

ROZWÓJ SZTUCZNEJ INTELIGENCJI A AUTOMATYZACJA DOWODZENIA

Sztuczna Inteligencja (SI, zamiennie AI¹) oraz automatyzacja (zautomatyzowane systemy dowodzenia - ZSyD) stanowią jedno z najdynamiczniej rozwijających się dziedzin technologii teleinformatycznych w XXI wieku. Ich zastosowanie na Węzłach Łączności (WL), takich jak sieci komunikacyjne, infrastruktura telekomunikacyjna oraz Internet Rzeczy (IoT), stwarza zarówno nowe możliwości, jak i wyzwania. Węzły Łączności są kluczowym elementem Stanowiska Dowodzenia (SD), a ich unowocześnianie ma ogromne znaczenie dla pododdziałów, organów dowodzenia i pracy elementów infrastruktury Sił Zbrojnych i Instytucji MON.

Optymalizacja przepustowości

Zastosowanie sztucznej inteligencji na Węzłach Łączności umożliwi optymalizowanie zarządzania przepustowością sieci. Algorytmy SI mogą analizować i przewidywać wzorce ruchu sieciowego, przydzielając zasoby tam, gdzie są najbardziej potrzebne. Dzięki temu użytkownicy korzystają z bardziej stabilnego łącza, a cała infrastruktura działa efektywniej.

Systemy oparte na AI mogą monitorować stan sieci w czasie rzeczywistym, wykrywać i reagować na awarie oraz przeprowadzać konserwację predykcyjną². To z kolei redukuje czas od zgłoszenia awarii lub niesprawności do WOG'u³ do jej naprawy.

Implementacja zaawansowanych technologii sztucznej inteligencji (AI) oraz automatyzacji dowodzenia i kierowania walką na Węzłach Łączności jest procesem złożonym. Wymaga to adaptacji istniejącej infrastruktury i zapewnienia zgodności systemów, badaniem i testowaniem protokołów, co wiąże się często z wysokimi nakładami finansowymi oraz koniecznością posiadania specjalistycznej wiedzy przez administratorów, techników komputerowych (kursy, szkolenia).

¹ Artificial Intelligence – (AI) próbuje się definiować jako dziedzinę wiedzy obejmującą m.in. sieci neuronowe, robotykę i tworzenie modeli zachowań inteligentnych oraz programów komputerowych symulujących te zachowania, włączając w to również uczenie maszynowe (ang. machine learning), głębokie uczenie (ang. deep learning);

² Konserwacja predykcyjna to strategia obejmująca techniki takie jak uczenie maszynowe i monitorowanie zasobów w celu identyfikowania anomalii oraz wad urządzeń i maszyn, zanim wystąpi awaria.

³ WOG – Wojskowe Oddziały Gospodarcze

Ryzyko związane z bezpieczeństwem

Chociaż AI i ZSyD zwiększają poziom bezpieczeństwa, to jednocześnie wprowadzają nowe ryzyka. Systemy oparte na sztucznej inteligencji mogą stać się celem zaawansowanych ataków cybernetycznych na wojskowe zasoby (bazy danych), w których hakerzy wykorzystują techniki AI do przełamывania zabezpieczeń. Niezwykle istotne jest więc opracowanie i wdrażanie odpowiednich środków ochronnych i właściwym oszacowaniu ryzyka. Przy dynamice i realizowaniu zadań pododdziały muszą mieć opracowane szczegółowo procedury dołączania nowego urzędnika lub usługi funkcjonalnej, Procedury Bezpiecznej Eksploatacji (PBE) oraz Szczególne Wymagania Bezpieczeństwa (SWB).

Rozwój AI niesie ze sobą również dylematy etyczne. Automatyczne podejmowanie decyzji przez systemy AI rodzi pytania o odpowiedzialność i przejrzystość tych procesów. Ważne jest, aby technologie te były rozwijane z poszanowaniem zasad etyki i z myślą o dobro żołnierza i możliwie w optymalny sposób wspomagały wykonanie zadania, często bez jego bezpośredniej wiedzy i decyzji.

Jak już mówiłem Węzły Łączności są kluczowym elementem Stanowiska Dowodzenia (SD), od których zależy efektywność operacyjna pododdziałów i ich dowódców oraz bezpieczeństwo prowadzenia operacji na różnych szczeblach Sił Zbrojnych. Wprowadzenie AI i automatyzacji do tych systemów ma ogromne znaczenie dla poprawy komunikacji, szybkości reakcji oraz koordynacji działań.

Cyberbezpieczeństwo

Sztuczna Inteligencja może analizować ogromne ilości danych ze wszystkich Aparatowńi, radiostacji, stanowisk serwerowych na Węzle Łączności w celu identyfikacji ataków cybernetycznych, takich jak DDoS⁴ czy próby włamań. Dzięki tej technologii możliwe jest szybsze i bardziej precyzyjne wykrywanie potencjalnych zagrożeń i natychmiastowe eliminowanie ich.

Należy zwrócić też uwagę na ochronę zasobów i naszych baz danych. Rozwój technologii takich jak blockchain⁵ może zostać zintegrowany z sieciami na Węzłach Łączności w celu zabezpieczenia przesyłanych danych przed manipulacją i wyciekiem. Blockchain, dzięki swojej

⁴ Rozproszona odmowa dostępu do usługi (Distributed Denial of Service, DDoS) to broń uderzająca w cyberbezpieczeństwo. Jej celem jest zakłócenie działania usług lub wyłudzenie środków finansowych.

⁵ Blockchain jest definiowany jako rejestr zdecentralizowanych danych, które są bezpiecznie współużytkowane. Technologia blockchain umożliwia grupie wybranych uczestników dzielenie się danymi. Dzięki usługom blockchain w chmurze dane transakcyjne z wielu źródeł można łatwo gromadzić, integrować i udostępniać.

strukturze rozproszonej i niezmienności zapisów, stanowi dodatkową warstwę ochrony w komunikacji i przechowywaniu danych.

Dla funkcjonowania Organów Dowodzenia Węzły Łączności są kluczowe, dlatego ich ochrona przed cyberatakami stanowi wyzwanie na poziomie nie tylko mikro, ale również globalnym (DKWOC)⁶. Konieczne jest wprowadzenie zaawansowanych systemów monitorowania i zarządzania, które zapewnią ciągłość działania i odporność na różnorodne ataki cybernetyczne (CSRiT)⁷.

Skalowalność i wydajność

Wraz z rosnącym zapotrzebowaniem na transfer danych, struktury Stanowisk Dowodzenia muszą być rozwijane z myślą o ultraszybkiej łączności, na przykład w systemach edge computing⁸. Nowoczesne technologie muszą sprostać wyzwaniom związanym z ogromnymi ilościami przesyłanych danych, co wymaga ciągłego rozwoju infrastruktury sieci teleinformatycznych i wprowadzania innowacji w zakresie przepustowości. ZSyD i optymalizacja energetyczna Węzłów Łączności są kluczowe w kontekście ograniczania śladu węglowego i wspierania zrównoważonego rozwoju. Dobrze wykonany Bilans Energetyczny⁹, stanowi klucz do utrzymania stabilności urządzeń na Węzle Łączności. Efektywne zarządzanie energią nie tylko obniża koszty, ale także stanowi ważny element przed wykryciem WŁ SD przez wrogi element, co zwiększa bezpieczeństwo operacyjne.

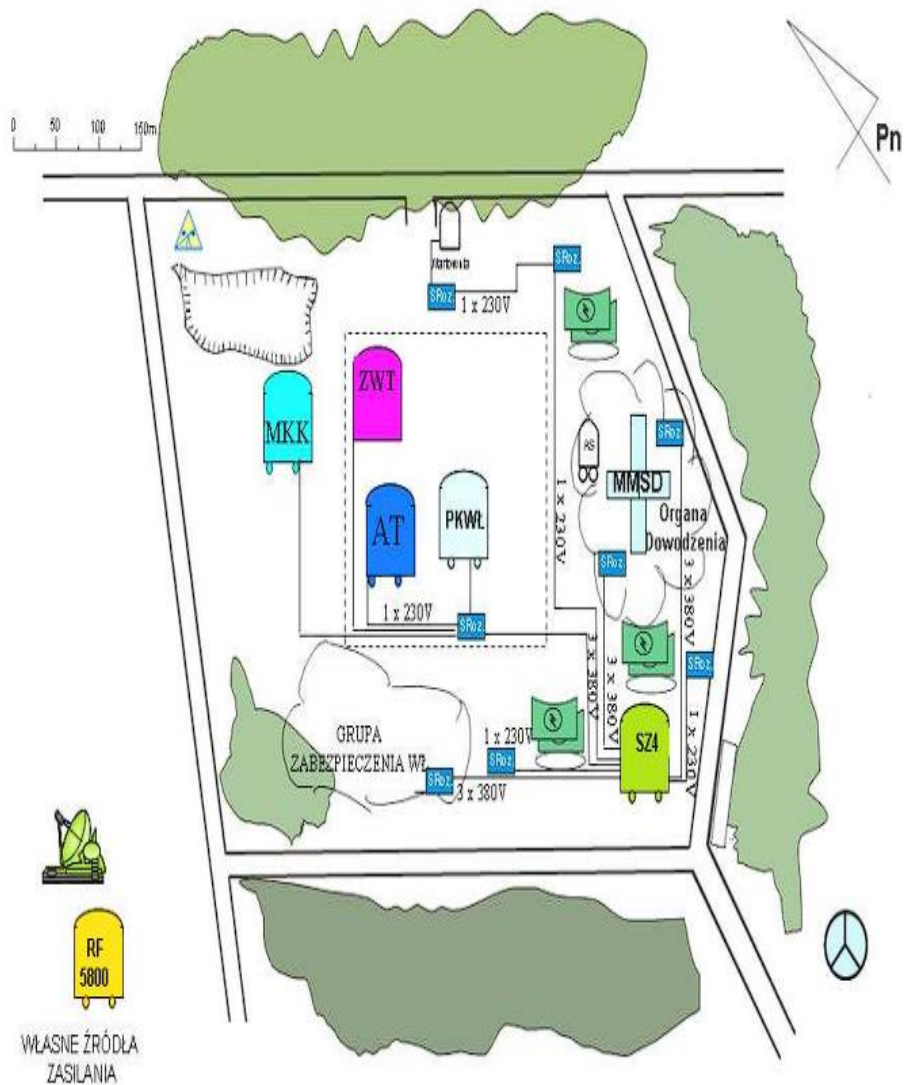
⁶ DKWOC – Dowództwo Komponentu Wojsk Cyberprzestrzeni.

⁷ CSRiT - Computer Security Incident Response Team - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego MON.

⁸ Edge computing oznacza umieszczenie mocy obliczeniowej i przechowywania danych blisko źródła, w którym te dane są generowane. Dzięki temu w chmurze odbywa się mniej procesów, co rozwiązuje problemy z przesyłaniem danych na duże odległości i opóźnieniami. Do najważniejszych zalet edge computing należą zwiększona dostępność i skrócony czas przesyłania danych.

Różni się on od tradycyjnego modelu przetwarzania i analizy danych w scentralizowanym centrum danych - w chmurze lub we własnej siedzibie firmy - ponieważ dane są przetwarzane na „brzegu” sieci.

⁹ Bilans Energetyczny - dokument ten jest powiązany ze schematem połączeń elektrycznych węzła łączności SD BZ, przedstawia się go w formie tabelarycznej; zawiera następujące informacje: – numer stacji zasilania; – typ i moc stacji zasilania; – typ zasilanego sprzętu i jego maksymalny pobór mocy; – sumaryczne zestawienie mocy odbieranej przez urządzenia biorcze.



Rysunek nr 1 Połączenia energetyczne na Węźle Łączności SD¹⁰

¹⁰ Źródło: Dokumentacja Służby Operacyjno – Technicznej Na Węźle Łączności Stanowiska Dowodzenia Brygady Zmechanizowanej/Pancernej – Marek Witkowski.

Lp	Nr st. zasilania	Typ st. zasilania	Moc (KW)	Lp	Nr st. aparat.	Typ	Moc (KW)
1	13456	SZ 30KW	30	1	14	AT	4
				2	15	ZWT	2
					16	MKK	2
					17-18	MMSD	4
					19	PKWŁ	4
					20-21	ZWD - 3	4
					22-23	ZWD - 1	4
					24-25	ZWDSz	4
Moc dostarczana			30	Moc odbierana			28
2	13245	Zespół 30KW na przyczepie	30	1		warsztat naprawy poj.	2
						warsztat łącz.	2
						bat.punkt amun.	2
						bat. punkt. sanit.	2
						bat. punkt. tank.	2
						PSŁ	4
						bat. punkt. żyw.	4
Moc dostarczana			30	Moc odbierana			16

Rysunek nr 2 Przykładowa Tabela Bilansu Energetycznego¹¹

Współpraca technologii SI z komunikacją kwantową

Sztuczna Inteligencja może wspierać rozwój budowy i struktury Węzłów Łączności na poziomie komunikacji kwantowej^{12,13}, ich zabezpieczenie kryptograficzne oraz integracje z Platformami Bojowymi, Wozami Dowodzenia, które zapewniają wysoki poziom bezpieczeństwa i szybkości komunikacji. Łączenie klasycznych i kwantowych technologii komunikacyjnych otwiera nowe możliwości w zakresie ochrony danych oraz efektywności świadomości operacyjnej. Wprowadzenie technologii kwantowej na potrzeby pracy stanowisk w Organach Dowodzenia i na WŁ wymaga projektowania nowych złożonych algorytmów i architektur baz danych np. SQL¹⁴.

¹¹ Źródło: Węzeł Łączności Stanowiska Dowodzenia Brygady Zmechanizowanej/Pancernej – Marek Witkowski.

¹² Komunikacja kwantowa to technologia wykorzystująca zasady mechaniki kwantowej, takie jak splątanie i superpozycja, do przesyłania informacji w sposób, który jest teoretycznie odporny na podsłuch i włamanie.

¹³ Komunikacja kwantowa to dziedzina fizyki kwantowej stosowanej, ściśle związana z przetwarzaniem informacji kwantowej i teleportacją kwantową. Jej najciekawszym zastosowaniem jest ochrona kanałów informacyjnych przed podsłuchem za pomocą kryptografii kwantowej.

¹⁴ (Structured Query Language) SQL to język komputerowy bardzo podobny do angielskiego, ale rozpoznawany przez programy baz danych. Każde wykonywane zapytanie w rzeczywistości używa języka SQL.

Nowe technologie na Węzle Łączności

Węzły Łączności przyszłości zdolne są do samodzielnego podejmowania decyzji - AI, takich jak optymalizacja tras przesyłu danych czy reagowanie na zmieniające się warunki obciążenia sieci telekomunikacyjnej. Sieci autonomiczne wykorzystujące sztuczną inteligencję mogą zwiększyć efektywność i niezawodność komunikacji, jednocześnie obniżając koszty. Trzeba tutaj też zwrócić uwagę na separowanie sieci i podnoszenie klauzul bezpieczeństwa, nowe technologie i zabezpieczenia na poziomie kwantowym stanowią ważny element tych sieci komputerowych.

Na przykładzie Sieci V2X¹⁵ (Vehicle-to-Everything)¹⁶, rozwój komunikacji między pojazdami a infrastrukturą (np. sygnalizacją świetlną) stawia nowe wyzwania, przed Siłami Zbrojnymi, pododdziały łączności muszą działać w czasie rzeczywistym. Sieci V2X mogą poprawić bezpieczeństwo na drogach, optymalizować ruch uliczny i wspierać rozwój inteligentnych miast poprzez integrację systemów transportowych z infrastrukturą komunikacyjną. Ale również wprowadzać dla usług funkcjonalnych wykorzystywanych przez wojsko dodatkowe parametry, stanowiące źródło informacji.

Internet Rzeczy (IoT)

Internet Rzeczy¹⁷ (IoT) odgrywa kluczową rolę w integracji i zarządzaniu zróżnicowanymi urządzeniami oraz sensorami, które współpracują w czasie rzeczywistym. IoT umożliwia gromadzenie, przetwarzanie oraz analizę dużych ilości danych pochodzących z różnych źródeł, co pozwala na podejmowanie bardziej precyzyjnych decyzji operacyjnych i strategicznych.

Integracja sensorów i baz danych z IoT na Węzłach Łączności przy Stanowiskach Dowodzenia może znacząco poprawić świadomość operacyjną, umożliwiając monitorowanie stanu wojsk, dostępność zasobów oraz lokalizację jednostek w czasie rzeczywistym. Na przykład czujniki umieszczone w sprzęcie wojskowym mogą dostarczać dane o jego stanie technicznym, co umożliwia szybką reakcję w przypadku awarii lub potrzeby przeprowadzenia konserwacji, wysłanie uzupełnienia zapasów.

Ponadto, IoT wspiera zarządzanie logistyką i zaopatrzeniem, monitorując poziomy magazynowe, zużycie paliwa i innych krytycznych zasobów. W połączeniu

¹⁵ V2X to skrót od „Vehicle to Everything”, czyli systemu komunikacyjnego umożliwiającego pojazdom interakcję z różnymi elementami otoczenia, w tym innymi pojazdami, pieszymi, sygnalizacją świetlną, znakami drogowymi, placami budowy i wieloma innymi.

¹⁶ Vehicle-to-everything zakłada, że samochód stanie się jednym z przedmiotów w internecie rzeczy. Będzie zatem komunikował się w czasie rzeczywistym z innymi pojazdami, infrastrukturą, pieszymi, internetem i urządzeniami elektronicznymi.

¹⁷ Internet rzeczy (IoT – Internet of Things) oznacza sieć obiektów fizycznych — „rzeczy” — które są wyposażone w czujniki, oprogramowanie i inne technologie w celu łączenia się i wymiany danych z innymi urządzeniami i systemami za pośrednictwem Internetu. Urządzenia te obejmują zarówno zwykłe przedmioty gospodarstwa domowego, jak i zaawansowane narzędzia przemysłowe.

z zaawansowanymi algorytmami sztucznej inteligencji, Logistycy – pododdziały zaopatrzenia mogą automatycznie optymalizować trasy dostaw, minimalizując opóźnienia oraz koszty.

Internet Rzeczy przyczynia się również do zwiększenia poziomu bezpieczeństwa na Stanowiskach Dowodzenia poprzez wdrożenie systemów monitoringu i kontroli dostępu, które mogą wykrywać i reagować na zagrożenia w czasie rzeczywistym. Podczas operacji wojskowych, IoT może wspierać także koordynację działań na polu walki, umożliwiając szybką wymianę informacji pomiędzy jednostkami a dowództwem.

Rozwój technologii IoT i ich integracja z Węzłami Łączności przy Stanowiskach Dowodzenia stanowi kluczowy element modernizacji infrastruktury wojskowej, przyczyniając się do zwiększenia efektywności, poziomu bezpieczeństwa i szybkości reakcji w różnorodnych sytuacjach operacyjnych.

Rozwój sztucznej inteligencji i automatyzacja systemów dowodzenia stanowi zarówno wyzwanie, jak i szansę. Nowe technologie przyczyniają się do optymalizacji przepustowości, efektywnego działania ZSyD oraz poprawy bezpieczeństwa sieci. Jednak ich implementacja wiąże się z dużą złożonością, ryzykiem związanym z bezpieczeństwem oraz problemami etycznymi. Kluczowe jest, aby wprowadzać te technologie w sposób odpowiedzialny i z myślą o długofalowym rozwoju Sił Zbrojnych.