Cybersecurity and Law

2025 Nr 2 (14)

DOI: 10.34567/cal/215572

Selected Aspects of Air–Cyberspace Integration in Military Operations

Wybrane aspekty integracji działań powietrznych i działań w cyberprzestrzeni

Paweł MRÓZ
Akademia Sztuki Wojennej
ORCID: 0000-0001-9751-4574
E-mail:p.mroz@pracownik.akademia.mil.pl

Abstract

Modern air forces have become deeply dependent on cyberspace, now recognized as a critical integrator of all other domains. The digitalization means that effective air operations require support from both defensive and offensive cyber capabilities. Defensive cyberspace operations protect C5ISRT architectures and platform systems from disruption, manipulation, and degradation, which could undermine situational awareness and slow decision-making at best. Offensive cyberspace operations, such as digital SEAD, allow commanders to shape the battlespace, neutralize air defence networks, and create windows of opportunity for safe and effective employment of airpower, particularly in A2/AD environments.

The article emphasizes that cyberspace operations can significantly reduce the risk to air assets by suppression of enemy air defences, interfering with communications, and deceiving the adversary. Integrating cyberspace effects with air operations is increasingly essential for achieving air superiority against advanced, networked adversary systems. Historical cases such as Operation Orchard and Operation Midnight Hammer illustrate how cyberspace actions can serve as a force enabler, integrator, and multiplier, reinforcing the emerging concept of cyber-enabled air superiority.

Keywords
air warfare, air operations, cyberspace operations

Streszczenie

Współczesne siły powietrzne są w coraz większym stopniu zależne od działań w cyberprzestrzeni, która stała się równoprawną domeną operacyjną oraz kluczowym integratorem pozostałych domen operacyjnych. Cyfryzacja systemów dowodzenia, rozpoznania, łączności i wsparcia sprawia, że efektywne prowadzenie działań powietrznych wymaga zarówno obronnych, jak i ofensywnych zdolności w cyberprzestrzeni. Defensywne działania chronią systemy C5ISRT przed zakłóceniem, manipulacją i degradacją, których skutki mogłyby doprowadzić do utraty przewagi informacyjnej i spowolnienia procesów decyzyjnych. Z kolei ofensywne zdolności – takie jak manipulacja danymi, degradacja systemów przeciwnika czy cyfrowy SEAD – umożliwiają przygotowanie środowiska operacyjnego oraz stworzenie warunków do bezpiecznego użycia lotnictwa, szczególnie w prospektywnym środowisku A2/AD.

W artykule wskazano, że działania w cyberprzestrzeni mogą znacząco zmniejszyć ryzyko dla sił powietrznych, poprzez obezwładnienie systemów obrony powietrznej, zakłócenie łączności i dezinformację przeciwnika. Integracja działań w cyberprzestrzeni z działaniami komponentu powietrznego staje się niezbędna dla osiągania przewagi w powietrzu, zwłaszcza wobec zaawansowanych, sieciocentrycznych systemów przeciwnika. Przykłady takie jak operacje Orchard i Midnight Hammer pokazują, że działania w cyberprzestrzeni mogą pełnić rolę równorzędnego elementu zespołu uderzeniowego i stanowią fundament rozwijanej koncepcji cyber-enabled air superiority.

Słowa kluczowe

siły powietrzne, działania w cyberprzestrzeni, działania powietrzne

Wprowadzenie

Postępująca cyfryzacja sprawia, że efekty osiągane w cyberprzestrzeni i poprzez cyberprzestrzeń stanowią coraz ważniejszy czynnik determinujący funkcjonowanie sił powietrznych w bieżącej działalności i w operacji. Zapewnia on efektywne funkcjonowanie wszystkich podsystemów i realizację wymaganych funkcji przez siły powietrzne, w tym rozpoznania, dowodzenia, zabezpieczenia, użycia aktywnych środków walki w działaniach ofensywnych i obrony powietrznej. Współczesne działania komponentu powietrznego są ściśle powiązane z wykorzystaniem spektrum elektromagnetycznego, przetwarzaniem danych i wymianą informacji w wymiarze wewnętrznym i zewnętrznym. Można zakładać, że każde działanie bojowe będzie wspierane działaniami w cyberprzestrzeni. W literaturze przedmiotu panuje zgoda, że cyberprzestrzeń jest nie tylko integratorem działań w pozostałych domenach operacyjnych, ale także umożliwia ona ich prowadzenie oraz multiplikuje ich efektywność.

W artykule przedstawiono ważniejsze obszary, w których wsparcie sił powietrznych poprzez działania w cyberprzestrzeni jest niezbędne. Szczególną uwagę zwrócono na wywalczenie przewagi w powietrzu, które jest zadaniem numer jeden komponentu powietrznego w każdej operacji, realizowanym na korzyść całości sił połączonych. Znaczenie tego zadania oraz prognozowana trudność jego realizacji w prospektywnym środowisku operacyjnym pozwala wyciągnąć wniosek, że wsparcie z cyberprzestrzeni będzie konieczne w jego realizacji.

Wysiłki badawcze skupiono na udzieleniu odpowiedzi na pytanie: Jakie znaczenie mają działania w cyberprzestrzeni dla efektywności działań powietrznych? Tak sformułowane główne pytanie badawcze zdekomponowano

na pytania szczegółowe: W jaki sposób działania w cyberprzestrzeni wspierają osiąganie efektów przez siły powietrzne w operacji? Jakie są najważniejsze obszary integracji działań w cyberprzestrzeni i działań powietrznych w prospektywnych operacjach wojskowych? W celu rozwiązania tak zarysowanego problemu badawczego, w badaniach wykorzystano metody analizy literatury oraz prognozowania i abstrahowania. Ponadto, zastosowano analizę przypadku, w stosunku do operacji, w których zidentyfikowano aspekty tytułowej integracji oraz analizę funkcjonalną w odniesieniu do funkcji realizowanych przez siły wydzielone do działań powietrznych i w cyberprzestrzeni w ramach operacji wojskowych.

Znaczenie wsparcia działań powietrznych z cyberprzestrzeni

Włączenie cyberprzestrzeni do współczesnej doktryny i praktyki wojskowej jako równoprawnej domeny oznacza potwierdzenie jej decydującego znaczenia w operacjach militarnych, w tym działaniach powietrznych. Niegdyś, działania w cyberprzestrzeni postrzegane były jako zdolność pomocnicza w działaniach podsystemu dowodzenia sił powietrznych, a obecnie stanowią one kluczowy czynnik mogący znacząco wpływać na osiąganie sukcesów w operacji, aczkolwiek jednocześnie stanowią newralgiczną podatność. Współczesne działania powietrzne są uzależnione od rozległych ekosystemów cyfrowych, mających znaczenie dla prawdopodobnie wszystkich obszarów determinujących możliwości efektywnego użycia potęgi powietrznej. W efekcie można stwierdzić, że działania w cyberprzestrzeni są istotnym elementem operacyjnych podstaw wojny powietrznej XXI wieku. Istotne są wszystkie obszary wykorzystania cyberprzestrzeni, zarówno defensywne jak i ofensywne[1].

Działania obronne w cyberprzestrzeni obejmują wykrywanie i neutralizację zagrożeń dla systemów przetwarzania danych oraz aktywne odtwarzanie ich bezpieczeństwa po ataku. Neutralizacja zagrożeń może być realizowana w sposób reaktywny i aktywny, inwazyjny i nieinwazyjny. Istotą ofensywnych działań w cyberprzestrzeni jest przetwarzanie danych przeciwnika w systemach lub w odniesieniu do tych systemów albo w cyberprzestrzeni, nad którą kontrolę ma przeciwnik. Poprzez ich realizację obezwładniania się, manipuluje oraz przygotowuje się środowisko operacyjne. W efekcie atakowany system przetwarzania danych np. ma ograniczaną funkcjonalność, trwale przestaje funkcjonować, zawiera intencjonalnie zmienione dane lub nie może być w pełni kontrolowany przez przeciwnika. Najkosztowniejsze oraz najbardziej czasochłonne są działania przygotowania środowiska pod kątem wykorzystania go w przyszłych operacjach, co wynika z trudności długotrwałego prowadzenia skrytych działań po przeniknięciu do systemów przetwarzania danych przeciwnika. Są to jednak wysiłki najbardziej pożądane z punktu widzenia uzyskiwanych efektów w operacji[2].

Obecnie, działania w cyberprzestrzeni potencjalnie mogą zapewniać dowódcy komponentu powietrznego istotne efekty mające znaczenie w walce o przewagę w powietrzu, która jest warunkiem koniecznym możliwości wykorzystania przestrzeni powietrznej i jednym z najniebezpieczniejszych

[1] C. Melella, Coordination in Offensive and Defensive Cyberoperations: Dissecting China, Russia, and NATO's Approaches in Cyberspace, University of Genoa, Genua 2024, https://tesidottorato.depositolegale.it/bitstream/20.500.14242/184682/1/phdunige_5157198.pdf.
[2] DD-3.20 Operacje w cyberprzestrzeni, CDiSZ, Bydgoszcz 2020, s. 3-10.

działań powietrznych. Uprzednio, walka o przewagę w powietrzu była prowadzona jedynie przez organiczne środki komponentu powietrznego, a w głównej mierze statki powietrzne. Następnie, do wsparcia działań tego typu zaczęto wykorzystywać środki oddziaływania o dużych zasięgach komponentów lądowego i morskiego oraz zespoły bojowe wojsk specjalnych.

W szczególności, obezwładnienie naziemnych systemów obrony powietrznej przeciwnika poprzez działania w cyberprzestrzeni (Digital/Cyber SEAD) pozwala na osiąganie tradycyjnych celów działań komponentu powietrznego innowacyjnymi metodami. Zakłócanie systemów łączności i wsparcia dowodzenia przeciwnika, ingerowanie w przesyłane dane lub fałszowanie danych na różnych etapach procesu rozpoznania i rażenia (kill chain) pozwala osiągnąć przewagę w powietrzu bez konieczności wprowadzania środków walki, zwłaszcza załogowych, w przestrzeń oddziaływania systemów walki przeciwnika. To pozwala na zmniejszenie ryzyka dla załóg statków powietrznych i ograniczenie wysiłku lotnictwa przedzielonego do zadań SEAD[3].

Jednak skuteczne wykorzystanie takich działań w cyberprzestrzeni wymaga informacji rozpoznawczych w czasie rzeczywistym i uprzednio uzyskanego dostępu do systemów bazujących na oprogramowaniu komputerowym i spektrum elektromagnetycznym. Należy mieć świadomość, że takie wymagania są trudne do zrealizowania ze względu na ulotny charakter takich okazji, chociażby ze względu na priorytetowo traktowane defensywne działania przeciwnika w cyberprzestrzeni. Należy spodziewać się istotnych trudności w synchronizacji uzyskania efektów w obu domenach co powoduje niepewność i wzrost ryzyka działań powietrznych[4].

Udana integracja działań w cyberprzestrzeni i w innych domenach ukierunkowanych na osiąganie efektów w operacji przez komponent powietrzny zależy od synchronizacji stwarzanych warunków składających się na synergistyczne efekty. W szczególności w odniesieniu do sił powietrznych, wymagana dokładność synchronizacji jest relatywnie duża i może sięgać kilku lub kilkunastu minut. Jest to związane z wykorzystywaniem przestrzeni powietrznej oraz spektrum elektromagnetycznego przez środki walki sił powietrznych. Ich charakterystyki, wraz z zaawansowaniem technologicznym wykorzystujących je środków walki, są determinantami atrybutów sił powietrznych, w szczególności prędkości działań, zasięgu i zdolności do manewru w trzech wymiarach. W efekcie, działania środków walki sił powietrznych charakteryzowane są jako relatywnie wszechobecne, zdolne do szybkiej koncentracji, szybkiego przenoszenia wysiłku i szybkiej zmiany celów działań. Jednocześnie jednak posiadają one ograniczenia, z których należy przytoczyć nieciągłość działań, wynikającą z ograniczonego udźwigu. Względnie niewielka ilość paliwa zabieranego przez środki napadu powietrznego przekłada się na ograniczony czas ich przebywania w przestrzeni powietrznej. Precyzyjny dobór okien czasowych do realizacji poszczególnych działań ma kluczowe

[3] S.E. Dean, Killer Code: Cyber-Supported SEAD, European Security and Defence, https://euro-sd.com/2021/08/articles/exclusive/23246/cyber-supported-sead/#; [dostęp: 16.09.2021]; J. Speed, P. Stathopoulos, SEAD Operations of the Future. The Necessity of Jointness, "Journal of the JAPCC" 2018, no. 26, s. 38.

[4] F.A.H. Pedersen, J.T. Jacobsen, Narrow Windows of Opportunity: The Limited Utility of Cyber Operations in War, "Journal of Cybersecurity" 2024, vol. 10(1), https://doi.org/10.1093/cybsec/tyad023.

znaczenie dla bezpieczeństwa sił i efektywności osiągania efektów przez komponent powietrzny[5].

Istotnym wsparciem dla działań sił powietrznych są działania w cyberprzestrzeni związane z zakłócaniem i manipulacją danych nawigacyjnych przeciwnika, w tym nawigacji satelitarnej. Prowadzenie takich działań może doprowadzić do chaosu w systemie obrony powietrznej przeciwnika, w tym do utraty świadomości sytuacyjnej na stanowiskach kierowania walką, a nawet porażenia sił własnych w ramach tzw. ognia bratobójczego. Szczególnie pożądanymi efektami byłyby brak reakcji systemów obrony powietrznej przeciwnika, w tym lotnictwa, spowodowanie ich przedwczesnej reakcji (wzbudzenia) oraz skierowanie wysiłku w niewłaściwy region.

Znaczenie cyberprzestrzeni dla sił powietrznych wyraża się również w uzależnieniu od tej domeny i w powstających z tego względu niezwykle istotnych podatnościach, które wykorzystane przez przeciwnika mogą powodować skutki katastrofalne dla komponentu powietrznego. Cyberataki mogą zakłócić planowanie misji lotniczych, pogorszyć lub zniekształcić świadomość sytuacyjną, a także zagrozić bezpieczeństwu misji lotniczych. Konflikt na Ukrainie potwierdził, że siły powietrzne są jednymi z pierwszych celów współczesnych działań wojennych, a działania ofensywne w cyberprzestrzeni poprzedzają działania kinetyczne ukierunkowane na obniżenie ich zdolności[6]. Celami są przede wszystkim systemy utrzymania świadomości sytuacyjnej i dowodzenia. Rosnące wykorzystanie bezzałogowych systemów powietrznych (UAS)[7] i Internetu rzeczy na polu walki (IoBT – Internet of Battle Things)[8] oraz fakt, że platformy załogowe również są nasycone oprogramowaniem dodatkowo zwiększa liczbę potencjalnych celów cyberataków[9].

Podatność jest także wynikiem zasad dowodzenia działaniami powietrznymi, wśród których jest scentralizowanie dowodzenia na najwyższym zasadnym szczeblu oraz zdecentralizowanie realizacji działań. Wprowadzenie w życie tej zasady pozwala traktować bezpieczne i skuteczne systemy wsparcia dowodzenia jako jedne z kluczowych wymagań własnego środka ciężkości lub elementem, bez którego funkcja dowodzenia nie może być zapewniona (tzw. single point of failure). Architektura systemów C5ISRT, umożliwiających dowodzenie, kontrolę działań, łączność, ISR oraz targeting, stanowi bowiem złożony system nerwowy sił powietrznych. Jej znaczenie, złożoność i wzajemna zależność podsystemów sprawiają, że jest ona zarówno niezbędna, jak i podatna na zagrożenia.

Jej podatność jest także wynikiem coraz większego skomplikowania tych systemów C5ISRT oraz wykorzystywania najnowszych rozwiązań sprzętowych i przetwarzania danych[10]. Ponadto, jak pokazuje konflikt ukraińsko-rosyjski,

[5] AJP-3.3(B) Allied Joint Doctrine for Air and Space Operations, NSO, Bruksela 2016.
[6] V. C. Onesimiuc, Influence of Cyber Dimension on Air Force Activities Case Study: The Conflict in Ukraine, "Romanian Military Thinking" 2023, https://doi.org/10.55535/rmt.2023.4.10.
[7] Z.X. Wang, i in., A survey on cybersecurity attacks and defenses for unmanned aerial systems, "Journal of Systems Architecture" 2023, vol. 138, https://doi.org/10.1016/j.sysarc.2023.102870.
[8] L. Zhu, S. Majumdar, C. Ekenna, An invisible warfare with the internet of battlefield things: A literature review, "Human Behavior and Emerging Technologies" 2021, vol. 3, https://doi.org/10.1002/hbe2.231.
[9] L. Cwojdziński, Cybersecurity of United States Air Force Weapons Systems – Ensuring Mission Security, "Przegląd Komunikacyjny" 2023, https://doi.org/10.35117/a_eng_23_05_01.
[10] H. Ahmad i in., A review on C3I systems' security: vulnerabilities, attacks, and countermeasures, "ACM Computing Surveys", vol. 55, Issue 9, Article No. 192,

w miarę przedłużania się operacji, strony adaptują swoje systemy bez możliwości ich testowania w warunkach laboratoryjnych, a także poszerzają możliwości ich kompatybilności programowej i sprzętowej. Co więcej, na niższych szczeblach taktycznych wyzwaniem jest fakt nadania wyższego priorytetu dla dostępności aplikacji, co budzi wątpliwości i rodzi wyzwania w zakresie bezpieczeństwa w cyberprzestrzeni[11].

Znaczenie niezawodności systemów C5ISRT jest związane z tym, że bezpieczeństwo i efektywność kampanii powietrznych zależą od nieprzerwanego przepływu danych w czasie quasirzeczywistym między sensorami, stanowiskami dowodzenia i aktywnymi środkami walki. Zakłócanie, infekcja złośliwym oprogramowaniem, czy manipulacja danymi, może doprowadzić do załamania hermetyczności i integralności systemu, przegrania z przeciwnikiem w rywalizacji w ramach pętli decyzyjnych OODA (observe, orient, decide, act) oraz uniemożliwienia osiągnięcia wskazanych komponentowi powietrznemu celów[12].

Z punktu widzenia efektywności, w skoordynowanych działaniach połączonych wystarczyć może zaledwie to, że takie niepożądane działania obniżą szybkość podejmowania decyzji poprzez wywołanie dezorientacji wśród operatorów środków walki i dowódców. Te efekty są multiplikowane w specyficznych sytuacjach, np. gdy atak cybernetyczny jest nieuświadomiony i nieoczekiwany przez personel. Zjawisko to może zachodzić w sytuacji ataku przypominającego awarię sprzętu lub oprogramowania (ang. effect of non-atribution) i jego największy potencjał występuje przed rozpoczęciem jawnych działań zbrojnych, a także w dniu ich rozpoczęcia tj. w tzw. dniu zero[13].

Zagrożenia prowadzące do takich rezultatów mogą być przygotowane i przeprowadzone się na wielu poziomach. Dla przykładu, na poziomie sieci ataki typu man-in-the-middle mogą przechwytywać dane lub przekierowywać przepływ informacji. Na poziomie sprzętowym zagrożenie mogą stanowić ukryte backdoory. Nasilenie takiego zagrożenia wynika m.in. z faktu, że siły zbroje wykorzystują sprzęt i podzespoły dostępne na rynku cywilnym. Są one produkowane i dostarczane w łańcuchach dostaw przez firmy, które nie mają obowiązku dochowania najwyższych standardów bezpieczeństwa, co umożliwia wprowadzenie ukrytych modyfikacji do potencjalnego wykorzystania w przyszłości. Podobnie jest na poziomie oprogramowania, gdzie względnie oczywistym sposobem jest ukrycie fragmentu złośliwego kodu. Po uaktywnieniu takich zmian przeciwnik uzyska możliwości atakowania systemów komputerowych, np. platform bojowych poprzez modyfikowanie danych celów lub dostarczanie fałszywych danych telemetrycznych. W ogólności, znaczące zagrożenia płyną z również faktu wykorzystywania przez siły zbrojne państw sprzętu starych typów. Próba integracji go w sieciach w ramach systemu walki może prowadzić do zagrożenia dla pozostałych elementów ugrupowania[14].

---

https://doi.org/10.1145/3558001; E. Cieślak, Air Defense of the Baltic States: Looking toward the Future, "Safety & Defense" 2021, vol. 7(2), s. 12-21, https://doi.org/10.37105/sd.158.

[11] V. Putrenko, N. Pashynska, Military Situation Awareness: Ukrainian Experience, "Applied Cybersecurity & Internet Governance" 2024, vol. 3, no. 1, doi:10.60097/ACIG/190341.

[12] B. Jensen, Operational Art in the Age of Battle Networks, [w:] S.G. Jones, S.P. Daniels, War and the Modern Battlefield. Insights from Ukraine and the Middle East, CSIS, New York 2025, s. 35.

[13] The Fog of the day zero, JAPCC Conference Proceedings, Kalkar 2018.

[14] M. Schulze, Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations, [w:] Jančárková T. i in., 20/20 Vision: The Next Decade, NATO CCDCOE Publications, Tallinn 2020, s. 183-194.

Biorąc pod uwagę powyższe uwarunkowania należy wskazać, że skuteczne, adaptacyjne i odporne działania defensywne w cyberprzestrzeni są podstawowym oczekiwaniem sił powietrznych w stosunku do specjalistów ds. cyberprzestrzeni. Lista koniecznych czynności jest długa[15], ale warto zwrócić uwagę na zabezpieczenie przed hakerami systemów CNS w lotnictwie (Communication, Navigation, Surveillance), tj. łączności, nawigacji i dozorowania ruchu lotniczego. Systemy te są niezbędne do wydajnego zarządzania ruchem lotniczym poprzez zapewnienie świadomości w relacjach pomiędzy załogami statków powietrznych, załogami i nawigatorami naprowadzania lub kontrolerami ruchu lotniczego oraz pomiędzy dowodzącymi działaniami różnych sił wykorzystujących przestrzeń powietrzną (również spoza komponentu powietrznego). W literaturze przedmiotu podkreśla się również znaczenie zapobiegania wyciekom wrażliwych informacji, zagwarantowania ograniczenia dostępu do sprzętu i danych o znaczeniu krytycznym osobom niepowołanym oraz ochrony systemów rażenia przed zdalną ingerencją. Z kolei zapewnienie zdolności do podtrzymania działań powietrznych jest związane z koniecznością zabezpieczenia przed ingerencją takich systemów jak zasilania, paliwowych i logistycznych w bazach lotniczych, w innych miejscach do startów i lądowań oraz w jednostkach sił powietrznych innych niż lotnicze (radiotechnicznych, obrony przeciwlotniczej i przeciwrakietowej).

Potencjalne obszary wykorzystania cyberprzestrzeni do wsparcia działań powietrznych

Jawne źródła nie dostarczają zbyt wielu, szczegółowo przedstawionych przykładów wsparcia bojowych działań powietrznych przez działania w cyberprzestrzeni. Jednym z wyjątków jest operacja Orchard, której istotą był izraelski nalot na syryjski obiekt jądrowy Al-Kibar w 2007 r. Jest on szeroko omawianym przykładem zintegrowania działań w cyberprzestrzeni, rozpoznania radioelektronicznego (SIGINT – signals intelligence) i walki elektronicznej z ofensywną operacją powietrzną. Izrael wykorzystał działania w cyberprzestrzeni jako kluczowy element pozwalający lotnictwu wejść w silnie chronioną przestrzeń powietrzną bez wykrycia przez systemy rozpoznania przestrzeni powietrznej. Najważniejszym elementem wsparcia było stworzenie przeciwnikowi fałszywego obrazu sytuacji powietrznej. Najprawdopodobniej poprzez ingerencję w systemy radarowe i dowodzenia syryjskiej obrony przeciwlotniczej, izraelskie służby miały doprowadzić do tego, że operatorzy nie mieli na wskaźnikach zobrazowania izraelskich statków powietrznych, F-15I i F-16I, które wykonywały lot w syryjskiej przestrzeni powietrznej[16].

W operacji najprawdopodobniej wykorzystano oprogramowanie o nazwie Senior Suter, umożliwiające zarówno infiltrację, jak i manipulację danymi w radarach oraz przejęcie danych lub zakłócenie łączności. Taka metoda, w literaturze izraelskiej nazywana elektronicznym sabotażem, pozwoliła na zachowanie pełnej skrytości nalotu. Samoloty mogły wlecieć głęboko w syryjską przestrzeń powietrzną bez konieczności fizycznego niszczenia i zakłócania stacji radiolokacyjnych i elementów naziemnych systemów przeciwlotniczych

[15] Air Force Cyber Security: Key Threats and Solutions, SHH Academy, https://www.ssh.com/academy/air-force-cyber-security-key-threats-and-solutions?utm_source=chatgpt.com [dostęp: 01.10.2025].

[16] D.A. Fulghum, R. Wall, A. Butler, Israel Shows Electronic Prowess, "Aviation Week", https://archive.aviationweek.com/issue/20071126, [dostęp: 16.11.2007].

z powietrza, co podniosłoby alarm. W praktyce był to "cyberodpowiednik" działań SEAD, lecz przeprowadzony bez użycia rakiet antyradiolokacyjnych i zakłócania z powietrza[17].

Drugą ważną warstwą wsparcia był wymiar informacyjno-rozpoznawczy. Izrael mógł wykorzystać cyberprzestrzeń jako narzędzie do wcześniejszego rozpoznania struktury syryjskich systemów OPL i ich podatności w ramach działań o charakterze przygotowania środowiska operacyjnego. Być może poznano luki w systemie rażenia i rozpoznania na odpowiednich wysokościach. To umożliwiło precyzyjne zaplanowanie momentu ataku, tras lotu oraz skoordynowanie wszystkich etapów operacji. Działania w cyberprzestrzeni zapewniły zatem zarówno taktyczne zneutralizowanie przeciwnika w czasie nalotu, jak i przygotowanie całej operacji powietrznej, zwiększając bezpieczeństwo załóg oraz prawdopodobieństwo powodzenia.

Niektórzy autorzy wskazują na moralne zalety działań ofensywnych w cyberprzestrzeni w porównaniu do kinetycznych metod działania. W ataku w Syrii działania w cyberprzestrzeni pozwoliły na precyzyjne osiągnięcie celu bez zbędnego rozlewu krwi[18]. W przeciwieństwie do tego rozwiązania, jedno z pierwszych uderzeń lotniczych w ramach operacji Pustynna Burza było skierowane na Bagdad. Porażono elementy systemu łączności odcinając irackie dowództwo od jednostek w polu. Bombę skierowano do kanału klimatyzacji w centrum miasta.

Operacja Orchard pokazała, że działania w cyberprzestrzeni mogą wspierać lotnictwo stanowiąc czynnik zwielokratniający jego możliwości (force multiplier) w skali operacyjnej. Obezwładniono systemy obrony powietrznej państwa, pozwalając tym samym na wykonanie misji, która być może byłaby niemożliwa do zrealizowania przy użyciu wyłącznie tradycyjnych środków. Przytoczony przykład, choć odosobniony w zakresie rozmachu, pokazuje potencjał działań w cyberprzestrzeni i pozwala przenieść dyskusję o potencjale działań ofensywnych w cyberprzestrzeni ze sfery domysłów do faktów.

Jedną z konsekwencji przytoczonych działań w Syrii był rozwój koncepcji zintegrowanej walki o przewagę powietrzną z wykorzystaniem działań w cyberprzestrzeni, określanej jako Cyber-Enabled Air Superiority. Koncepcje te, choć niejawne w szczegółach, są wzmiankowane w literaturze przedmiotu, piśmiennictwie specjalistycznym oraz dokumentach doktrynalnych i formalnych, umacniając pozycję cyberprzestrzeni jako integratora, domeny zwielokratniającej zdolności i umożliwiającej realizację wielu działań w innych domenach (ang. enabler, integrator, force multiplier)[19].

Nadzieje w związku z potencjalnym wsparciem walki o przewagę w powietrzu wynikają z wyzwań jakie stawiają przez potęgą powietrzną silne systemy antydostępowe (A2/AD – Anti Access/Area Denial) rozbudowywane przez takie państwa jak Rosja. Obezwładnienie lub przełamanie tych systemów wydaje się trudnym i ryzykownym zadaniem, ale niezbędnym dla możliwości zapewnienia swobody manewru w domenach powietrznej, lądowej i morskiej. Trudność wynika z wykorzystywania w systemie A2/AD zaawansowanych

[17] J. Healey, Cyber Effects in Warfare: Categorizing the Where, What, and Why, "Texas National Security Review" 2024, vol. 7, Issue 4, s. 37-50, https://tnsr.org/2024/08/cyber-effects-in-warfare-categorizing-the-where-what-and-why.

[18] D.E. Denning, Stuxnet: what has changed, "Future Internet" 2012, vol. 4, s. 676, doi:10.3390/fi4030672.

[19] G. Ashworth, D.W. Alvin, B.C. Saltzman, Department of the Air Force Posture Statement. Fiscal Year 2026, Departmet of the Air Force, Waszyngton 2025, s. 5.

środków dalekiego zasięgu w zakresie rozpoznania, w tym satelitarnych, a także rażenia, które najprawdopodobniej będą zintegrowane poprzez wpięcie ich w sieć informacyjną i powiązanie z redundantnymi stanowiskami dowodzenia. Tworzy to tzw. transparentne pole walki, w którym trudno będzie o skryte podejście i zaskoczenie przeciwnika przy sprawnym jego podsystemie rozpoznania przestrzeni powietrznej. Ponadto, obrona przeciwlotnicza z pewnością będzie wielowarstwowa, co uniemożliwi wlot na każdej wysokości. Należy się również spodziewać, że istotne węzły takiego systemu będą rozproszone, silnie bronione i w miarę możliwości znacznie oddalone od linii styczności wojsk (od granicy), a przez to trudnodostępne dla większości środków napadu powietrznego. Wydaje się zatem, że uzasadnione jest niewykluczanie i rozwijanie sposobów wykorzystania ofensywnych zdolności w cyberprzestrzeni do stworzenia korzystnych warunków. Warunki te zapewniłyby okna czasowe i przestrzenne umożlwiające przetrwanie lotnictwu i środkom rażenia, w tym dalekiego zasięgu, takich jak JASMM ER. Umożliwiałoby to osiąganie znaczących efektów przez lotnictwo np. poprzez realizację tzw. pulse air operations (działań udarowych)[20].

Siły Powietrzne USA poszły o krok dalej uważając, że przyszłe konflikty będą wymagały posiadania organicznych, taktycznych zdolności ofensywnych w cyberprzestrzeni i organizują skrzydło odpowiedzialne za to zadanie. Przeznaczenie tych sił ma być ograniczone do wsparcia działań lotnictwa. Zdolności będą generowane w skali taktycznej z wykorzystaniem możliwości oddziaływania w cyberprzestrzeni przez samoloty piątej i szóstej generacji wykonane w technologii STEALTH. Będą one uzupełniały się wzajemnie ze zdolnościami sił powietrznych w zakresie walki radioelektronicznej i operacji informacyjnych. Głównie chodzi o lotnictwo taktyczne i samoloty F-35 i F-22, aczkolwiek należy spodziewać się, że dołączą do nich bezzałogowe statki powietrzne wykonane w technologii STEALTH, takie jak prototypy rozwijane w ramach programu Collaborative Combat Aircraft. Ich przeznaczeniem ma być zwielokrotnienie wskaźników bojowych i możliwości przetrwania samolotów załogowych poprzez operowanie w roli tzw. lojalnego skrzydłowego[21]. Powyższą decyzję podjęto na podstawie wyników gier wojennych. Przyjęto, że istniejące dowództwo ds. działań w cyberprzestrzeni – US Cyber Command – będzie koncentrować się na efektach o znaczeniu strategicznym i operacyjnym. Tym samym, nie będzie ono w stanie wspierać realizacji podstawowych zadań sił powietrznych przy wykorzystaniu tak specjalistycznych środków walki jak np. F- 5[22].

Przykładem wprowadzenia w życie tego podejścia była operacja Midnight Hammer, w ramach której Siły Powietrzne USA najprawdopodobniej skorzystały ze wsparcia zarówno US Cyber Command jak i własnych, organicznych zasobów oddziaływania w cyberprzestrzeni. Należy podkreślić, że cele tej operacji miały znaczenie strategiczne i związane były z zatrzymaniem rozwoju programu nuklearnego Iranu. W ramach ich realizacji, w dniu 21 czerwca 2025 r. przeprowadzono uderzenia na trzy obiekty infrastruktury irańskiego programu

[20] P.J. MacKenzie, NATO Joint Air Power and Offensive Cyber Operations, Joint Air Power Competence Centre, Kalkar 2017, s. 9-11.
[21] E. Cieślak, Unnamed Aircraft Systems: Challenges to Air Defense, "Safety & Defense" 2021, vol. 7(1), s. 72-78, https://doi.org/10.37105/sd.110.
[22] M. Pomerleau, ‘This is overdue’. Air Force creating tactical cyber capabilities to ensure air superiority, https://defensescoop.com/2024/05/23/air-force-creating-tactical-cyber-capabilities-ensure-air-superiority, [dostęp: 23.05.2024].

jądrowego wykorzystując m.in. siedem samolotów B-2 i ponad 24 rakiety Tomahawk do zadań uderzeniowych oraz ponad 125 samolotów do zadań wspierających. Wśród nich były F-35, które realizowały zadania osłony samolotów uderzeniowych m.in. w ramach misji SEAD, prowadząc oddziaływanie w spektrum elektromagnetycznym (oprócz działań kinetycznych)[23]. Na podstawie szczątkowych doniesień prasowych można wnioskować, że do obezwładnienia obrony powietrznej Iranu oraz systemów łączności w rejonach przelotu i ataku w znaczącym stopniu wykorzystano również strategiczne środki podległe dowództwu US Cyber Command. Analizując złożoność tej operacji można zgodzić się, że działania w cyberprzestrzeni mają potencjał do stanowienia nie tylko elementu wsparcia, ale równoprawnego członka zespołu uderzeniowego lotnictwa. Co więcej, przy okazji informowania o przebiegu tych działań przez przedstawicieli sił zbrojnych USA potwierdzono, że współcześnie żadne operacje wojskowe Stanów Zjednoczonych, w tym działania sił powietrznych, nie są realizowane bez wsparcia z cyberprzestrzeni, zwłaszcza w nieprzyjaznym i zdegradowanym środowisku. Operacja Midnight Hammer stanowi zatem kolejny przykład zintegrowania i zsynchronizowania działań w obu domenach – cyberprzestrzeni i powietrznej[24].

Podsumowanie

Skuteczne działania obronne w cyberprzestrzeni są warunkiem sine qua non zapewnienia funkcjonowania sił powietrznych w dzisiejszym, ucyfrowionym świecie. Jednakże w świetle prognozowanych charakterystyk przyszłego środowiska operacyjnego siły powietrzne potrzebują głębokiej integracji również z ofensywnymi działaniami w cyberprzestrzeni. Jednym z najistotniejszych zadań do wspólnej realizacji z wykorzystaniem obu domen jest walka o przewagę w powietrzu prowadzona w warunkach oddziaływania środków systemu A2/AD przeciwnika. Zadanie to jest warunkiem wstępnym do zapewnienia swobody działań we wszystkich domenach, a zatem powinno mieć wysoki priorytet wśród celów na poziomie operacyjnym. Z tego względu, niezbędne jest rozwijanie zdolności do wsparcia komponentu powietrznego w cyberprzestrzeni w ramach koncepcji cyber-enabled air superiority.

Przygotowanie działań w cyberprzestrzeni do tego typu wsparcia wymaga wcześniejszego, długotrwałego dostępu do systemów przetwarzania danych przeciwnika („ciągłej obecności") i znaczących kosztów. Co więcej, te nakłady mogą zostać zaprzepaszczone, ponieważ ciągle istnieje ryzyko związane z nagłą utratą dostępu w sytuacji wykrycia i usunięcia luk przez przeciwnika. Koszty mogą być trudne do zaakceptowania również w związku ze świadomością, że wygenerowane przez nie efekty zwykle będą wykorzystane tylko raz. Niemniej, uprawnionym wydaje się być sąd, że znaczenie wywalczenia odpowiedniego stopnia kontroli przestrzeni powietrznej uzasadnia tak duże nakłady, a korzyści z wywalczenia przewagi w powietrzu są trudne do przecenienia.

[23] J.A. Tirpak, Air Force Confirms SEAD Role of F-35s in Midnight Hammer, https://www.airandspaceforces.com/air-force-sead-role-f-35s-midnight-hammer/?utm_source=chatgpt.com. [dostęp: 21.11.2025].

[24] M. Pomerleau, Cyber Command supports strikes on Iran's nuclear facilities, but officials keep details under wraps, https://defensescoop.com/2025/06/23/cyber-command-supports-attack-iran-nuclear-facilities-midnight-hammer/?utm_source=chatgpt.com, [dostęp:23.06.2025].

Bibliografia

Ahmad H. i in., A review on C3I systems' security: vulnerabilities, attacks, and countermeasures, "ACM Computing Surveys", vol. 55, Issue 9, Article No. 192, https://doi.org/10.1145/3558001.

Air Force Cyber Security: Key Threats and Solutions, SHH Academy, https://www.ssh.com/academy/air-force-cyber-security-key-threats-and-solutions?utm_source=chatgpt.com.

AJP-3.3(B) Allied Joint Doctrine for Air and Space Operations, NSO, Bruksela 2016.

Ashworth G., Alvin D.W., Saltzman B.C., Department of the Air Force Posture Statement. Fiscal Year 2026, Departmet of the Air Force, Waszyngton 2025.

Cieślak E., Air Defense of the Baltic States: Looking toward the Future, "Safety & Defense" 2021, vol. 7(2), https://doi.org/10.37105/sd.158.

Cieślak E., Unnamed Aircraft Systems: Challenges to Air Defense, "Safety & Defense" 2021, vol. 7(1), https://doi.org/10.37105/sd.110.

Cwojdziński, L., Cybersecurity of United States Air Force Weapons Systems – Ensuring Mission Security, "Przegląd Komunikacyjny" 2023, https://doi.org/10.35117/a_eng_23_05_01.

DD-3.20 Operacje w cyberprzestrzeni, CDiSZ, Bydgoszcz 2020.

Dean S.E., Killer Code: Cyber-Supported SEAD, https://euro-sd.com/2021/08/articles/exclusive/23246/cyber-supported-sead/#.

Denning D.E., Stuxnet: what has changed, "Future Internet" 2012, vol. 4, doi:10.3390/fi4030672.

Fulghum D.A., Wall R., Butler A., Israel Shows Electronic Prowess, "Aviation Week", https://archive.aviationweek.com/issue/20071126.

Healey J., Cyber Effects in Warfare: Categorizing the Where, What, and Why, "Texas National Security Review" 2024, vol. 7, Issue 4, https://tnsr.org/2024/08/cyber-effects-in-warfare-categorizing-the-where-what-and-why.

Jensen B., Operational Art in the Age of Battle Networks, [w:] S.G. Jones, S.P. Daniels, War and the Modern Battlefield. Insights from Ukraine and the Middle East, CSIS, New York 2025.

MacKenzie P.J., NATO Joint Air Power and Offensive Cyber Operations, Joint Air Power Competence Centre, Kalkar 2017.

Melella, C., Coordination in Offensive and Defensive Cyberoperations: Dissecting China, Russia, and NATO's Approaches in Cyberspace, University of Genoa, Genoa 2024, https://tesidottorato.depositolegale.it/bitstream/20.500.14242/184682/1/phdunige_5157198.pdf

Onesimiuc V.C., Influence of Cyber Dimension on Air Force Activities Case Study: The Conflict in Ukraine, "Romanian Military Thinking" 2023, https://doi.org/10.55535/rmt.2023.4.10.

Pedersen F.A.H., Jacobsen J.T., Narrow Windows of Opportunity: The Limited Utility of Cyber Operations in War, "Journal of Cybersecurity" 2024, vol. 10(1), https://doi.org10.1093/cybsec/tyad023.

Pomerleau M., 'This is overdue'. Air Force creating tactical cyber capabilities to ensure air superiority, https://defensescoop.com/2024/05/23/air-force-creating-tactical-cyber-capabilities-ensure-air-superiority.

Pomerleau M., Cyber Command supports strikes on Iran's nuclear facilities, but officials keep details under wraps, https://defensescoop.com/2025/06/23/cyber-command-supports-attack-iran-nuclear-facilities-midnight-hammer/?utm_source=chatgpt.com.

Putrenko V., Pashynska N., Military Situation Awareness: Ukrainian Experience, "Applied Cybersecurity & Internet Governance" 2024, vol. 3, no. 1, doi:10.60097/ACIG/190341.

Schulze M., Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations, [w:] T. Jančárková i in., 20/20 Vision: The Next Decade, NATO CCDCOE Publications, Tallinn 2020.

Speed J., Stathopoulos P., SEAD Operations of the Future. The Necessity of Jointness, "Journal of the JAPCC" 2028, ed. 26.

Tirpak J.A., Air Force Confirms SEAD Role of F-35s in Midnight Hammer, https://www.airandspaceforces.com/air-force-sead-role-f-35s-midnight-hammer/?utm_source=chatgpt.com.

The Fog of the day zero – Joint Air & Space in the Vanguard, JAPCC Conference Proceedings, Kalkar 2018.

Wang Z.X., i in., A survey on cybersecurity attacks and defenses for unmanned aerial systems, "Journal of Systems Architecture" 2023, vol. 138, https://doi.org/10.1016/j.sysarc.2023.102870.

Zhu L., Majumdar S., Ekenna C., An invisible warfare with the internet of battlefield things: A literature review, "Human Behavior and Emerging Technologies" 2021, vol. 3, https://doi.org/10.1002/hbe2.231.