrożenia [5, 12]. Cyberataki na infrastrukturę krytyczną mogą mieć charakter skoordynowany z działaniami kinetycznymi lub stanowić element długotrwałej presji strategicznej prowadzonej poniżej progu wojny [3, 27]. W tym kontekście kluczowe znaczenie ma harmonizacja standardów ochrony infrastruktury krytycznej w ramach Unii Europejskiej oraz NATO [8, 10].

6. Edukacja, kapitał ludzki i innowacje technologiczne

Jednym z najpoważniejszych wyzwań dla cyberbezpieczeństwa państw wschodniej flanki NATO pozostaje deficyt wysoko wykwalifikowanych specjalistów [13, 29]. Dynamiczny rozwój technologii, w tym sztucznej inteligencji, uczenia maszynowego oraz Internetu Rzeczy, powoduje, że zapotrzebowanie na ekspertów ds. cyberbezpieczeństwa rośnie szybciej niż możliwości systemów edukacyjnych [15, 28].

Państwa Bukaresztańskiej Dziewiątki podejmują coraz bardziej zróżnicowane działania w tym obszarze, rozwijając programy kształcenia akademickiego, szkolenia dla administracji publicznej oraz współpracę z sektorem prywatnym [4, 11]. Inwestycje w kapitał ludzki należy postrzegać jako element długofalowej strategii bezpieczeństwa, którego znaczenie jest porównywalne z modernizacją sił zbrojnych [17, 25].

7. Współpraca regionalna w ramach Bukaresztańskiej Dziewiątki

Format Bukaresztańskiej Dziewiątki, mimo że nie posiada sformalizowanych struktur instytucjonalnych, odgrywa istotną rolę w koordynacji stanowisk państw wschodniej flanki NATO w zakresie bezpieczeństwa, w tym cyberbezpieczeństwa [12, 20]. Regularne konsultacje polityczne oraz wymiana doświadczeń umożliwiają lepsze dostosowanie polityk narodowych do wyzwań regionalnych [5, 17].

W kontekście cyberbezpieczeństwa B9 może pełnić funkcję platformy integrującej działania państw regionu, zwłaszcza w obszarze ochrony infrastruktury krytycznej, reagowania na incydenty oraz przeciwdziałania dezinformacji [2, 6]. Wzmocnienie współpracy w tym formacie mogłoby przyczynić się do zwiększenia spójności działań NATO na wschodniej flance [1, 27].

8. Cyberbezpieczeństwo a art. 5 Traktatu Waszyngtońskiego

Jednym z kluczowych problemów teoretycznych i praktycznych pozostaje kwestia zastosowania art. 5 Traktatu Waszyngtońskiego w odpowiedzi na cyberatak [1, 7]. Brak jednoznacznych kryteriów określających, kiedy cyberatak może zostać uznany za zbrojną napaść, powoduje, że cyberprzestrzeń pozostaje obszarem strategicznej niejednoznaczności [3, 26].

Z perspektywy państw wschodniej flanki NATO szczególnie istotne jest wypracowanie wspólnych procedur reagowania na poważne incydenty cybernetyczne, które mogłyby zagrozić bezpieczeństwu całego Sojuszu [27, 28]. W tym kontekście kluczową rolę odgrywa współpraca polityczna oraz ćwiczenia symulacyjne prowadzone w ramach NATO [7, 10].

9. Znaczenie wojny rosyjsko-ukraińskiej dla przyszłości bezpieczeństwa Europy

Wojna rosyjsko-ukraińska ma charakter przełomowy nie tylko z perspektywy bezpieczeństwa regionalnego, lecz także globalnego porządku międzynarodowego [25, 26]. Cyberprzestrzeń stała się trwałym elementem rywalizacji mocarstw, a jej znaczenie będzie rosło wraz z postępującą cyfryzacją społeczeństw i gospodarek 14, 15].

Dla państw wschodniej flanki NATO konflikt ten stanowi impuls do przyspieszenia reform w obszarze cyberbezpieczeństwa oraz do pogłębienia współpracy regionalnej i transatlantyckiej [1, 12]. Doświadczenia Ukrainy pokazują, że brak odpowiedniej odporności cyfrowej może prowadzić do eskalacji kryzysów i osłabienia zdolności obronnych państwa [2, 28].

Wnioski

Cyberbezpieczeństwo wschodniej flanki NATO w obliczu wojny rosyjsko-ukraińskiej należy postrzegać jako jeden z kluczowych wymiarów współczesnego bezpieczeństwa regionalnego i międzynarodowego [1, 7]. Analiza przeprowadzona w artykule wskazuje, że cyberprzestrzeń stała się trwałym polem rywalizacji strategicznej, a jej znaczenie będzie rosło w nadchodzących dekadach [15, 25].

Państwa Bukaresztańskiej Dziewiątki, działając w ramach NATO i Unii Europejskiej, posiadają potencjał do budowy spójnego systemu cyberbezpieczeństwa, który może skutecznie wzmacniać odstraszanie i odporność wschodniej flanki Sojuszu [12, 27]. Warunkiem powodzenia tych działań jest dalsza integracja polityk narodowych, inwestycje w kapitał ludzki oraz konsekwentne traktowanie cyberbezpieczeństwa jako elementu strategicznego bezpieczeństwa państwa i regionu 4, 17, 29].

Bibliografia

1. NATO, *NATO 2022 Strategic Concept*, Madryt 2022.
2. ENISA, *ENISA Threat Landscape 2023*, Ateny 2023.
3. NATO CCDCOE, *Cyber Operations and the Use of Force*, Tallinn 2021.
4. Ministerstwo Obrony Narodowej RP, *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Warszawa 2022.
5. Polski Instytut Spraw Międzynarodowych, *Cyberbezpieczeństwo Polski i wschodniej flanki NATO*, Warszawa 2023.
6. ENISA, *Cybersecurity and Resilience of Critical Infrastructure*, Ateny 2022.
7. NATO CCDCOE, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge 2017.
8. Komisja Europejska, *Dyrektywa NIS2*, Bruksela 2022.
9. Komisja Europejska, *EU Cybersecurity Strategy for the Digital Decade*, Bruksela 2020.
10. NATO, *Cyber Defence Pledge*, Bruksela 2016.
11. Ministerstwo Cyfryzacji RP, *Krajowy System Cyberbezpieczeństwa – założenia i funkcjonowanie*, Warszawa 2021.
12. Polski Instytut Spraw Międzynarodowych, *Współpraca regionalna w Europie Środkowej po agresji Rosji na Ukrainę*, Warszawa 2024.
13. Bógdał-Brzezińska A., *Cyberbezpieczeństwo państwa*, Warszawa 2019.
14. Klimburg A., *The Darkening Web: The War for Cyberspace*, New York 2017.
15. Nye J., *Cyber Power*, Cambridge 2010.
16. Kuehl D., *From Cyberspace to Cyberpower*, Washington 2009.
17. Zenderowski R., *Europa Środkowo-Wschodnia w XX i XXI wieku*, Warszawa 2018.
18. Świder K., *Europa Środkowo-Wschodnia w myśli geopolitycznej XX wieku*, Warszawa 2018.
19. Eberhardt P., *Europa Środkowa jako region geopolityczny*, Warszawa 2005.

20. Gizicki W., Łoś P., *Geopolityka Trójmorza*, Przestrzeń Społeczna 2019.

21. Kurečić P., *The Three Seas Initiative: Geographical Determinants and Geopolitical Foundations*, Hrvatski Geografski Glasnik 2018.

22. Bieńczyk-Missala A., *Od Międzymorza do Trójmorza – meandry polityki zagranicznej Polski*, Stosunki Międzynarodowe 2018.

23. Melissen J., *The New Public Diplomacy*, London 2005.

24. Druckman D., Wallensteen P., *Negotiating with Leaders*, London 2016.

25. Cohen S., *Geopolitics: The Geography of International Relations*, Lanham 2015.

26. Mackinder H.J., *Democratic Ideals and Reality*, London 1919.

27. Rada Unii Europejskiej, *EU–NATO Cooperation on Cybersecurity*, Bruksela 2022.

28. RAND Corporation, *Cyber Deterrence and Stability*, Santa Monica 2020.

29. World Economic Forum, *Global Cybersecurity Outlook*, Geneva 2023.

Anna Kowalczyk

Wyższa Szkoła Kształcenia Zawodowego we Wrocławiu

https://orcid.org/0009-0001-4157-089X

Agnieszka Doskocz

Leoxr Sp. z o.o. w Radomiu

https://orcid.org/0009-0003-0453-6857

Jacek Doskocz

Leoxr Sp. z o.o. w Radomiu

https://orcid.org/0000-0002-5299-2465

Analiza przedstawiania ataków dronów w kontekście wojny Rosyjsko-Ukraińskiej na platformie YouTube – perspektywa propagandy, wizualizacji i cyfrowej mobilizacji

Streszczenie

Konflikt rosyjsko-ukraiński (2022–2025) stanowi paradygmat wojny cyfrowej (digital war), w której kluczowym elementem stała się triada technologiczna: media społecznościowe, cyfrowy crowdfunding i komercyjne drony. Celem niniejszego artykułu jest analiza sposobów wizualnego i narracyjnego przedstawiania ataków dronów na polu bitwy w materiałach wideo publikowanych na platformie YouTube, z naciskiem na ich rolę w strategicznej komunikacji i mobilizacji zasobów. Badanie, oparte na analizie treści wideo (2021-2024), identyfikuje dominujące wzorce wizualne oraz techniki propagandowe. Materiały te, często rejestrowane w wysokiej rozdzielczości z użyciem cyfrowego zoomu, tworzą „perspektywę oka Boga" (God's-eye view), która sprzyja postrzeganiu walki jako technicznego, moralnie zdystansowanego aktu, co jest spójne z mechanizmami dehumanizacji wroga (np. określeniami „foreign animal hunter" lub „ukronaziści"). Kwestia ta jest kluczowa, ponieważ wojna jest prowadzona również

w sferze medialnej, gdzie widzowie są aktywnie zaangażowani i zmotywowani do pomocy finansowej (crowdfundingiem) oraz do przekazywania informacji, co wspiera politykę państwa i buduje poparcie dla działań militarnych. To zaangażowanie przekształca się w pieniądze, które są wykorzystywane do zakupu i uzbrajania kolejnych dronów FPV, tworząc samo-wzmacniający się cykl pozytywnego sprzężenia zwrotnego (*self-reinforcing positive feedback cycle*) [1,2]. W ten sposób treści wideo stają się walutą, napędzającą machinę wojenną i kształtującą globalną percepcję konfliktu [3,4],. Badanie podkreśla, że mediacyjne funkcje platformy, takie jak gromadzenie archiwów i mobilizacja poparcia, stają się równie istotne, jak ich funkcja jako kanału propagandy i dezinformacji.

Słowa kluczowe: drony, YouTube, wojna rosyjsko-ukraińska, propaganda wizualna, mediatyzacja, crowdfunding, wojna partycypacyjna.

Analysis of the portrayal of drone strikes in the context of the Russian-Ukrainian war on YouTube – the perspective of propaganda, visualization, and digital mobilization

Abstract

The Russian-Ukrainian conflict (2022–2025) represents a paradigm of digital war, in which a technological triad has become a key element: social media, digital crowdfunding, and commercial drones. The aim of this article is to analyze the ways in which drone attacks on the battlefield are presented visually and narratively in video materials published on the YouTube platform, with emphasis on their role in strategic communication and resource mobilization. The study, based on video content analysis (2021-2024), identifies dominant visual patterns and propaganda techniques. These materials, often recorded in high resolution using digital zoom, create a "God's-eye view" perspective, which facilitates the perception of combat as a technical, morally distanced act, consistent with mechanisms of enemy dehumanization (e.g., terms such

as "foreign animal hunter" or "ukronazis"). This issue is crucial, because war is also being waged in the media sphere, where viewers are actively engaged and motivated to provide financial assistance (through crowdfunding) and to share information, which supports state policy and builds support for military operations. This engagement translates into money that is used to purchase and arm successive FPV drones, creating a self-reinforcing positive feedback cycle. In this way, video content becomes a currency, driving the war machine and shaping global perception of the conflict. The study emphasizes that the mediating functions of the platform, such as archival collection and mobilization of support, become as important as their function as a channel for propaganda and disinformation.

Keywords: drones, YouTube, Russian-Ukrainian war, visual propaganda, mediatization, crowdfunding, participatory warfare.

Wprowadzenie: wojna jako spektakl i proces partycypacyjny

Współczesny konflikt rosyjsko-ukraiński jest powszechnie określany jako najbardziej zmediatyzowane i udokumentowane wydarzenie w historii, charakteryzujące się wszechobecnością treści generowanych przez użytkowników (UGC) [5]. Rozwój cyfrowy (tzw. Digital Turn) umożliwił jednostkom, wyposażonym w smartfony i dostęp do platform cyfrowych, stanie się zarówno głównymi dokumentalistami wojny, jak i jej głównymi odbiorcami [5].

Centralnym elementem tej transformacji jest bezprecedensowe wykorzystanie dronów (UAV), w tym tanich, komercyjnych dronów FPV, które stały się narzędziem integrującym walkę kinetyczną z wojną informacyjną. Jak ujęto w literaturze, jest to "wojna cyfr" (war of digits), w której stuknięcie w ekran może aktywować zrzut granatu z drona, stanowiąc ostateczną integrację walki kinetycznej i informacyjnej [6],[7].

W kontekście analizy treści wideo z dronów na YouTube, kluczowe jest zrozumienie, że platforma ta pełni funkcję wykraczającą poza zwykłe archiwum czy kanał informacyjny. Jest

to arena wojny partycypacyjnej (participative warfare), w której granice między pokojowymi obywatelami (quīritēs) a walczącymi żołnierzami (mīlitēs) ulegają zatarciu, a społeczeństwo jest aktywnie wciągane w konflikt[8],[9],[10]. W tej nowej ekologii wojennej, widzowie nie są biernymi obserwatorami; są czynnie angażowani i motywowani do wspierania wysiłku wojennego na wielu poziomach.

2. Cyfrowa mobilizacja: triada mediów, crowdfundingu i dronów

Wojna w domenie cyfrowej jest strategicznie prowadzona nie tylko w celu zniszczenia przeciwnika na froncie, ale także w celu uzyskania i utrzymania wsparcia globalnej i krajowej publiczności. Spektakularne materiały z ataków dronów są centralnym elementem tego procesu mobilizacyjnego, wpływając na politykę, finanse i morale.

2.1. Angażowanie widzów i wzmacnianie linii frontu (crowdfunding)

Najważniejszą formą zaangażowania publiczności w mediach społecznościowych jest cyfrowy crowdfunding, który stał się "finansową bronią wojny" [11,12]. Zjawisko to, napędzane globalnymi horyzontalnymi sieciami platform mediów społecznościowych i systemów płatności online, umożliwia cywilom na całym świecie bezpośrednie wspieranie jednostek wojskowych [13],[14],[15].

Mechanizm Sprzężenia Zwrotnego: Filmy z dronów, często ukazujące ich śmiertelną skuteczność, są rutynowo udostępniane przez jednostki wojskowe lub mil-blogerów w celu:

◦ Uzasadnienia wydatków: Filmy służą jako dowód, że zebrane fundusze są dobrze wykorzystywane, co przyciąga kolejnych darczyńców [16],[17].

◦ Wzmacniania cyklu wsparcia: Cykl ten, opisany jako pętla pozytywnego sprzężenia zwrotnego, polega na tym, że udany materiał wideo stymuluje dalsze datki, co prowadzi do zakupu i uzbrojenia większej liczby dronów FPV, które następnie generują nowy, emocjonalny kontent[18],[19].

Personalizacja Aktu Zabijania: Elementy recepcji społecznej są celowo wykorzystywane do zwiększenia zaangażowania. W literaturze zauważono, że drony są często nazywane imieniem sponsora lub na ich amunicji umieszczane są osobiste, śmiertelne wiadomości od darczyńców (np. „T90 go BOOM" lub „Love from Odessa"), co personalizuje i wciąga widza w akt walki [20]. [21].

Skala Zjawiska: Choć część darowizn trafia przez oficjalne platformy, ogromna ilość środków jest zbierana przez pośredników i przekazywana bezpośrednio jednostkom frontowym, często poza kontrolą tradycyjnej hierarchii wojskowej [22],[23],[24],[25].

2.2. Kształtowanie polityki i promocja strategiczna

Wojna w mediach ma bezpośredni wpływ na politykę wewnętrzną i zewnętrzną. Wizualizacje z dronów są wykorzystywane jako potężne narzędzie w strategicznej komunikacji [27]:

- Wpływ na Poparcie Międzynarodowe: Kampania informacyjna, transmitująca sukcesy ukraińskie na polu bitwy, jest kluczowa dla utrzymania międzynarodowego wsparcia i dostaw broni [28,29,30]. W ten sposób sukces na polu bitwy kształtuje strategię darczyńców, zamiast odwrotnie [31, 30],. Udane akcje dronów, dokumentowane i udostępniane w mediach, są "przekazywane" zachodnim wyborcom jako dowód, na co zostały przeznaczone ich pieniądze i dlaczego dalsze wsparcie jest potrzebne [31, 29, 30].
- Budowanie Grupy Wyborców i Wpływ na Politykę Wewnętrzną: Choć bezpośredni związek z budowaniem grupy wyborców w kontekście polskiej ankiety nie jest badany w źródłach, ogólna strategia dezinformacji ma udokumentowany wpływ na procesy demokratyczne i politykę [32], [33]. W kontekście ukraińskim, cyfrowa mobilizacja i uczestnictwo w dyskursie wojennym prowadzi do zatarcia granic między żołnierzem a cywilem [34],[35],[36]. Obywatele, którzy angażują się w infowar i aktywizm (np. poprzez dotacje i przekazywanie informacji), stają się uczestnikami [36],[37], a ich

zaangażowanie jest wykorzystywane do promowania i legitymizowania krajowej polityki obronnej, co jest procesem centralnie zachęcanym przez władze [4].

3. Wizualność i narracja jako waluta zaangażowania

Wideo z ataków dronów na YouTube jest podstawowym produktem informacyjnym, który generuje opisaną wyżej partycypację i fundusze.

3.1. Estetyka ataku i dehumanizacja

Ujęcia z dronów są skonstruowane komunikacyjnie tak, aby maksymalizować efekt propagandowy [38]. Analiza treści ujawnia trzy dominujące typy ujęć [39]:

- Ujęcia Rozpoznawcze i Panoramika: Często prezentują „perspektywę oka Boga" (God's-eye view) [40], zapewniając szeroki widok pola bitwy. Chociaż ta perspektywa może obniżać psychologiczne obciążenie związane z zabijaniem, pokazując ofiary jako zdystansowane sylwetki [41],[40], to jednocześnie intymne zbliżenia w jakości 4K FHD, z użyciem nawet 56-krotnego zoomu cyfrowego, ujawniają „nieskrępowane i całkowite okrucieństwo" pola walki [42],[43],[44].

- Ujęcia Ataku i Efektu Trafienia: Są to sekwencje montażowe wzmocnione dramaturgią (muzyką, slow motion i powtórkami), upodabniające sceny walki do estetyki gier wideo [45],[46],[47]. W narracji towarzyszącej tym wizualizacjom stosuje się techniki propagandowe, takie jak Osłanianie Etykietami (Name Calling), polegające na odczłowieczaniu wroga. Przykładowo, rosyjski dron Lancet został nazwany „foreign animal hunter" (zagraniczny łowca zwierząt) [48],[49],[50]. Stosuje się również technikę Transferu (Transfer), gdzie umieszczenie ukraińskiej flagi w zasięgu ataku drona symbolicznie przedstawia całe państwo jako legalny cel wojenny, godny zniszczenia [51], [50].

3.2. Podwójna rola wideo: propaganda i kontrola

Drony nie tylko generują propagandę wymierzoną w przeciwnika, ale też mają potencjał do „nadzorowania wydajności bojowej własnych żołnierzy" [52],[53]. W warunkach nowoczesnej, profesjonalnej wojny, dowództwo, siedzące za ekranami, zyskuje możliwość bezpośredniej, optycznej i w czasie rzeczywistym kontroli manewrów, efektywności ostrzału i dyscypliny podległych jednostek [54]. Choć w kontekście ukraińskim ta opresyjna funkcja jest minimalizowana [55], to perspektywa "wszechwidzącego oka" drona ma potencjał do narzucenia mobilnej kontroli nad własnymi oddziałami [52],[56].

Co więcej, wszechobecność wideo z frontu na platformach społecznościowych, nawet jeśli są to nagrania wroga, pozwala na "podwójny mechanizm sprawdzający" zachowanie własnych żołnierzy, gdyż ich błędy stają się publicznie dostępne [57].

4. Psychologiczne i społeczne skutki cyfrowego spektaklu

Intensywny obieg materiałów wojennych ma głębokie konsekwencje dla odbiorców i uczestników konfliktu.

4.1. Hierarchia partycypacji i erozyjne działanie mediów

Wojna partycypacyjna ustanawia hierarchię zaangażowania [58]. Obejmuje ona różne poziomy: od pasywnego widza (uciekiniera z Nowej Zelandii) [59], przez zaangażowanie w infowar i aktywizm (NAFO, darczyńcy), po ochotników i żołnierzy w walce kinetycznej, ponoszących największe ryzyko [59].

Dla masowego odbiorcy, nadmiar treści medialnych może prowadzić do „znużenia współczuciem" (compassion fatigue) [60] lub „emocjonalnej znieczulicy". Zjawisko to, opisywane jako „efekt Húrina", polega na paraliżującej, bezsilnej obserwacji cierpienia, w której widzowie, choć zaangażowani w obieg informacji, pozostają bierni i ulegają „fałszywemu poczuciu aktywności" [34],[61],[62],[63]. Pomimo heroizmu i jedności

pokazywanej w niektórych materiałach [64],[65], ostatecznie chroniczne bombardowanie sprzecznymi informacjami może prowadzić do obojętności [66].

4.2. Ryzyko dezinformacji i manipulacji

Dominacja treści UGC w mediach społecznościowych w połączeniu z modelem rosyjskiej propagandy „firehose of falsehood" (potok fałszu) – charakteryzującym się dużą objętością, szybkością i brakiem spójności z obiektywną rzeczywistością [67],[68],[69],[14] – stwarza warunki do manipulacji i osłabienia krytycznego myślenia [70],[71].

Fałszywe obrazy i narracje związane z dronami są intensywnie wykorzystywane w celach propagandowych [72]. Choć większość fałszerstw jest prosta (dekontekstualizacja obrazów) [73], są one dystrybuowane w celu wpływania na globalną opinię publiczną i podważania legitymacji działań [74]. W ten sposób walka o uwzględnienie polityki jest prowadzona równolegle z walką kinetyczną.

5. Wnioski

Analiza wizualnego i narracyjnego przedstawiania ataków dronów na YouTube potwierdza, że platformy społecznościowe są obecnie integralnym elementem prowadzenia wojny, służąc zarówno celom kinetycznym (poprzez dostarczanie informacji w czasie rzeczywistym i środków finansowych), jak i strategicznym (poprzez budowanie poparcia politycznego i finansowego).

1. Cykl finansowania i partycypacji: Filmy z dronów stanowią kluczową walutę w cyfrowym obiegu, mobilizując globalną widownię do pomocy finansowej (crowdfundingu) na skalę przemysłową [11],[4]. To zaangażowanie cywilów w dostarczanie środków i informacji zaciera tradycyjne granice między cywilem a żołnierzem [34].

2. Narracja i wpływ polityczny: Propagandowe przedstawienie ataków dronów (bohaterstwo, techniczna wyższość, dehumanizacja) jest strategicznie wykorzystywane do kierowania promocji polityki i utrzymywania poparcia, szczególnie w krajach zachodnich, gdzie oczekuje się widocznych sukcesów militarnych w zamian za wsparcie finansowe [31],[30].

3. Wizualny reżim dominacji: Wizualizacje z dronów, oferujące perspektywę God's-eye view i intymne zbliżenia, mogą być nie tylko bronią, ale też narzędziem nadzoru nad własnymi wojskami [52] oraz przyczyniają się do normalizacji przemocy i erozji krytycznego myślenia u odbiorców (efekt Húrina) [62],[63].

W epoce wojny cyfrowej zrozumienie, w jaki sposób technologia wizualna aktywnie kształtuje wsparcie polityczne i mechanizmy finansowania konfliktu, jest niezbędne dla bezpieczeństwa informacyjnego.

Bibliografia

1. Abdulrazek, S. “Turkey Continues its Drone War in Northern Syria.” *Asharq Al-Awsat*, 5 August 2022. https://english.aawsat.com/home/article/3799211/turkey-continues-its-drone-war-northern-syria.

2. Abushbak, A.M., T. Majeed, & K.S. Kusuma. “Mobile Phone Activism During Israel’s ‘Operation Guardian of the Wall’ in Gaza.” *Media, War & Conflict* 00, no. 0 (2024): 1–18. https://doi.org/10.1177/17506352241249063.

3. Agamben, Giorgio. *What is an Apparatus? and Other Essays*. Stanford: Stanford University Press, 2019.

4. Agostinho, Daniela, Simon Gade, Nanna B. Thylstrup, & Kristin Veel, eds. *(W)archives: Archival Imaginaries, War, and Contemporary Art*. Berlin: Sternberg Press, 2020.

5. Allinson, J. “The Necropolitics of Drones.” *International Political Sociology* 9, no. 2 (2015): 113–127. https://doi.org/10.1177/1749568215582312.

6. Amnesty International. “Amnesty International investigation concludes Israel is commiting genocide against Palestinians in Gaza.” Last modified 2024. https://www.amnesty.org/en/latest/news/2024/12/amnesty-international-concludes-israel-is-committing-genocide-against-palestinians-in-gaza/.

7. Archambault, Étienne, & Yannick Veilleux-Lepage. “Drone imagery in Islamic State propaganda: flying like a state.” *International Affairs* 96, no. 4 (2020): 955–973. doi: 10.1093/ia/iiaa014.

8. Asaro, P.M. “The labor of surveillance and bureaucratized killing: new subjectivities of military drone operators.” *Social Semiotics* 23, no. 2 (2013): 196–224.

9. Associated Press. “Live Updates: Zelenskyy Declines US Offer to Evacuate Kyiv,” 26 February 2022. https://apnews.com/article/russia-ukraine-business-europe-united-nations-kyiv-6ccba0905f1871992b93712d3585f548.

10. Azarova, V. “Israel’s Unlawfully Prolonged Occupation: Consequences Under an Integrated Legal Framework.” European Council on Foreign Relations, 2 June 2017. https://ecfr.eu/publication/israels_unlawfully_prolonged_occupation_7294/.

11. BAE Systems. *ARGUS-IS Brochure*. Columbia, MD: BAE Systems, 2013.

12. Bergen, Peter, Marisa Salyk-Virk, & David Sterman. *The World of Drones Database*. New America, 2020. https://www.newamerica.org/international-security/reports/world-drones/.

13. Bevir, M., & R.A.W. Rhodes, eds. *Routledge Handbook of Interpretive Political Science*. London: Routledge, 2016.

14. Bleiker, Roland. "Mapping visual global politics." In *Visual Global Politics*, edited by Roland Bleiker, 1–29. London: Routledge, 2018.

15. Boichak, O., & A. Hoskins. "My War: Participation in Warfare." *Digital War* 3 (2022): 1–8. https://doi.org/10.1057/s42984-022-00060-7.

16. Bousquet, Antoine. *The Eye of War: Military Perception from the Telescope to the Drone*. Minneapolis: University of Minnesota Press, 2018.

17. Boyko, Kateryna, & Roman Horbyk. "Swarm Communication in a Totalizing War: Media Infrastructures, Actors and Practices in Ukraine during the 2022 Russian Invasion." In *Media and the War in Ukraine*, edited by Mervi Pantti & Mette Mortensen, 37–56. New York: Peter Lang, 2023.

18. Bregman, Ahron. *Israels Wars: A History since 1947*. 4th ed. Milton Park, Abingdon, Oxon; New York, N.Y.: Routledge, 2016.

19. Chayka, K. "Watching the World's First TikTok War." *The New Yorker*, 3 March 2022. https://www.newyorker.com/culture/infinite-scroll/watching-the-worlds-first-tiktok-war.

20. Chouliaraki, Lilie. "The Humanity of War: Iconic Photojournalism of the Battlefield." In *Visual Security Studies: Sights and Spectacles of Insecurity and War*, edited by J. Vuori & R. Saugmann, 71–90. Routledge, 2018.

21. Crilley, R. "Seeing Syria: The Visual Politics of the National Coalition of Syrian Revolution and Opposition Forces on Facebook." *Middle East Journal of Culture and Communication* 10, no. 2–3 (2017): 133–158. https://doi.org/10.1163/18739865-01002004.

22. Danchev, Alex. "Witnessing." In *Visual Global Politics*, edited by Roland Bleiker, 332–338. London: Routledge, 2018.

23. Der Derian, James. “War.” In *Visual Global Politics*, edited by Roland Bleiker, 328–331. London: Routledge, 2018.

24. El Zein, H., & A. Abusalem. “Social Media and War on Gaza: A Battle on Virtual Space to Galvanise Support and Falsify Israel Story.” *Athens Journal of Mass Media and Communications* 1, no. 2 (2015): 109–120. DOI:10.30958/ajmmc.1-2-2.

25. Ford, Matthew. “From Innovation to Participation: connectivity and the conduct of contemporary warfare.” *International Affairs* 100, no. 4 (2024): 1531–1549. https://doi.org/10.1093/ia/iiae061.

26. Ford, Matthew. “Ukraine, Participation and the Smartphone at War.” *Political Anthropological Research on International Social Sciences* (2023): 1–29. https://doi.org/10.1163/25903276-bja10048.

27. Ford, Matthew, & Andrew Hoskins. *Radical War: Data, Attention and Control in the 21st Century*. Oxford: Oxford University Press, 2022.

28. General Atomics. *Predator C ‘Avenger’ UAV*, promotional video, 2009. www.youtube.com/watch?v=v0dHKWjXn-E.

29. Global Initiative Against Transnational Organized Crime. “A New Paradigm for Organized Crime: Crime by Drone.” Geneva: Global Initiative Against Transnational Organized Crime, 2025. https://globalinitiative.net/wp-content/uploads/2025/10/GI-TOC-Crime-by-Drone_revised-version.pdf.

30. Grossman, Dave. *On Killing: The Psychological Cost of Learning to Kill in War and Society*. New York: Back Bay Books, 1996.

31. Hoskins, Andrew, & Peter Shchelin. “The War Feed: Digital War in Plain Sight.” *American Behavioral Scientist* 67, no. 3 (2023): 449–463. https://doi.org/10.1177/00027642221144848.

32. Human Rights Watch. “October 7th Crimes Against Humanity, War Crimes by Hamas-led Groups.” Last modified 2024. https://www.hrw.org/news/2024/07/17/october-7-crimes-against-humanity-war-crimes-hamas-led-groups.

33. International Human Rights and Conflict Resolution Clinic at Stanford Law School and Global Justice Clinic at NYU School of Law. *Living Under Drones: Death, Injury, and Trauma to Civilians from US Drone Practices in Pakistan*. 2012. https://www-cdn.law.stanford.edu/wp-content/uploads/2015/07/Stanford-NYU-Living-Under-Drones.pdf.

34. Jones, Craig. "Shooting Gaza: Israel's Visual War." *Human Geography* 4, no. 1 (2011): 38–56. https://doi.org/10.1177/194277861100400104.

35. Jünger, Ernst. *Storm of Steel*. Translated by Michael Hofmann. New York: Penguin Books, 2017.

36. Jünger, Ernst. "Total Mobilization." In *The Heidegger Controversy*, edited by Richard Wolin, 119–139. Cambridge, MA: MIT Press, 1993.

37. Kaempf, Sebastian. "Digital Media." In *Visual Global Politics*, edited by Roland Bleiker, 99–103. London: Routledge, 2018.

38. Kindervarter, K.H. "The Emergence of Lethal Surveillance: Watching and Killing in the History of Drone Technology." *Security Dialogue* 47, no. 3 (2016): 223–238. https://doi.org/10.1177/0967010615616011.

39. Kittler, Friedrich. *Optical Media: Berlin Lectures 1999*. Cambridge: Polity, 2019.

40. Korać, Srđan T. "Is Drone Becoming the New 'Apparatus of Domination'?: Battlefield Surveillance in the Twenty-First Century Warfare." *Filozofija i Drustvo* 34, no. 3 (2023): 377–398. https://doi.org/10.2298/FID2303377K.

41. López-Cantos, Francisco. "The drone warfare. Fact-checking, fake-pictures and necropolitics." *Cogent Social Sciences* 10, no. 1 (2024): 1–18. https://www.tandfonline.com/doi/full/10.1080/23311886.2024.2426706.

42. Manor, I., & R. Crilley. "Visually Framing the Gaza War of 2014." *Media, War & Conflict* 11, no. 4 (2018): 369–391. https://www.jstor.org/stable/10.2307/26976773.

43. Mazzetti, Mark. "The Drone Zone." *The New York Times*, 6 July 2012. http://www.nytimes.com/2012/07/08/magazine/the–drone–zone.html.

44. Méheut, Constant, & Daria Mitiuk. "Crowdfunding, Auctions and Raffles: How Ukrainians are Aiding the Army." *New York Times*, 7 March 2024.

45. Merrin, William. *Digital War: A Critical Introduction*. London: Routledge, 2019.

46. Möller, Frank. “Witnessing Violence Through Photography.” *Global Discourse* 7, no. 2–3 (2017): 264–281. http://dx.doi.org/10.1080/23269995.2017.1339979.

47. O’Loughlin, Ben, & Andrew Hoskins. *War and Media: The emergence of diffused war*. Cambridge England: Polity, 2010.

48. PBS. *NOVA: Rise of the Drones*. Documentary, 2013. https://www.youtube.com/watch?v=IOzCiCl05Ec.

49. Patrikarakos, David. *War in 140 Characters: How Social Media is Reshaping Conflict in the Twenty-First Century*. New York: Basic Books, 2017.

50. Peregrine, S., & D. Yanow. *Interpretive Research Design. Concepts and Processes*. New York: Routledge, 2012.

51. Pleska, Anna, Andrew Hoskins, & Kjersti Renaud. “A Framework for Interrogating Social Media Images to Reveal an Emergent Archive of War.” *International Journal of Humanities and Arts Computing* 13, no. 1–2 (2019): 196–222. https://www.euppublishing.com/doi/full/10.3366/ijhac.2019.0236.

52. Rose, Gillian. *Visual Methodologies: An Introduction to Researching with Visual Materials*. 4th ed. Sage Publications, 2016.

53. Schiffer, Zoë. “Elon Musk attacked my article accusing him of gaming Twitter’s algorithm for more attention. In some ways, it gave him exactly what he wanted.” *Business Insider*, 15 February 2024. https://www.businessinsider.com/musk-changed-twitter-algorithm-tweets-didnt-get-attention-book-20

24-2.

54. Segate, R.V. “Channeled Beneath International Law: Mapping Infrastructure and Regulatory Capture as Israeli-American Hegemonic Reinforcers in Palestine.” *Communication Law and Policy* 28, no. 4 (2023): 332–366. https://doi.org/10.1080/10811680.2024.2334081.

55. Singer, Peter W. “The Soldiers Call It War Porn.” *Spiegel Online*, 12 March 2010. http://www.spiegel.de/international/world/interview–with–defense–expert–p–w–singer–thesoldiers–call–it–war–porn–a–682852.html.

56. Singer, Peter W., & Emerson T. Brooking. *LikeWar: The Weaponization of social media*. New York: Mariner Books, 2019.

57. Sontag, Susan. *Regarding the Pain of Others*. London: Penguin Books, 2003.

58. Spansvoll, Runar. "The Weaponisation of Social Media, Crowdfunding and Drones: A People's War in the Digital Age." *The RUSI Journal* 169, no. 1-2 (2024): 46–60. https://doi.org/10.1080/03071847.2024.2350478.

59. Tawil-Souri, Helga. "Digital Occupation: Gaza's High-Tech Enclosure." *Journal of Palestine Studies* 41, no. 2 (2012): 27–43. https://doi.org/10.1525/jps.2012.XLI.2.27.

60. Tivadar, L.M. "The Gaza Strip and the Israel-Hamas Conflict: From 2008 until Nowadays." *Acta Musei Napocensis* 58/II (2021): 293–311. DOI: https://doi.org/10.54145/ActaMN.

61. Virilio, Paul. *War and Cinema: The Logistics of Perception*. Translated by Patrick Camiller. London: Verso, 1989.

62. Webb, D., L. Wirbel, & B. Sulzmann. "From Space, No One Can Watch You Die." *Peace Review: A Journal of Social Justice* 22, no. 1 (2010): 31–39.

63. Yarchi, M., & L. Boxman-Shabtai. "The Image War Moves to TikTok Evidence from the May 2021 Round of the Israeli-Palestinian Conflict." *Digital Journalism* (2023). https://doi.org/10.1080/21670811.2023.2291650

BezpieczenstwoNarodowe.pl