

Cybersecurity and Law

2025 Nr 1(13)

DOI: 10.35467/cal/214604



GNSS Jamming – idea, technical aspects and legal context

Zakłócanie GNSS – idea, aspekty techniczne i uwarunkowania prawne

Grzegorz STACH

Marynarka Wojenna

ORCID: 0009-0007-5720-4353

E-mail: stachgrzegorz@yahoo.co.uk

Dariusz ZMYŚŁOWSKI

Instytut Systemów Łączności, Wydział Elektroniki, Wojskowa Akademia Techniczna

ORCID: 0000-0002-1214-1308

E-mail: dariusz.zmyslowski@wat.edu.pl

Abstract

Navigation using global navigation satellite systems (GNSS) is widely available and widely used. Disturbances in navigation signals are caused by natural phenomena (e.g., atmospheric activity or the Sun's activity, cosmic radiation), electromagnetic signal propagation, and environmental influences (e.g., multipath propagation). Intentional and harmful interference with GNSS signals through jamming, spoofing, or meaconing is common and constitutes a component of hostile activity, particularly in asymmetric and hybrid operations. This study focuses on intentional GNSS interference, detailing its technical characteristics, classification, effects, and legal issues. It also presents measurement results of such interference from the Gulf of Gdańsk region. The following research methods were used to achieve this goal: analysis of knowledge sources, expert interviews, field measurements, and synthesis and inference of collected data. This study confirms that intentional GNSS jamming has a significant current impact and is widely used. Measurement data collected in the Gulf of Gdańsk region reveal the presence and extent of this interference. This article presents the goals of intentional jamming of GNS signals and provides a general technical analysis. The legality of intentional GNSS jamming is assessed, and potential legal implications are identified in the context of state liability for its consequences. The research conclusions indicate that GNSS are essential

to modern economies, armed forces, and public safety, but their vulnerabilities require continuous improvement of security technologies, detection methods, continuous monitoring of their operations, and the introduction of appropriate legal regulations to protect them.

Keywords

EW, GNSS, jamming, monitoring, NAVWAR

Streszczenie

Nawigacja wykorzystująca globalne systemy nawigacji satelitarnej GNSS (*ang. Global Navigation Satellite Systems*) jest powszechnie dostępna i szeroko stosowana. Zaburzenia sygnałów nawigacyjnych są efektem zjawisk naturalnych (m.in. aktywność fizyczna atmosfery czy Słońca, promieniowanie kosmiczne, itp.), bądź propagacji sygnałów elektromagnetycznych i oddziaływania otoczenia (np. wielodrogowość). z kolei intencjonalne i szkodliwe oddziaływanie na sygnały GNSS poprzez ich zakłócanie (*ang. jamming*), fałszowanie (*ang. spoofing*) lub mylenie (*ang. meaconing*) jest częste i stanowi element nieprzyjaznej aktywności, szczególnie w działaniach asymetrycznych i hybrydowych. Celem opracowania jest przedstawienie czym są intencjonalne zakłócenia GNSS, jakie są ich główne charakterystyki techniczne oraz skutki oddziaływania, jaka jest ich klasyfikacja oraz jakie są prawne aspekty ich stosowania, a także prezentacja wyników pomiarów tych zakłóceń zrealizowanych w rejonie Zatoki Gdańskiej. Do osiągnięcia celu wykorzystano następujące metody badawcze: analiza źródeł wiedzy, wywiad ekspercki, pomiary terenowe oraz synteza zebranych danych i wnioskowanie. Wszystkie zamierzenia badawcze zostały osiągnięte, a uzyskane rezultaty wskazują jak istotnym narzędziem oddziaływania są celowe zakłócenia GNSS oraz jakie jest ich obecne znaczenie i skala użycia. Zebrane dane pomiarowe wskazują na występowanie tego typu zakłóceń w rejonie Zatoki Gdańskiej. W niniejszym artykule przedstawiono cele intencjonalnego zakłócania sygnałów systemów GNS oraz dokonano ich ogólnej analizy technicznej. Poddano ocenie legalność celowych zakłóceń GNSS oraz wskazano potencjalne implikacje prawne w kontekście odpowiedzialności państw za ich skutki.

Wnioski z badań wskazują, że GNSS są niezbędne dla nowoczesnej gospodarki, sił zbrojnych i bezpieczeństwa publicznego, ale ich podatności wymuszają nieustanne doskonalenie technologii zabezpieczających, metod detekcji, ciągłego monitorowania działania oraz wprowadzania adekwatnych regulacji prawnych do ich ochrony.

Słowa kluczowe

EW, GNSS, monitoring, NAVWAR, zakłócanie

Wprowadzenie

Globalne satelitarne systemy nawigacyjne GNSS (*ang. Global Navigation Satellite Systems*) dzięki usługom lokalizacyjnym, które oferują mają kluczowe znaczenie dla współczesnej gospodarki, przemysłu, społeczeństw, sił zbrojnych, służb ratunkowych i reagowania kryzysowego. Nawigacja w oparciu o usługi globalnych systemów nawigacji satelitarnej GNSS jest powszechnie dostępna i szeroko wykorzystywana, a zakres i skala jej zastosowań szybko się rozszerzają. Świadczą o tym coroczne raporty technologiczne i prognostyczne kluczowych instytucji specjalizujących się w kreowaniu strategii, rozwoju i implementacji systemów i aplikacji GNSS, takich jak: ESA (*ang. European Space Agency*)¹, EUSPA (*ang. European Union Agency for the Space Programme*)² czy NASA (*ang. National Aeronautics and Space Administration*)³.

Jednak funkcjonowanie aplikacji i systemów opartych na GNSS może być zagrożone przez wiele czynników, zarówno naturalnych, jak i sztucznych. Na przestrzeni ostatnich lat obserwuje się doniesienia⁴, raporty i analizy⁵, wskazujące na rosnącą liczbę zaburzeń działania nawigacji satelitarnej, a czasami wręcz niemożność jej użycia. Obserwację i relacje składane przez ludzi znajdujących się w różnych sytuacjach życiowych wskazują na okresowe problemy użycia aplikacji wyznaczających trasy marszu lub podróży, bądź wyznaczanie bieżącej pozycji w zupełnie innym miejscu niż dana osoba się znajdowała⁶. z kolei piloci lotnictwa transportowego, zarówno pasażerskiego jak również cargo, wskazywali na incydentalną niedostępność sygnałów GNSS w określonych rejonach, o konkretnych porach i na wybranych wysokościach, co uniemożliwiało prowadzenie nawigacji satelitarnej w operacjach lotniczych. Podobne relacje składały osoby utrzymujące systemy nawigacyjne w Lotniczym

¹ <https://www.esa.int/>, [dostęp: 15.10.2024].

² <https://www.euspa.europa.eu/>, [dostęp: 15.10.2024].

³ <https://www.nasa.gov/>, [dostęp: 15.10.2024].

⁴ GPS Jammer Delays Flights in France, 2017. <https://rntfnd.org/2017/09/15/gps-jammer-delays-flights-in-france/>, [dostęp: 15.10.2024]; W. Papiernik, Duże zakłócenia sygnału GPS w Polsce. Ostrzeżenie dla pilotów, Cyberdefence24, 2024. <https://cyberdefence24.pl/technologie/problemy-z-gps-w-polsce-o-co-tu-chodzi>, [dostęp: 15.10.2024]; S. Palczewski, Problemy z GPS w Polsce. O co tu chodzi?, Cyberdefence24, 2024. <https://cyberdefence24.pl/technologie/problemy-z-gps-w-polsce-o-co-tu-chodzi>, [dostęp: 15.10.2024]; P. Łobaza, Kto zakłóca GPS w Polsce? Tak, dobrze myślisz, Telepolis, 2024. <https://www.telepolis.pl/wiadomosci/wydarzenia/sygnał-gps-polska-zakłócenia>, [dostęp: 15.10.2024].

⁵ GPS anti-jamming: Building resilience to today's greatest threats - Spire: Global Data and Analytics, <https://spire.com/blog/space-reconnaissance/gps-anti-jamming-building-resilience-to-today-greatest-threats/> [dostęp: 06.10.2024]. Fundamentals of GPS Threats, Spirent Communications, 2022. <https://www.spirent.com/assets/wp-fundamentals-of-gps-threats>, [dostęp: 11.01.2025]. Protecting commercial aircraft against GPS spoofing threats, Spirent Communications, 2022. <https://www.spirent.com/assets/ebook-protecting-commercial-aircraft-against-gps-spoofing-threats>, Buesnel G., Holbrow M., GNSS Threats, Attacks and Simulations, Spirent Communications, 2017. <https://www.gps.gov/governance/advisory/meetings/2017-06/buesnel.pdf>, [dostęp: 11.01.2025]. GPS Spoofing: Final Report published by WorkGroup, OPSGROUP, 2024. <https://ops.group/blog/gps-spoofing-final-report/>, [dostęp: 15.10.2024].

⁶ K. Klawiter, Drony spadają nad Bałtykiem. GPS zwariował. Kto za tym stoi?, YouTube, 2025. https://youtu.be/aQqpDQFhWtk?si=R_8thE-IVyGBr3WI, [dostęp: 16.06.2025].

Pogotowia Ratunkowego⁷ oraz prowadzące pomiary geodezyjne z użyciem samolotów⁸. W ostatnich miesiącach nastąpił gwałtowny wzrost zdarzeń polegających na czasowym lub miejscowym braku sygnału GNSS lub podawaniu w rejonie Zatoki Gdańskiej błędnych wskazań pozycji bądź trasy za pomocą aplikacji bazujących na nawigacji satelitarnej⁹. Podobne sytuacje pojawiały się także w innych krajach. Wiele wskazuje, że są one skutkiem celowego zaburzenia działania GNSS¹⁰. Analiza obszaru badawczego wskazuje, że zapewnienia ciągłości działania (*ang. continuity of operations*) i odporności GNSS (*ang. GNSS resilience*) na intencjonalne zaburzanie czy też uniemożliwianie ich operacyjnego wykorzystania lub fałszowania efektów ich funkcjonowania nabrało kluczowego znaczenia i stało się palącą potrzebą na poziomie narodowym. Zastosowanie GNSS do wsparcia działalności w wielu obszarach życia człowieka jest codziennością, a w wielu przypadkach staje się koniecznością. Incydenty utrudniania lub blokowania działania systemów nawigacji satelitarnej przez Federację Rosyjską i inne państwa czy też organizacje terrorystyczne, obserwowane są w ostatnim czasie, zwłaszcza na obszarze Polski¹¹, w rejonie Morza Bałtyckiego¹², Morza Czarnego¹³ i Morza Śródziemnego¹⁴ czy w Zatoce Perskiej¹⁵. Coraz częściej słyszy się o problemach

⁷ Wnioski z rozmów z managerami lotnictwa ratunkowego, badanie własne, Warszawa, 2025.

⁸ Wywiad ekspercki – badania geodezyjne z wykorzystaniem samolotów, badanie własne, Warszawa 2025.

⁹ Zagrożenie katastrofą lotniczą w Polsce? Tajemnicze urządzenie z Rosji zakłóca sygnał GPS, Super express, 2024. <https://www.se.pl/wiadomosci/swiat/zagrozenie-katastrofa-lotnicza-w-polsce-tajemnicze-urządzenie-z-rosji-zakłoca-gps-aa-AwTX-yGSN-GpY6.html>, [dostęp: 15.10.2024].

¹⁰ Rosjanie zakłócają sygnał GPS. ISW: To test systemów zagłuszających, polsatnews.pl, 2024. <https://www.polsatnews.pl/wiadomosc/2024-01-19/isw-rosjanie-zakłocaja-sygnał-gps-to-test-systemow-zagłuszajacych/>, [dostęp: 15.10.2024].

¹¹ R. Makowiec, Zakłócenia GPS w Polsce. Jakiego sprzętu może używać Rosja?, Cyberdefence24, 2024. <https://cyberdefence24.pl/armia-i-služby/zakłocenia-gps-w-polsce-jakiego-sprzetu-moze-uzywac-rosja>, [dostęp: 15.10.2024]; K. Pawłowicz, Zakłócenia GPS w Polsce. Instytut Studiów nad Wojną zabrał głos, 2024. <https://www.tysol.pl/a116057-zakłocenia-gps-w-polsce-instytut-studiow-nad-wojna-zabral-glos>, [dostęp: 15.10.2024].

¹² Wu D. L.: Innovation: Recent GPS jamming in regions of geopolitical conflict. GPS World. <https://www.gpsworld.com/innovation-recent-gps-jamming-in-regions-of-geopolitical-conflict/> [dostęp: 09.03.2025]; Media: Rosja rozmieszcza w Kaliningradzie wielki „zagłuszacz”, system walki elektronicznej Murmańsk-BN, Polskie Radio24, 2019. [dostęp: 15.10.2024]. <https://polskieradio24.pl/artykul/2300338,media-rosja-rozmieszcza-w-kaliningradzie-wielki-zagłuszacz-system-walki-elektronicznej-murmansk-bn>, [dostęp: 2024-10-15]. Krasucha-C4 w natarciu, czyli o tym jak Rosjanie zagłuszają sygnały GPS i telefonii komórkowej, Defence24, 2002, <https://defence24.pl/sily-zbrojne/krasucha-c4-w-natarciu-czyli-o-tym-jak-rosjanie-zagłusza-ja-sygnały-gps-i-telefonii-komorkowej>, D. Alankiewicz, Facebook, 2024. https://www.facebook.com/permalink.php?story_fbid=2108943229468266&id=100010578286338&ref=embed_post, [dostęp: 15.10.2024].

¹³ G.A. Angelov, Suspected Russian GPS jamming risks fresh dangers in Black Sea region. Radio Free Europe/Radio Liberty. <https://www.rferl.org/a/russia-gps-jamming-black-sea-romania-bulgaria-ukraine/32655397.html> [dostęp: 09.03.2025].

¹⁴ Electronic interference in Mediterranean. shipping.nato.int. <https://shipping.nato.int/nsc/operations/news/2019/electronic-interference-in-mediterranean.aspx> [dostęp: 09.03.2025].

¹⁵ T.J. Owen, Electronic interference in the Persian Gulf. MariTrace. <https://www.ww3.maritrace.com/post/electronic-interference-in-the-persian-gulf> [dostęp: 09.03.2025]. Shipping industry faces GPS disruption in Persian Gulf. Satelles, Inc. <https://satelles.com/shipping-industry-faces-gps-jamming-in-persian-gulf/> [dostęp: 09.03.2025].

z wykorzystaniem i dostępnością GNSS w transporcie lotniczym czy morskim¹⁶. W związku z prowadzeniem przez Siły Zbrojne Federacji Rosyjskiej działań hybrydowych w stosunku do Polski oraz innych członków NATO obserwuje się zwiększone oddziaływanie sił i środków walki elektronicznej EW (*ang. Electronic Warfare*) i nawigacyjnej NAVWAR (*ang. Navigation Warfare*), co przejawia się zaburzeniami pracy systemów GNSS. Na przestrzeni ostatnich trzech lat obserwuje intensyfikację występowania incydentów. Wykorzystanie GNSS nie jest zwykle możliwe także w rejonach konfliktów zbrojnych, np. wzdłuż frontu wojny na Ukrainie, co wiąże się z utrudnieniami z wykorzystaniem UAV przez każdą ze stron konfliktu¹⁷. W realizacji opracowania zastosowano podejście analityczne wsparte badaniami terenowymi w szczególności wykorzystano metody: analizy źródeł wiedzy, analizy „przypadków” opisujących incydenty i ich skutki, wywiadu eksperckiego, pomiarów sygnałów i analizy zebranych danych pomiarowych, syntezy wiedzy z zebranego materiału.

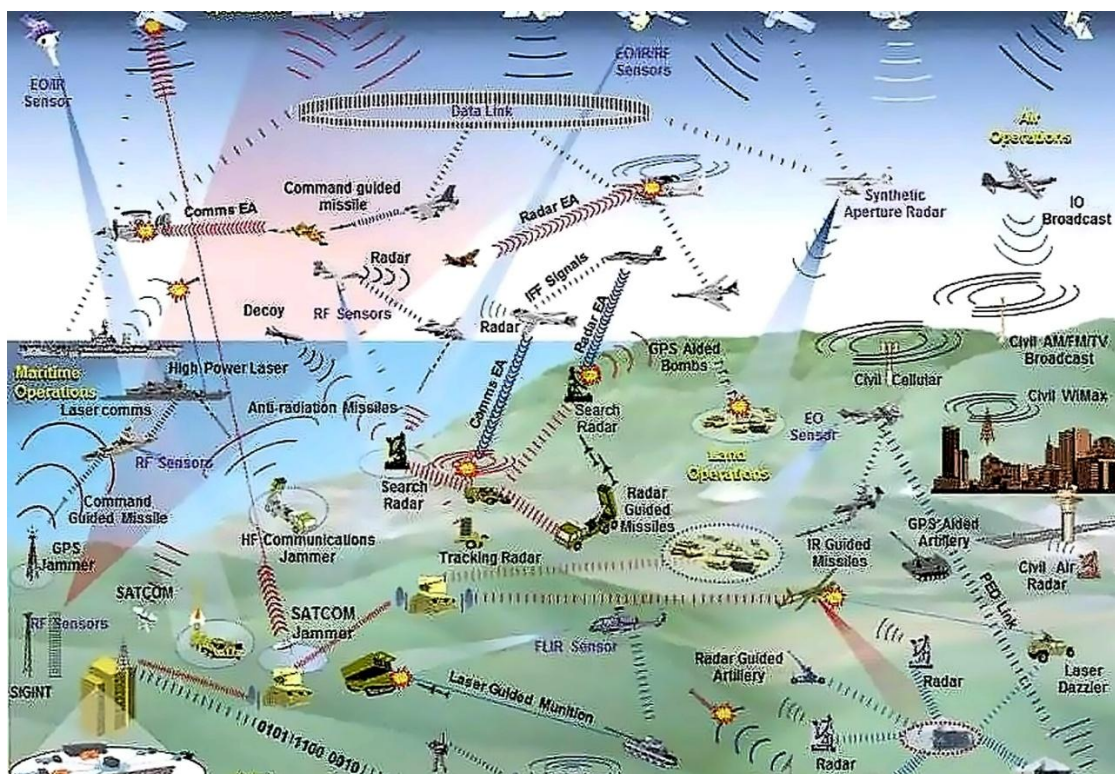
Idea zakłócania GNSS

GNSS w trakcie swojego rozwoju ewoluował od systemu dla wojska i zastosowań profesjonalnych (np. geodezja i kataster) do niemal powszechnego wykorzystania. Od technologii niszowej i trudno dostępnej GPS stał się dziś rozwiązaniem powszechnym.

Konieczne jest przeformatowanie potrzeb, oczekiwań i „zaufania” do „narzędzi” współczesnej cywilizacji bazujących na GNSS. Siły zbrojne na całym świecie polegają na GNSS w zakresie PNT. Od zaspokojenia potrzeb wojska, agencji rządowych, w tym wywiadowczych zaczęła się historia GPS. Obecnie nawigację satelitarną wykorzystuje większość wojskowych pojazdów/ samolotów/ okrętów/ platform bezzałogowych, systemów rozpoznania i kierowania ogniem oraz zaawansowane systemy uzbrojenia (np. pociski rakietowe, UAV czy amunicja krążąca), a także systemy walki C2 (*ang. Command&Control*), C4ISR (*ang. Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance*), ale również żołnierze na ćwiczeniach i w trakcie prowadzenia działań wszelkiego typu. Na Rysunku 1. przedstawiono główne obszary zastosowań GNSS w operacjach wojskowych.

¹⁶ A. Felski, Let us prepare the officer of the watch on jamming and spoofing. TransNav, „International Journal on Marine Navigation and Safety of Sea Transportation” 2019, no. 13 (4), s. 847–851.

¹⁷ C. Panella, A hidden electronic warfare battle is raging in Ukraine and demanding more from the soldiers fighting it, special drone unit says. Business Insider. <https://www.businessinsider.com/hidden-electronic-warfare-battle-demanding-more-of-ukrainian-soldiers-2025-2> [dostęp: 09.03.2025].



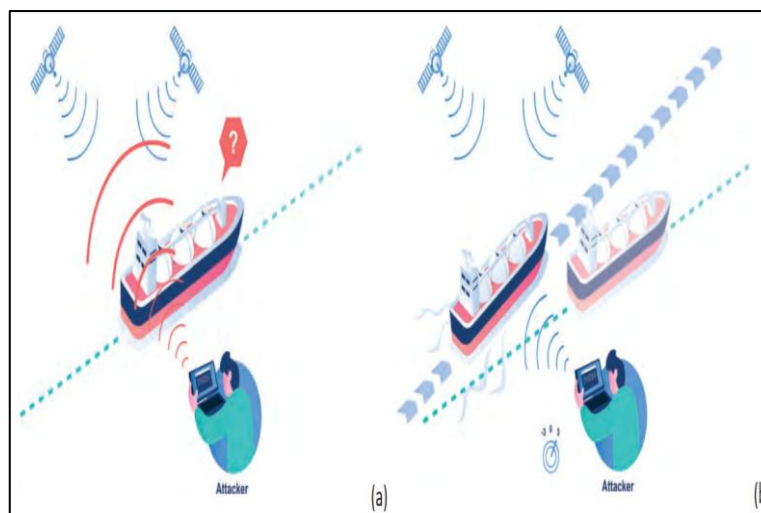
Źródło: https://euro-sd.com/wp-content/uploads/2024/02/JADC2_US-DoD.png.

18 M. Amelia, *Cyberataki w kosmosie: jak bezpieczne są nasze satelity?* HumanMag, 2023. <https://www.humanmag.pl/cyberataki-w-kosmosie-jak-bezpieczne-sa-nasze-satelity/>, [dostęp: 11.01.2024]. Jak hakerom udało się zniszczyć sieć Internetu satelitarnego Viasat?, SAT Kurier, 2023. <https://satkurier.pl/news/230559/jak-hakerom-udalo-sie-zniszczyc-siec-internetu-satelitarnego-viasat.html>, [dostęp: 11.01.2024]. M. Colaluca, K. Walter, C. Miller, N. Saunders, M. Sutton, *Lessons Learned from the KA-SAT Cyberattack: Response, Mitigation and Information Sharing blackhat*, 2023. <https://www.blackhat.com/us-23/briefings/schedule/index.html#lessons-learned-from-the-ka-sat-cyberattack-response-mitigation-and-information-sharing-34478>, [dostęp: 11.10.2024].

GNSS dostarczają danych wejściowych. W ogólnej percepcji manipulowanie sygnałami GNSS kojarzone jest z ich fałszowaniem (*ang. spoofing*), jednak spotyka się również działanie polegające na myleniu sygnałów (*ang. meaconing*). Natomiast zakłócanie (*ang. jamming*) sygnałów GNSS ma na celu blokowanie lub utrudnianie ich odbioru poprzez spowodowanie, że moc sygnału użytkowego docierającego od odbiornika GNSS jest zbyt mała aby można było dokonać jego skutecznej, bezbłędnej detekcji. Różnica pomiędzy ww. typami intencjonalnego oddziaływania na GNSS została przedstawiona na rysunku 1. Systemowo rzecz ujmując, manipulowanie sygnałami GNSS ma na celu wprowadzenie niepewności, naruszenie integralności informacyjnej oraz zaburzenie procesów bazujących na danych służących do pewnego i dokładnego określania pozycji, precyzyjnej i niezawodnej nawigacji i synchronizacji czasowej PNT (*ang. positioning, navigation, time*).

Może to doprowadzić do destabilizacji wybranych sektorów przemysłu lub gospodarki w danym rejonie, zachwiania społecznego zaufania do państwa i jego służb czy też do niepewności i paniki obywateli. Manipulacje sygnałami GNSS są jedną z technik walki nawigacyjnej NAVWAR realizowanymi w środowisku elektromagnetycznym¹⁹. Są one relatywnie tanimi narzędziami oddziaływania asymetrycznego, efektywnymi w działaniach hybrydowych. To skuteczny arsenał w operacjach terrorystycznych i działaniach grup przestępczych, które mają na celu zmylenie służb strzegących porządku publicznego i prawa.

Rys. 2. Idea (a) *jammingu* i (b) *spoofingu*.



Źródło: *Intertanko: Jamming and spoofing of Global Navigation Satellite Systems (GNSS). Intertanko, London, UK, 2019.*

¹⁹ Instrukcja walki nawigacyjnej (NAVWAR) w Siłach Zbrojnych RP DU-6.3.4., Warszawa 2022.

Aspekty techniczne zakłócania GNSS

GNSS jak każde systemy techniczne czy antropotechniczne posiadają pewne podatności (*ang. Vulnerabilities*)²⁰, w tym podatności na zagrożenia związane z oddziaływaniem w cyberprzestrzeni. Składają się na nie podatności elementów składowych GNSS, takich jak: urządzenia, aplikacje, protokoły, mechanizmy sterowania, techniki zapewnienia bezpieczeństwa, itp. Mając na uwadze zakres zastosowań GNSS przez poszczególne kraje lub społeczeństwa można mówić o krajowych podatnościach GNSS (*ang. National GNSS Vulnerabilities*), które odnoszą się do całości zasobów GNSS mających wpływ na infrastrukturę krytyczną danego kraju oraz systemów, rozwiązań, aplikacji infrastruktury krytycznej zależnych od GNSS. Należy zauważyć, że na jakość estymacji pseudoodległości w GNSS opartej na pomiarze czasu propagacji sygnału z satelity do użytkownika może wpływać kilka zjawisk, w tym również celowe oddziaływanie zakłócające. Każde źródło elektromagnetyczne oddziałujące na sygnały zakłóca proces estymacji czasu propagacji. Klasyfikacja głównych zakłóceń dla odbiorników GNSS uwzględnia różnorodne aspekty oddziaływania na sygnały GNSS czy też na elementy systemów GNSS. W tej kwestii kluczowe jest odniesienie się do źródła wywołującego zaburzenie działania GNSS oraz jego charakterystyki. Rodzaje emisji wpływających negatywnie na GNSS można podzielić na²¹:

- 1) zamierzone lub intencjonalne (*ang. intentional*) – są nimi: zagłuszanie lub inaczej zakłócanie (*ang. jamming*), fałszowanie (*ang. spoofing*) i mylenie (*ang. meaconing*);
- 2) niezamierzone lub nieintencjonalne (*ang. non-intentional*) – wynika głównie z oddziaływania otoczenia na sygnały propagowane od satelity do odbiornika użytkownika końcowego lub też z wpływu otoczenia na odbiornik.

Pierwsze z nich występują powszechnie w operacjach wojskowych (regularnych i nieregularnych) lub motywowanych działaniami pozaprawnymi. Zakłócanie GNSS jest bowiem działaniem nielegalnym, zarówno w Polsce²², jak i w innych krajach²³.

²⁰ Norma ISO/IEC 27005, ISO, 2018.

²¹ F. DAVIS, GNSS Interference Threats and Countermeasures, ArtTech House, 2015; O. Julien, Vulnerabilities of GNSS, the presentation for eKNOT, Ecole Nationale de l'Aviation Civile Toulouse, 2018; D. Zmysłowski, Jamming & spoofing in GNSS, Warszawa 2025; Z. Wu, Y. Zhang, Y. Yang, C. Liang, R. Liu, Spoofing and Anti-Spoofing Technologies of Global Navigation Satellite System: A Survey, IEEE Access, 2020.

<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9187240>, [dostęp: 11.01.2025].

²² Zob. ustawa z dnia 7 kwietnia 2022 r. – Prawo komunikacji elektronicznej (Dz.U. j.t. z 2022 poz. 1641) – art. 437–447; ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. 2002 Nr 74, poz. 676) – art. 5 ust. 2 pkt 5 i 7. Ustawa o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018, z późn. zm.).

²³ S. Bu-Pasha, Vulnerabilities in Localization With Regard to GNSS and Harmful Radio Interference: International and EU Law Aspects, IEEE Access, 2018.

Pierwsze doniesienia prasowe odnotowujące tego typu działania odnosiły się celowego ukrywania swojej pozycji przez pracowników za pomocą prostych jammerów, głównie zakłócających jedną częstotliwość GPS²⁴. Można zatem wnioskować, że podaż na rynku rządzeń zakłócających przyczynia się do ich nielegalnego użycia i staje się coraz bardziej powszechne również w obszarach mało lub wcale nie związanych z wojskiem.

Sygnały zakłócające można podzielić w oparciu o ich charakterystykę spektralną bazującą na częstotliwości nośnej f_{int} i szerokość pasma B_{int} , w odniesieniu do częstotliwości nośnej sygnału GNSS f_{GNSS} i zajętej szerokości pasma B_{GNSS} . Mając powyższe na uwadze wyróżniamy:

- zakłócenia pozapasmowe, odnoszące się do sygnałów zakłócających, których częstotliwość nośna znajduje się w pobliżu docelowego pasma częstotliwości GNSS: $(f_{\text{int}} < f_{\text{GNSS}} - B_{\text{GNSS}}/2 \text{ lub } f_{\text{int}} > f_{\text{GNSS}} + B_{\text{GNSS}}/2)$;
- zakłócenia wewnątrzpasmowe, odnoszące się do sygnałów zakłócających o częstotliwości nośnej w paśmie częstotliwości GNSS: $(f_{\text{GNSS}} - B_{\text{GNSS}}/2 < f_{\text{int}} < f_{\text{GNSS}} + B_{\text{GNSS}}/2)$.

Ponadto zakłócenia można dalej klasyfikować według ich charakterystyki w dziedzinie częstotliwości w następujący sposób:

- zakłócenia wąskopasmowe NBI (*ang. Narrowband Interference - NBI*), w ich przypadku zajęcie widma jest mniejsze w stosunku do szerokości pasma sygnału GNSS: $(B_{\text{int}} \ll B_{\text{GNSS}})$;
- zakłócenia szerokopasmowe WBI (*ang. Wideband Interference - WBI*), w tym przypadku zajęcie widma jest porównywalne z szerokością pasma sygnału GNSS: $(B_{\text{int}} \approx B_{\text{GNSS}})$;
- zakłócenia falą ciągłą CWI (*ang. Continuous Wave Interference - CWI*), które stanowią one ostateczną granicę w zakłóceniu wąskopasmowym NBI i pojawiają się jako pojedynczy ton w dziedzinie częstotliwości: $(B_{\text{int}} \rightarrow 0)$.

Ponadto, zakłócenia mogą mieć charakterystykę zmienną w zależności od częstotliwości, na przykład sygnały *chirp* charakteryzującą się liniową zmianą częstotliwości chwilowej w czasie, pojawiające się w ten sposób jako WBI. Tego rodzaju sygnały zakłócające są zazwyczaj generowane przez urządzenia zakłócające. Urządzenia takie są w stanie transmitować silne sygnały *chirp* o dużej mocy i częstotliwości kilku megaherców w ciągu kilku mikrosekund, zakłócając w ten sposób prawidłowy odbiór sygnału każdego kanału GNSS²⁵.

Zakłócanie sygnału GNSS (jamming) jest realizowane poprzez oddziaływanie sygnałem zakłócającym na sygnał użytkowy GNSS propagowany w kanale telekomunikacyjnym pomiędzy satelitą a odbiornikiem użytkownika końcowego. Takie działanie odbywa się poprzez addytywne wprowadzenie do kanału, którym propaguje się właściwy sygnał GNSS, sygnału zakłócającego. Powoduje to zmianę bilansu energetycznego w kanale, co z reguły doprowadza

²⁴ GPS Spoofing: Final Report published by WorkGroup, OPSGROUP, 2024. <https://ops.group/blog/gps-spoofing-final-report/>, [dostęp: 15.10.2024].

²⁵ DAVIS F., GNSS Interference Threats and Countermeasures, ArtTech House 2015.

do zmiany stosunku sygnału użytecznego do sygnału zakłócającego i szumu kanałowego, skutkiem czego jest wyeliminowanie sygnału użytecznego GNSS na wejściu odbiornika GNSS. Efekt jest taki, że odbiornik zazwyczaj dokona detekcji sygnału zakłócającego zamiast sygnału użytecznego GNSS niosącego wiadomość nawigacyjną, znaczniki czasu oraz PRN satelity. Sygnały zakłócające mogą mieć postać: NBI, WBI, CWI, chirp lub mieć postać o różnym czasie trwania. Moc sygnału zakłócającego, czas jego trwania oraz częstotliwość mają kluczowe znaczenie przy realizacji zakłócania GNSS.

Metodyka i wyniki badania zakłóceń GNSS

Na potrzeby niniejszego opracowania przeprowadzone zostało praktyczne badanie polegające na identyfikacji sygnałów zakłóceń celowych GNSS oraz wykonaniu pomiarów ich wartości. Czynności pomiarowe zrealizowano w rejonie południowo-wschodniego Bałtyku, ze szczególnym uwzględnieniem Zatoki Gdańskiej. Pomiary wykonano w zakresie częstotliwości (1525 – 1600) MHz, obejmującym pasma pracy systemów GNSS: GPS/Galileo L1 (1575,42 MHz), BeiDou B1 (1561 MHz) oraz GLONASS L2. Uzyskane wyniki ujawniły obecność powtarzalnych anomalii w pasmach L1/B1, mogących wskazywać na występowanie celowych zakłóceń sygnału użytecznego ww. konstelacji GNSS. Zaobserwowane zjawiska nie wykazywały korelacji z naturalnymi czynnikami środowiskowymi ani z danymi publikowanymi w ogólnodostępnych źródłach, co potwierdzone zostało przez brak oficjalnych i wiarygodnych systemów wczesnego ostrzegania użytkowników przed bieżącymi zagrożeniami dla integralności i dostępności sygnałów GNSS w tym rejonie²⁶. Do rejestracji sygnałów wykorzystano odbiornik wykonany w technologii radia programowalnego SDR (*ang. software defined radio*) RTL-SDR v.3 oraz antenę helikalną o prawoskrętnej polaryzacji kołowej RHCP (*ang. right-hand circular polarization*), przystosowaną do pracy w paśmie L. Zastosowany zestaw pomiarowy charakteryzował się wysokim współczynnikiem koszt–efekt, pozwalając na prowadzenie wiarygodnych i powtarzalnych obserwacji przy niewielkich nakładach finansowych, co czyni go szczególnie przydatnym w zastosowaniach badawczych oraz dydaktycznych. Pomimo prostoty konstrukcji, konfiguracja ta umożliwia rejestrację sygnałów o bardzo niskim poziomie mocy oraz obserwację zmian charakterystyki widma w czasie rzeczywistym. Dane przetwarzano w środowisku SoapySDR, natomiast analizę właściwą przeprowadzono z wykorzystaniem autorskich skryptów w języku Python. Zastosowane rozwiązanie sprzętowo-programowe może stanowić bazę dla nisko-kosztowych sieci monitorujących zakłócenia GNSS, zdolnych do ciągłego śledzenia poziomu zakłóceń w pasmach L i raportowania danych

²⁶ Council of the European Union, Note to Delegations – Addressing the rise in GNSS interference in Europe and the need for coordinated monitoring and alerting mechanisms, Brussels, 22 May 2025.

w czasie zbliżonym do rzeczywistego. Tego typu konfiguracja wpisuje się w postulaty Unii Europejskiej dotyczące rozwoju zdecentralizowanych, ekonomicznych systemów detekcji i raportowania zakłóceń w regionie Europy Północnej. W trakcie przeprowadzonych pomiarów w paśmie o częstotliwości (1525–1600)MHz odnotowano pojedynczy przypadek zakłóceń, których charakterystyka wskazuje na wąskopasmowe zakłócenia CWI. Zjawisko to zaobserwowano podczas jednej z sesji pomiarowych prowadzonych w rejonie Zatoki Gdańskiej. W zarejestrowanym widmie odnotowano występowanie wąskiej linii sygnałowej o stałej częstotliwości, utrzymującej się przez kilka minut. Zakłócenie miało charakter stabilny - nie wykazywało modulacji ani przemiatania częstotliwości, co pozwala zaklasyfikować je jako typowe CWI o małej szerokości pasma. Poziom sygnału zakłócającego przekraczał tło szumowe o kilka decybeli, powodując lokalne podbicie szumu w rejonie częstotliwości roboczej systemów GPS i Galileo (ok. 1575,42 MHz). Ze względu na ograniczony czas obserwacji i jednorazowy charakter zjawiska, nie było możliwe przeprowadzenie pełnej analizy korelacyjnej ani ustalenie kierunku pochodzenia sygnału. Niemniej jednak parametry zaobserwowanego zdarzenia – stabilna częstotliwość, brak modulacji oraz wąskie pasmo – wskazują na antropogeniczne źródło emisji, najprawdopodobniej urządzenie generujące sygnał zakłóceń w paśmie L. Pojedyncza obserwacja, mimo że ograniczona czasowo, potwierdza praktyczną przydatność zastosowanego nisko-kosztowego zestawu pomiarowego. Uzyskane dane dowodzą, że nawet prosty odbiornik SDR, przy odpowiedniej konfiguracji, może być skutecznym narzędziem do wstępnej detekcji i dokumentacji epizodycznych zakłóceń GNSS. Wyniki te stanowią punkt wyjścia do dalszych, bardziej systematycznych badań prowadzonych w oparciu o dłuższe serie obserwacji i wielopunktową rejestrację sygnałów.

Regulacje ITU dotyczące zakłóceń GNSS

Sektor Radiokomunikacji Międzynarodowej Unii Telekomunikacyjnej ITU–R (*ang. International Telecommunication Union- Radiocommunication Sector*) jest wyspecjalizowaną agencją Organizacji Narodów Zjednoczonych odpowiedzialną za koordynację globalnego wykorzystania widma radiowego oraz orbit satelitarnych. Podstawowy dokument regulujący te kwestie – *ITU Radio Regulations* – ma charakter traktatu międzynarodowego, ratyfikowanego przez wszystkie państwa członkowskie ITU. Zgodnie z art. 15 *Radio Regulations* (edycja 2020) administracje państw mają obowiązek „podejmowania wszelkich możliwych środków w celu unikania szkodliwych zakłóceń” (*ang. harmful interference*) w stosunku do stacji radiowych innych państw oraz „natychmiastowego eliminowania” takich zakłóceń, jeśli zostaną one stwierdzone²⁷. Definicja „szkodliwego zakłócenia” została jednoznacznie

²⁷ International Telecommunication Union, Radio Regulations, Edition of 2020, Article 15 – Interferences. Geneva: ITU, 2020

określona w § 1.166 regulaminu jako *zakłócenie, które zagraża funkcjonowaniu służby radiokomunikacyjnej pracującej zgodnie z regulaminem lub w sposób istotny pogarsza, utrudnia lub przerywa odbiór usług radiowych*.

W kontekście systemów GNSS, które są regulowane nadzorowane przez służbę radionawigacji satelitarnej RNSS (ang. *radio navigation satellite service*), ochrona ta ma charakter priorytetowy. RNSS została wymieniona w załączniku 4 *Radio Regulations* jako służba wymagająca szczególnego traktowania w zakresie koordynacji widma i zapobiegania zakłóceniom. W tym celu ITU wprowadziła szereg rezolucji i zaleceń, m.in. Rezolucję ITU-R 208 (Rev.WRC-19), w której podkreślono potrzebę międzynarodowej współpracy w zakresie przeciwdziałania celowym zakłóceniom sygnałów nawigacyjnych oraz wymiany informacji o incydentach²⁸. Państwa członkowskie ITU zobowiązane są również do raportowania przypadków szkodliwych zakłóceń do Biura Radiokomunikacyjnego ITU (ITU-BR). Procedura ta została opisana w *Article 15, Sections 15.21–15.35 Radio Regulations* i przewiduje możliwość zgłaszania incydentów zarówno między administracjami krajowymi, jak i bezpośrednio do ITU-BR. Biuro może następnie prowadzić mediację między zainteresowanymi stronami oraz opublikować zgłoszone przypadki w oficjalnym biuletynie ITU. Dodatkowo, w rekomendacjach serii ITU-R SM (Spectrum Management), w tym ITU-R SM.1132-2 „General principles and methods for sharing between radiocommunication services”, określono metody identyfikacji i klasyfikacji zakłóceń oraz wskazano, że każde państwo członkowskie powinno posiadać krajowy system monitorowania widma zdolny do detekcji sygnałów zakłócających w czasie rzeczywistym. W konsekwencji, z prawnego punktu widzenia, celowe lub tolerowane przez państwo zakłócanie sygnałów RNSS w sposób, który uniemożliwia prawidłowe funkcjonowanie usług radionawigacyjnych innych państw, może być traktowane jako naruszenie zobowiązań traktatowych wynikających z *Radio Regulations*. Tego rodzaju działanie stanowi podstawę do złożenia oficjalnej skargi lub noty dyplomatycznej w ramach procedur ITU-BR, a w przypadkach uporczywych – może skutkować eskalacją na forum Organizacji Narodów Zjednoczonych ONZ/ UNO (ang. *United Nations Organization*) lub Międzynarodowej Organizacji Lotnictwa Cywilnego ICAO (ang. *International Civil Aviation Organization*). Zgodnie z art. 15 *Radio Regulations* (ITU, 2020), wszystkie państwa członkowskie – w tym również Federacja Rosyjska, będąca stroną traktatu i uczestnikiem Światowych Konferencji Radiokomunikacyjnych – są zobowiązane do zapobiegania oraz eliminowania szkodliwych zakłóceń w służbach radiokomunikacyjnych innych państw. Pomimo tych zobowiązań, w ostatnich latach liczne raporty międzynarodowych agencji, w tym EUROCONTROL, EUSPA oraz Europejskiej Służby Działań Zewnętrznych (EEAS), wskazują na znaczny wzrost liczby incydentów zakłóceń GNSS

²⁸ ITU Radiocommunication Assembly Resolution 208 (Rev.WRC-19) – Protection of RNSS Frequencies from Harmful Interference, Geneva: ITU, 2019.

w regionie Morza Bałtyckiego²⁹. z doniesień tych wynika, że zakłócenia te mogą być związane z działalnością zaawansowanych systemów walki elektronicznej (EW), które –zgodnie z dostępnymi danymi technicznymi – prawdopodobnie znajdują się w rejonie obwodu kaliningradzkiego Federacji Rosyjskiej i dysponują zdolnością do emisji w pasmach częstotliwości wykorzystywanych przez systemy GNSS. Nie istnieją jednak publicznie dostępne dane pozwalające jednoznacznie potwierdzić lokalizację ani źródło poszczególnych emisji. Przykładowe systemy tego typu przedstawiono w Tabeli 1³⁰.

Tabela 1. *Systemy walki elektronicznej Federacji Rosyjskiej stosowane do oddziaływania na GNSS³¹*

System	Pasmo działania	Zakres zakłóceń GNSS	Zasięg działania	Uwagi dodatkowe
R-330Zh "Zhitel"	0,1–2,0 GHz	GPS, INMARSAT, Iridium, Galileo	do 25 km	Zakłócenia mobilne i stacjonarne
R-330M1P "Diabazol"	0,1–2,0 GHz	GPS, GSM, komunikacja satelitarna	do 30 km	Następca systemu „Mandat”
R-340RP "Pole-21"	1,176–1,602 GHz	GPS, GLONASS, Galileo, BeiDou	do 75 km	Rozmieszczany także na infrastrukturze cywilnej
RB-341V "Leer-3"	0,935–1,705 GHz	łączność komórkowa, potencjalnie GNSS	do 100km (Zależny od Orlan-10)	System UAV + Orlan-10
RB-636 "Svet-KU"	0,025–18 GHz	GNSS (pośrednio), szerokie pasmo	nieznany	Wykorzystywany do SIGINT i zakłócania aktywnego

Źródło: *Janes C4ISR & Mission Systems: Electronic Warfare. Yearbook 2023–2024*

²⁹ European Union External Action Service (EEAS), Situation Awareness on GNSS Interference in Northern Europe, Brussels, March 2024; European Union Aviation Safety Agency (EASA), Safety Information Bulletin – GPS/GNSS Signal Degradation in the Baltic Region, Cologne, April 2024; EUROCONTROL, Performance Review Report 2024, Brussels 2024.

³⁰ Janes C4ISR & Mission Systems: Electronic Warfare. Yearbook 2023–2024.

³¹ Ibidem.

Działania zgłoszeniowe państw regionu. W 2025 r. administracje państw basenu Morza Bałtyckiego wielokrotnie sygnalizowały w ITU przypadki „harmful interference” wobec RNSS. Zgodnie z opublikowaną agendą i omówieniami posiedzeń RRB, szczegółowo rozpatrzono zawiadomienia Estonii, Finlandii, Łotwy i Litwy dotyczące zakłóceń GNSS nad regionem. Równolegle, Polska - wraz z siedmioma innymi państwami UE i Ukrainą - złożyła 17–18 marca 2025 r. skargę do ITU na celowe ingerencje w łączność satelitarną w Europie, domagając się ich zaniechania i środków naprawczych. ITU (RRB) potwierdziła uporczywość zjawiska i wezwała zainteresowane administracje, w tym Federację Rosyjską, do pilnego usunięcia zakłóceń oraz udziału w spotkaniach mediacyjnych. Pomimo podjętych działań dyplomatycznych i technicznych, realne efekty interwencji pozostają ograniczone, a obserwacje prowadzone w kolejnych miesiącach wskazują, że zakłócenia GNSS w regionie Bałtyku nadal występują, co podważa skuteczność obecnych mechanizmów egzekwowania postanowień *Radio Regulations* w praktyce³².

Zalecenia ICAO i IMO w zakresie zakłóceń GNSS

W lotnictwie cywilnym podstawowe wymagania wobec urządzeń radionawigacyjnych i ochrony przed zakłóceniami określa ICAO Annex 10, Vol. I.³³ Dokument wymaga od państw zapewnienia zgodności instalacji nawigacyjnych z normami (SARPs) oraz ustanowienia procedur zgłaszania, badania i eliminowania harmful interference w pasmach RNSS. ICAO w nowszych materiałach programowych rekomenduje też, aby państwa oraz dostawcy usług nawigacji lotniczej ANSP (ang. *Air Navigation Service Provider*), którym na przykładzie Polski jest Polska Agencja Żeglugi Powietrznej PAŻP/PANSA (ang. *Polish Air Navigation Service Agency*) wdrażały środki łagodzące RFI (wieloźródłowa nawigacja, procedury awaryjne i raportowanie incydentów). Po stronie żeglugi morskiej IMO (ang. *International Maritime Organization*) przypomina, że celowe zakłócanie GNSS stanowi istotne ryzyko dla bezpieczeństwa żeglugi i ochrony środowiska morskiego. W okólniku MSC.1/Circ.1644 Komitet Bezpieczeństwa Morskiego wprost wzywa państwa do: powstrzymania się od interferencji w sygnały GNSS, minimalizowania zakłóceń ze swojego terytorium, publikowania ostrzeżeń dla żeglarzy o znanych okresach/rejonach zakłóceń oraz przeciwdziałania nieautoryzowanym transmisjom w pasmach nawigacyjnych. Te linie działania zostały ponowione we wspólnym oświadczeniu IMO–ICAO–ITU z marca/czerwca 2025 r.

³² International Telecommunication Union (ITU), Radio Regulations Board – Summary Record of the 25th Meeting (RRB25.1), Geneva, 21 March 2025, Document RRB25-1/8. European Union External Action Service (EEAS), Joint Complaint by EU and Associated States on Deliberate Interference with Satellite Communications Submitted to ITU, Brussels, 18 March 2025.

³³ ICAO, Annex 10 to the Convention on International Civil Aviation, Volume I - Radio Navigation Aids, latest amendment, Montreal: International Civil Aviation Organization.

Prawo międzynarodowe i odpowiedzialność państwa

Zgodnie z zasadami prawa międzynarodowego, każde państwo ponosi odpowiedzialność za działania lub zaniechania, które można mu przypisać i które stanowią naruszenie jego zobowiązań międzynarodowych. Ramy tej odpowiedzialności określa dokument *Articles on Responsibility of States for Internationally Wrongful Acts* (ARSIWA), przyjęty przez Komisję Prawa Międzynarodowego ONZ w 2001 roku. Zgodnie z art. 2 ARSIWA, za czyn międzynarodowo bezprawny uznaje się każde działanie państwa, które jest mu możliwe do przypisania i stanowi naruszenie obowiązku wynikającego z prawa międzynarodowego. W kontekście zakłóceń GNSS obowiązek ten łączy się z postanowieniami *ITU Radio Regulations*, które – jako traktat ratyfikowany m.in. przez Federację Rosyjską – nakładają na państwa obowiązek zapobiegania i eliminowania szkodliwych zakłóceń w służbach radiokomunikacyjnych³⁴.

Ocena legalności zakłóceń w Zatoce Gdańskiej

Z prawnego punktu widzenia, celowe zakłócanie sygnałów GNSS w rejonie Zatoki Gdańskiej należy rozpatrywać w świetle podstawowych zasad prawa międzynarodowego, w tym zasady suwerenności terytorialnej oraz zakazu działań transgranicznych powodujących szkodę innym państwom. Jeżeli źródło zakłóceń znajduje się poza granicami Polski, na przykład na terytorium obwodu kaliningradzkiego Federacji Rosyjskiej, mamy do czynienia z działaniem o charakterze transgranicznym, które w świetle zasady *sic utere tuo ut alienum non laedas* („nie używaj swojego terytorium w sposób szkodliwy dla innych”) stanowi naruszenie prawa międzynarodowego³⁵. Zasada ta, uznawana za element prawa zwyczajowego, nakłada na państwa obowiązek powstrzymywania się od prowadzenia jakiegokolwiek działalności na własnym terytorium, która mogłaby powodować szkodę lub zagrożenie dla bezpieczeństwa innego państwa.

Kontekst ten znajduje również potwierdzenie w postanowieniach Konwencji Narodów Zjednoczonych o prawie morza (UNCLOS, 1982), zgodnie z którymi wszystkie państwa są zobowiązane do takiego korzystania z mórz, które zapewnia poszanowanie praw i bezpieczeństwa innych uczestników wspólnoty międzynarodowej. Artykuły 87, 88 i 301 UNCLOS wskazują, że morza mają być wykorzystywane wyłącznie do celów pokojowych, a państwa powinny

³⁴ International Telecommunication Union, *Radio Regulations*, Edition of 2020, Article 15 – Interferences. Geneva: ITU, 2020. International Law Commission (ILC), *Articles on Responsibility of States for Internationally Wrongful Acts*, adopted by the ILC at its fifty-third session (2001), UN Doc. A/56/10.

³⁵ International Court of Justice (ICJ), *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 1996, ICJ Reports 226, §29

uniknąć jakichkolwiek działań, które mogłyby zagrażać bezpieczeństwu żeglugi lub porządkowi międzynarodowemu³⁶.

W tym kontekście szczególne znaczenie ma również zasada „due regard”, rozumiana jako obowiązek należytego poszanowania praw i interesów innych państw przy wykonywaniu własnych uprawnień na morzu. Oznacza to, że każde państwo, realizując swoje działania techniczne lub wojskowe w przestrzeni radiowej i morskiej, ma obowiązek uwzględniać ich możliwy wpływ na bezpieczeństwo innych użytkowników środowiska morskiego³⁷. Celowe lub tolerowane zakłócenia sygnałów GNSS, które oddziałują na żeglugę i lotnictwo cywilne w Zatoce Gdańskiej, mogą zatem zostać uznane za naruszenie nie tylko postanowień UNCLOS, lecz także ogólnych zasad odpowiedzialności państw za działania sprzeczne z prawem międzynarodowym³⁸.

Wnioski i rekomendacje

W związku z prowadzaniem przez SZ Federacji Rosyjskiej działań hybrydowych w stosunku do Polski oraz innych członków NATO obserwuje się większą aktywność środków walki elektronicznej. Wywołuje to zaburzenia pracy systemów GNSS, które wyzwalają konieczność ciągłego monitorowania stanu zakłóceń. Wyzwała to pilne wdrożenie systemów monitorowania, oceny i analizy zaburzeń sygnałów GNSS wraz z funkcją wyznaczenia źródeł ich pochodzenia. Ochrona infrastruktury krytycznej i SZ RP powinna uwzględniać wdrożenie urządzeń i systemów mitygujących zakłócenia GNSS. Sytuacje kryzysowe wywołane przez zaburzenia sygnałów GNSS wymagają zaangażowania operacyjnego sił i środków wielu instytucji państwa co wskazuje na konieczność zmian legislacyjnych. Co prawda, są podstawy prawne i wyznaczone zostały instytucje państwowe do monitorowania stanu działania GNSS i ich aplikacji, wdrożono też regulacje prawne pozwalające na egzekwowanie i karanie zakłócających lub fałszujących działanie GNSS, ale nie ma narzędzi technicznych, rozwiązań organizacyjnych oraz struktur, które koordynowałyby ochronę infrastruktury krytycznej, SZ RP, gospodarki, przemysłu oraz ludności w tym obszarze.

³⁶ United Nations Convention on the Law of the Sea (UNCLOS), Montego Bay, 10 December 1982, Articles 87, 88, 301.

³⁷ UNCLOS, Article 87(2): States shall have due regard to the interests of other States in their exercise of the freedom of the high seas.

³⁸ Ibidem.

Bibliografia

- Alankiewicz D., Facebook, 2024. https://www.facebook.com/permalink.php?story_fbid=2108943229468266&id=100010578286338&ref=embed_post.
- Amelia M., Cyberataki w kosmosie: jak bezpieczne są nasze satelity? HumanMag, 2023. <https://www.humanmag.pl/cyberataki-w-kosmosie-jak-bezpieczne-sa-nasze-satelity/>.
- Angelov G. A., Suspected Russian GPS jamming risks fresh dangers in Black Sea region. Radio Free Europe/Radio Liberty. <https://www.rferl.org/a/russia-gps-jamming-black-sea-romania-bulgaria-ukraine/32655397.html>.
- Buesnel G., Holbrow M., GNSS Threats, Attacks and Simulations, Spirent Communications, 2017. <https://www.gps.gov/governance/advisory/meetings/2017-06/buesnel.pdf>.
- Bu-Pasha S., Vulnerabilities in Localization With Regard to GNSS and Harmful Radio Interference: International and EU Law Aspects, IEEE Access, 2018.
- Colaluca M., Walter K., Miller C., Saunders N., Sutton M., Lessons Learned from the KA-SAT Cyberattack: Response, Mitigation and Information Sharing blackhat, 2023. <https://www.blackhat.com/us-23/briefings/schedule/index.html#lessons-learned-from-the-ka-sat-cyberattack-response-mitigation-and-information-sharing-34478>.
- Council of the European Union, Note to Delegations – Addressing the rise in GNSS interference in Europe and the need for coordinated monitoring and alerting mechanisms, Brussels, 22 May 2025.
- Dovis F., GNSS Interference Threats and Countermeasures, ArtTech House, 2015.
- Dovis F., GNSS Interference Threats and Countermeasures, ArtTech House 2015.
- Electronic interference in Mediterranean. shipping.nato.int. <https://shipping.nato.int/nsc/operations/news/2019/electronic-interference-in-mediterranean.aspx>.
- European Union Aviation Safety Agency (EASA), Safety Information Bulletin – GPS/GNSS Signal Degradation in the Baltic Region, Cologne, April 2024; EUROCONTROL, Performance Review Report 2024, Brussels, 2024.
- European Union External Action Service (EEAS), Joint Complaint by EU and Associated States on Deliberate Interference with Satellite Communications Submitted to ITU, Brussels, 18 March 2025.
- European Union External Action Service (EEAS), Situation Awareness on GNSS Interference in Northern Europe, Brussels, March 2024;
- EUSPA EO and GNSS Market Report, Luxembourg, 2022. https://www.euspa.europa.eu/sites/default/files/uploads/euspa_market_report_2022.pdf.
- Felski A., Let us prepare the officer of the watch on jamming and spoofing. TransNav, International Journal on Marine Navigation and Safety of Sea Transportation” 2019, no. 13 (4).
- Fundamentals of GPS Threats, Spirent Communications, 2022. <https://www.spirent.com/assets/wp-fundamentals-of-gps-threats>.
- GPS Jammer Delays Flights in France, 2017. <https://rntfnd.org/2017/09/15/gps-jammer-delays-flights-in-france/>.
- GPS Spoofing: Final Report published by WorkGroup, OPSGROUP, 2024. <https://ops.group/blog/gps-spoofing-final-report/>.
- GSA GNSS User Technology Report, Luxembourg, 2016.

- GSA GNSS User Technology Report, Luxembourg, 2020. <https://prod5.assets-cdn.io/event/6041/assets/8361034923-231960e68d.pdf>.
- https://euro-sd.com/wp-content/uploads/2024/02/JADC2_US-DoD.png.
- <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9187240>.
- <https://www.esa.int/>.
- <https://www.euspa.europa.eu/>.
- https://www.gsceuropa.eu/sites/default/files/sites/all/files/gnss_user_technology_report_web.pdf.
- <https://www.nasa.gov/>]
- ICAO, Annex 10 to the Convention on International Civil Aviation, Volume I — Radio Navigation Aids, latest amendment, Montreal: International Civil Aviation Organization.
- Instrukcja walki nawigacyjnej (NAVWAR) w Siłach Zbrojnych RP DU-6.3.4., Warszawa 2022.
- International Court of Justice (ICJ), Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996, ICJ Reports 226, § 29
- International Law Commission (ILC), Articles on Responsibility of States for Internationally Wrongful Acts, adopted by the ILC at its fifty-third session (2001), UN Doc. A/56/10.
- International Telecommunication Union (ITU), Radio Regulations Board – Summary Record of the 25th Meeting (RRB25.1), Geneva, 21 March 2025.
- International Telecommunication Union, Radio Regulations, Edition of 2020, Article 15 – Interferences. Geneva: ITU, 2020.
- Intertanko: Jamming and spoofing of Global Navigation Satellite Systems (GNSS). Intertanko, London, UK, 2019.
- ITU Radiocommunication Assembly Resolution 208 (Rev.WRC-19) – Protection of RNSS Frequencies from Harmful Interference, Geneva: ITU, 2019.
- Jak hakerom udało się zniszczyć sieć Internetu satelitarnego Viasat?, SAT Kurier, 2023. <https://satkurier.pl/news/230559/jak-hakerom-udalo-sie-zniszczyc-siec-internetu-satelitarnego-viasat.html>.
- Janes C4ISR & Mission Systems: Electronic Warfare. Yearbook 2023–2024.
- Julien O., Vulnerabilities of GNSS, the presentation for eKNOT, Ecole Nationale de l'Aviation Civile Toulouse 2018.
- Klawiter K., Drony spadają nad Bałtykiem. GPS zwariował. Kto za tym stoi?, YouTube, 2025 https://youtu.be/aQqpDQFhWtk?si=R_8thE-IVyGBr3WI.
- Krasucha-C4 w natarciu, czyli o tym jak Rosjanie zagłuszają sygnały GPS i telefonii komórkowej, Defence24, 2002, <https://defence24.pl/sily-zbrojne/krasucha-c4-w-natarciu-czyli-o-tym-jak-rosjanie-zaglushaja-sygnały-gps-i-telefonii-komorkowej>.
- Łobaza P., Kto zakłóca GPS w Polsce? Tak, dobrze myślisz, Telepolis, 2024. <https://www.telepolis.pl/wiadomosci/wydarzenia/sygnal-gps-polska-zaklocenia>.
- GPS anti-jamming: Building resilience to today's greatest threats - Spire: Global Data and Analytics, <https://spire.com/blog/space-reconnaissance/gps-anti-jamming-building-resilience-to-todays-greatest-threats/>.
- Makowiec R., Zakłócenia GPS w Polsce. Jakiego sprzętu może używać Rosja?, Cyberdefence24, 2024. <https://cyberdefence24.pl/armia-i-sluzby/zaklocenia-gps-w-polsce-jakiego-sprzetu-moze-uzywac-rosja>.
- Media: Rosja rozmieszcza w Kaliningradzie wielki „zagłuszacz”, system walki elektronicznej Murmańsk-BN, Polskie Radio24, 2019. <https://polskieradio24>.

- pl/artikul/2300338,media-rosja-rozmieszcza-w-kaliningradzie-wielki-zagluszacz-system-walki-elektronicznej-murmansk-bn.
- Norma ISO/IEC 27005, ISO, 2018.
- Owen T. J., Electronic interference in the Persian Gulf. MariTrace. <https://www.ww3.maritrace.com/post/electronic-interference-in-the-persian-gulf>.
- Palczewski S., Problemy z GPS w Polsce. O co tu chodzi?, Cyberdefence24, 2024. <https://cyberdefence24.pl/technologie/problemy-z-gps-w-polsce-o-co-tu-chodzi>.
- Panella C., A hidden electronic warfare battle is raging in Ukraine and demanding more from the soldiers fighting it, special drone unit says. Business Insider. <https://www.businessinsider.com/hidden-electronic-warfare-battle-demanding-more-of-ukrainian-soldiers-2025-2>.
- Papiernik W., Duże zakłócenia sygnału GPS w Polsce. Ostrzeżenie dla pilotów, Cyberdefence24, 2024. <https://cyberdefence24.pl/technologie/problemy-z-gps-w-polsce-o-co-tu-chodzi>.
- Pawłowicz K., Zakłócenia GPS w Polsce. Instytut Studiów nad Wojną zabrał głos, 2024. <https://www.tysol.pl/a116057-zaklocenia-gps-w-polsce-instytut-studiow-nad-wojna-zabral-glos>.
- Protecting commercial aircraft against GPS spoofing threats, Spirent Communications, 2022. <https://www.spirent.com/assets/ebook-protecting-commercial-aircraft-against-gps-spoofing-threats>.
- Rosjanie zakłócają sygnał GPS. ISW: To test systemów zagłuszających, pilsatnews.pl, 2024. <https://www.pilsatnews.pl/wiadomosc/2024-01-19/isw-rosjanie-zaklocaja-sygnał-gps-to-test-systemow-zagluszajacych/>.
- Shipping industry faces GPS disruption in Persian Gulf. Satelles, Inc. <https://satelles.com/shipping-industry-faces-gps-jamming-in-persian-gulf/>.
- Sokolenko P., GNSS signal monitoring. GPSPATRON. <https://gpspatron.com/gnss-signal-monitoring/>.
- UNCLOS, Article 87(2): States shall have due regard to the interests of other States in their exercise of the freedom of the high seas
- United Nations Convention on the Law of the Sea (UNCLOS), Montego Bay, 10 December 1982, Articles 87, 88, 301.
- Wnioski z rozmów z managerami lotnictwa ratunkowego, badanie własne, Warszawa, 2025.
- Wu D. L., Innovation: Recent GPS jamming in regions of geopolitical conflict. GPS World. <https://www.gpsworld.com/innovation-recent-gps-jamming-in-regions-of-geopolitical-conflict/>.
- Wu Z., Zhang Y., Yang Y., Liang C., Liu R. Spoofing and Anti-Spoofing Technologies of Global Navigation Satellite System: A Survey, IEEE Access, 2020.
- Wywiad ekspercki – badania geodezyjne z wykorzystaniem samolotów, badanie własne, Warszawa 2025.
- Zagrożenie katastrofą lotniczą w Polsce? Tajemnicze urządzenie z Rosji zakłóca sygnał GPS, Super express, 2024. <https://www.se.pl/wiadomosci/swiat/zagrozenie-katastrofa-lotnicza-w-polsce-tajemnicze-urządzenie-z-rosji-zakloca-gps-aa-AwTX-yGSN-GpY6.html>.
- Zmysłowski D., Jamming& spoofing in GNSS, Warszawa 2025.

