Małgorzata Orłowska[1], Michał Mogilnicki[2]
Akademia Sztuki Wojennej w Warszawie

https://doi.org/10.29316/9788368103373_15

WYBRANE CYBERZAGROŻENIA W LOGISTYCE XXI W. WYKORZYSTANIE SZTUCZNEJ INTELIGENCJI W OCHRONIE ŁAŃCUCHÓW DOSTAW

SELECTED CYBER THREATS IN 21ST-CENTURY LOGISTICS. THE USE OF ARTIFICIAL INTELLIGENCE IN SUPPLY CHAIN SECURITY

Streszczenie

Celem niniejszego rozdziału było ukazanie ewolucji logistyki w XXI w. w kontekście rosnącej podatności na zagrożenia cybernetyczne oraz analiza metod przeciwdziałania tym zagrożeniom, ze szczególnym uwzględnieniem zastosowania sztucznej inteligencji w ochronie łańcuchów dostaw. W pracy przeprowadzono kompleksową analizę wpływu cyberzagrożeń na funkcjonowanie logistyki, identyfikując kluczowe obszary ryzyka, w tym ataki na systemy zarządzania łańcuchem dostaw (SCM), zakłócenia w infrastrukturze teleinformatycznej oraz wykorzystanie dezinformacji jako narzędzia destabilizującego procesy logistyczne. Szczególną uwagę poświęcono zjawisku dezinformacji, które w dobie globalizacji i dynamicznego przepływu danych stanowi istotne zagrożenie dla bezpieczeństwa operacyjnego

[1] https://orcid.org/0000-0002-8446-8764, e-mail: m.orlowska@akademia.mil.pl
[2] https://orcid.org/0009-0003-2545-6266, e-mail: michalmogilnicki00@gmail.com

podmiotów logistycznych. Ponadto wskazano mechanizmy propagowania fałszywych informacji oraz ich wpływ na decyzje podejmowane w ramach zarządzania łańcuchem dostaw. Przeanalizowano również scenariusze manipulacji danymi i ich konsekwencje dla efektywności operacyjnej przedsiębiorstw logistycznych. W kontekście przeciwdziałania cyberzagrożeniom podjęto rozważania na temat wykorzystania sztucznej inteligencji jako jednego z narzędzi wykorzystywanych w ochronie łańcuchów dostaw. Omówiono zastosowanie algorytmów uczenia maszynowego w detekcji anomalii w systemach teleinformatycznych, wykrywaniu incydentów bezpieczeństwa oraz automatyzacji reakcji na potencjalne zagrożenia. Dodatkowo zwrócono uwagę na rolę sztucznej inteligencji w predykcji ryzyka oraz optymalizacji procesów logistycznych w kontekście zapewnienia ich odporności na cyberataki. Na podstawie przeprowadzonych analiz opracowano rekomendacje dotyczące wzmacniania cyberbezpieczeństwa w logistyce, ze szczególnym uwzględnieniem strategii integracji sztucznej inteligencji z tradycyjnymi metodami zarządzania bezpieczeństwem w łańcuchach dostaw. Wskazano kierunki przyszłych badań w obszarze ochrony systemów logistycznych przed zagrożeniami cybernetycznymi i dezinformacyjnymi. Całość opracowania zwieńczono podsumowaniem, w którym podkreślono wnioski dotyczące wyzwań i możliwości, jakie niesie XXI w. dla bezpieczeństwa logistyki w erze cyfrowej transformacji.

Słowa kluczowe: logistyka, zarządzanie, cyberbezpieczeństwo, dezinformacja, sztuczna inteligencja

Abstract

The aim of this chapter was to complete the evolution of logistics in the 21st century with respect to the application of cybersecurity vulnerabilities and analyse methods for preventing these threats, with a detailed application of artificial intelligence in supply chain protection. In a comprehensive approach to addressing the impact of cybersecurity threats on logistics operations, key threats were identified, including disruptions to the secure supply chain management (SCM) system, IT infrastructure disruptions, and the use of disinformation to destabilise logistics processes. Particular attention was paid to the phenomenon of disinformation, which in the era of globalisation and data exploitation constitutes a key safeguard for data security. Additionally, mechanisms for information propagation and its Impact on supply chain management decisions were identified. Data manipulation scenarios and their consequences for the operational efficiency of logistics companies were also analysed. In connection with countering cybersecurity threats, an assessment was conducted of the use of artificial intelligence to protect supply chains. Machine learning algorithms are used to detect anomalies in known ICT systems, detect security incidents, and automate risk responses. Additionally, attention is drawn to the risks posed by

artificial intelligence in threat prediction and logistics system optimisation, given their vulnerability to cyberattacks. Based on the analysis, recommendations were developed to strengthen cybersecurity in logistics by applying artificial intelligence strategies alongside traditional management methods for basic supplies. Information is provided on the implications of the research for protecting IT systems from cyber and disinformation threats. The concluding summary provides information on the significance of the conclusions regarding the opportunities and possibilities the 21st century offers for logistics security in the era of artificial transformation.

Keywords: logistics, military logistics, management, cybersecurity, disinformation, artificial intelligence

Wstęp

Rozważania na temat cyberzagrożeń w logistyce jako czynników negatywnie oddziałujących na cyberbezpieczeństwo branży wydają się uzasadnione. Bardzo mało jest publikacji poświęconych rozważaniom w tym zakresie. Sytuację problemową stanowiła próba ukazania, w jaki sposób cyberzagrożenia oraz dezinformacja wpływają na współczesną logistykę, a także jak sztuczna inteligencja może wspierać zapewnianie cyberbezpieczeństwa. Celem głównym opracowania było wyjaśnienie, co współcześnie stanowi wyzwanie dla cyberbezpieczeństwa logistyki (łańcuchów dostaw) oraz w jaki sposób można im przeciwdziałać. Z kolei celami szczegółowymi były ukazanie ewolucji logistyki, pod kątem wykorzystania technologii cyfrowych. Dokonanie analizy wybranych ryzyk, jakie są powszechnie obserwowane w logistyce, w wymiarze cyberbezpieczeństwa. Jak również, ukazanie dezinformacji jako istotnego cyberzagrożenia dla bezpieczeństwa logistyki. Hipotezę badawczą stanowił pogląd autorów, że możliwa jest synergia sztucznej inteligencji z personelem logistycznym, jeśli zrealizowane zostaną adekwatne działania przygotowawczo-edukacyjne w aspekcie zapewniania cyberbezpieczeństwa.

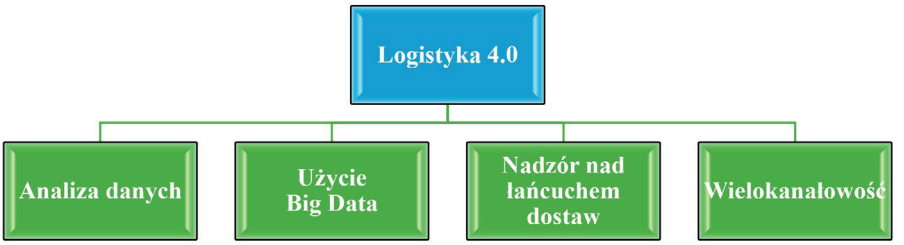
Cyfryzacja logistyki

W historii cywilizacji wyróżniono trzy ważne rewolucje przemysłowe, które doprowadziły do poważnych zmian gospodarczych i zwiększonej wydajności produkcji. Ich wynikiem był dynamiczny rozwój gospodarczy i poprawa jakości życia społeczeństw. Pierwsza rewolucja przemysłowa

była powiązana z rozpoczęciem wykorzystywania silników parowych, które pozwoliły na opracowanie narzędzi i maszyn, znacznie wydajniejszych od dotychczasowych. Druga rewolucja przemysłowa rozpoczęła się wraz z wynalezieniem maszyn zasilanych energią elektryczną, które przyczyniły się do tworzenia zarządzania produkcją i wprowadzenia masowej produkcji. Tymczasem trzecia rewolucja przemysłowa, opisana jako rewolucja naukowa i technologiczna, była oparta na automatyzacji procesów z wykorzystaniem informacji i technologii IT oraz zastosowaniu technologii IT w celu poprawy wydajności i jakości produkcji. Współcześnie coraz częściej mówi się o czwartej rewolucji przemysłowej, nazywanej Przemysłem 4.0 lub cyfrową transformacją (Płaczek, 2018).

Rozwój technologii cyfrowych zrewolucjonizował współczesną logistykę. Zauważalne są zmiany w sposobie zarządzania łańcuchem dostaw, procesami magazynowymi i transportowymi. Logistyka, podobnie jak przemysł, przeszła kilka etapów rozwoju, dostosowując się do zmian technologicznych i gospodarczych (Arvato, b.d.). Każda kolejna wersja logistyki odzwierciedlała coraz większy stopień automatyzacji i integracji w zarządzaniu łańcuchem dostaw. Logistyka 1.0 dotyczyła podstawowych operacji związanych z transportem, magazynowaniem i dystrybucją towarów. Realizowanych za pomocą papierowej dokumentacji i prostych metod zarządzania. Transport odbywał się głównie przy użyciu kolei i żeglugi, a jego głównym celem było przemieszczanie towarów z jednego punktu do drugiego (Tjahjono i in., 2017). Wraz z drugą rewolucją przemysłową i upowszechnieniem produkcji masowej logistyka zaczęła rozwijać się pod kątem optymalizacji procesów. W Logistyce 2.0 wprowadzono pierwsze systemy mechanizacji, takie jak przenośniki taśmowe i wózki widłowe, a także standaryzację transportu (np. konteneryzację). Dokumentacja wciąż była w większości papierowa, jednak zaczęły pojawiać się pierwsze systemy wspierające zarządzanie zapasami. Logistyka 3.0 stanowiła erę globalizacji i szerokiego wykorzystania technologii informatycznych. Wprowadzenie systemów zarządzania łańcuchem dostaw (SCM), systemów ERP oraz automatycznych systemów identyfikacji (np. kody kreskowe) pozwoliło na lepszą kontrolę i optymalizację procesów logistycznych (Orłowska, 2023). Powstały pierwsze systemy zarządzania magazynem (WMS) oraz systemy śledzenia przesyłek. Logistyka stała się kluczowym elementem strategii biznesowych, umożliwiając

firmom dostosowanie się do dynamicznych zmian rynkowych. Logistyka 4.0 odnosi się do wdrażania inteligentnych systemów oraz pełnej automatyzacji (Rysunek 1) (Sokołowska, 2024). Przy użyciu zaawansowanych technologii, takich jak sztucznej inteligencji (AI), Internetu Rzeczy (IoT), Big Daty, blockchainów, robotyzacji i autonomicznych pojazdów. Systemy zarządzania magazynem (WMS) i transportem (TMS) pracują w chmurze i są zintegrowane z innymi systemami w czasie rzeczywistym. Misją logistyki 4.0 jest dążenie do elastyczności, predykcyjnego zarządzania zapasami oraz minimalizacji kosztów operacyjnych (Barcik, Odlanicka-Poczobutt, 2020). Ponadto w logistyce 4.0 zyskały na znaczeniu: zrównoważony rozwój i ekologiczne rozwiązania, takie jak pojazdy elektryczne czy inteligentne zarządzanie flotą pojazdów przedsiębiorstwa.



Rysunek 1. Elementy Logistyki 4.0

Źródło: opracowanie własne na podstawie RedSteel, b.d.

Choć pojęcie Logistyki 5.0 nie jest jeszcze szeroko ugruntowane, pojawia się ono i wskazuje na kolejną fazę rozwoju. Zadaniem logistyki 5.0 ma być skupienie się na harmonijnym współdziałaniu ludzi i technologii, z naciskiem na zrównoważony rozwój oraz społeczną odpowiedzialność biznesu (Bielecki, 2022).

W dobie digitalizacji firmy logistyczne wdrożyły zaawansowane rozwiązania z obszaru technologii cyfrowych. Umożliwiło to tworzenie podstaw automatyzacji, optymalizacji i zwiększonej wydajności operacyjnej (Internet IoT), sztucznej inteligencji (AI), Big Data, Blockchain, Process Robotation – Logistics 4.0. Oczywiście, w oparciu głównie o narzędzia z obszaru cyber. Cyfryzacja logistyki umożliwia ciągłe monitorowanie i analizę danych w czasie rzeczywistym, co prowadzi do bardziej szczegółowego planowania transportu, zarządzania zapasami i zmniejszania kosztów operacyjnych.

Wykorzystanie cyfrowych, inteligentnych systemów analitycznych umożliwiło prognozowanie popytu, optymalizację tras oraz eliminację zbędnych przejazdów, co przekłada się na bardziej efektywne i ekologiczne zarządzanie flotą transportową (Ivanov i in., 2019).

Współczesne magazyny coraz częściej wykorzystują systemy automatyki, w tym autonomiczne roboty, drony oraz zaawansowane systemy identyfikacji towarów oparte na RFID i kodach kreskowych (Orłowska, Orłowski, 2024). Integracja tych technologii z systemami zarządzania magazynem (WMS) pozwala na zwiększenie precyzji operacji logistycznych, minimalizację błędów oraz redukcję czasu potrzebnego na kompletację zamówień. Cyfrowa transformacja logistyki ma również istotne znaczenie w kontekście zrównoważonego rozwoju. Inteligentne systemy monitorujące mogą optymalizować zużycie energii i paliwa, zmniejszając ślad węglowy transportu. Ponadto integracja systemów informatycznych umożliwia lepszą współpracę pomiędzy podmiotami w łańcuchu dostaw, zwiększając transparentność procesów i poprawiając efektywność logistyczną.

Widoczne zdaje się być, jak duże pole manewru mogą mieć cyberzagrożenia w obszarze logistyki. Z uwagi na to, jak istotne z punktu widzenia funkcjonowania państwa są branża i element gospodarki, należy mieć świadomość, że kluczowe jest zapewnienie ich bezpieczeństwa. Zarówno w wymiarze kinetycznym, jak i cybernetycznym. Każda ze wspomnianych wersji logistyki przynosiła dlań nowe zagrożenia dla bezpieczeństwa, a tym samym nowe zagrożenia dla podmiotu, wewnątrz którego „nowa logistyka" funkcjonowała. Obecnie zakorzeniająca się Logistyka 5.0 i jej istota skupiona wokół współdziałania systemów cybernetycznych oraz sztucznej inteligencji z ludźmi pozwalają przewidywać, że oprócz wielu szans będą pojawiać się zagrożenia cyberbezpieczeństwa podmiotów logistycznych. Zasadnym wydaje się podjąć rozważania na tym etapie dotyczące typów form ryzyka, z jakimi będzie już niedługo musiała się mierzyć logistyka w aspekcie cyberbezpieczeństwa.

Cyberzagrożenia procesów logistycznych – analiza współczesnych ryzyk

Zaawansowany już obecnie oraz ciągły i dynamiczny proces cyfryzacji logistyki niesie ze sobą liczne korzyści, jednak równolegle z rozwojem

technologii rośnie także liczba zagrożeń związanych z cyberbezpieczeństwem. Systemy logistyczne, zintegrowane z chmurą obliczeniową, Internetem Rzeczy (IoT) oraz sztuczną inteligencją (AI), stają się atrakcyjnym celem dla m.in. cyberprzestępców. Ataki mogą prowadzić do poważnych zakłóceń operacyjnych, strat finansowych oraz naruszenia poufności danych. Do najbardziej znanych cyberzagrożeń w logistyce należy zaliczyć ataki ransomware, czyli zastosowanie złośliwego oprogramowania szyfrującego dane w systemach zarządzania magazynem (WMS) lub transportem (TMS), wymagające okupu za ich odszyfrowanie. Przykładem takiego ataku było zdarzenie z roku 2017 w firmie Maersk, w trakcie którego unieruchomiono systemy globalnej logistyki morskiej. Co więcej, jako zagrożenia dla bezpieczeństwa z obszaru cyber należy rozumieć np. fałszywe e-maile i strony internetowe w celu wyłudzenia danych logowania do systemów logistycznych. Takie działania nazywane są phishingiem i socjotechnikami, które mogą doprowadzić do przejęcia kontroli nad łańcuchem dostaw lub manipulacji danymi dotyczącymi transportu i zapasów.

Kolejnym cyberzagrożeniem są ataki na IoT i inteligentne urządzenia ze względu na coraz większą liczbę procesów logistycznych zarządzanych przez zautomatyzowane systemy i urządzenia podłączone do Internetu. Niewłaściwie lub słabo zabezpieczone sieci mogą stanowić furtkę dla hakerów, którzy mogą np. przejąć kontrolę nad systemami monitorowania przesyłek lub autonomicznych pojazdów (Netbe.pl, b.d.).

Innym zagrożeniem jest złośliwe oprogramowanie (malware) wprowadzane do systemów ERP i SCM. Są to ataki wycelowane w zintegrowane systemy zarządzania łańcuchem dostaw (SCM) lub w systemy planowania zasobów przedsiębiorstwa (ERP). Ich działania mogą skutkować przejęciem kontroli nad procesami logistycznymi i wprowadzeniem nieautoryzowanych zmian w danych operacyjnych przedsiębiorstwa (Bartczak, 2022). Firmy logistyczne często współpracują z wieloma podmiotami zewnętrznymi oraz państwowymi, co zwiększa ryzyko ataków poprzez słabo zabezpieczone systemy partnerów. Przykładem zakłócenia łańcucha dostaw przez cyberatak na dostawcę był atak na firmę SolarWinds, który wpłynął na bezpieczeństwo wielu przedsiębiorstw na całym świecie (Vault-Tech, b.d.). Cyberzagrożenia mogą prowadzić do szeregu negatywnych skutków, takich jak np.: zakłócenia operacyjne – przestoje w magazynach, opóźnienia w dostawach, blokada

systemów śledzenia przesyłek, straty finansowe, koszty związane z usuwaniem skutków ataku, okup w przypadku ransomware, kary umowne za niewywiązanie się z kontraktów, naruszenie poufności danych, wyciek wrażliwych informacji o dostawcach, klientach i trasach transportowych, który może prowadzić do utraty zaufania klientów, manipulacja danymi, zmiana danych dotyczących dostaw, manipulacja trasami transportu czy sabotaż systemów logistycznych może mieć katastrofalne skutki.

Wskazane w tej części opracowania ryzyka zdają się podkreślać słuszność podjętych rozważań. Ryzyko jest stanem, w którym dany czynnik oddziaływujący lub podjęte działanie spowoduje negatywne dla podmiotu konsekwencje, stopień prawdopodobieństwa których jest wysoki. Procesom logistycznym oraz łańcuchom dostaw towarzyszy wiele rodzajów ryzyka, z których większość powoduje powstanie kolejnych, jeśli nie podejmie się adekwatnych działań, celem ich neutralizacji. Obecnie zagrożenia informacyjne zdają się przeżywać swój renesans. Warto podkreślić, że zagrożenia dla bezpieczeństwa informacyjnego mogą też mieć podłoże naturalne (Kitler, 2022). Brak kontroli oraz demokratyczny dostęp do tworzenia i upubliczniania treści użyźnił i zaorał pole pod rozkwit dezinformacji. Stanowi ona zagrożenie w każdym wymiarze bezpieczeństwa. W logistyce również, zarówno w ujęciu kinetycznym, jak i w ujęciu cyberbezpieczeństwa.

Dezinformacja jako wybrane zagrożenie dla logistyki i zarządzania łańcuchem dostaw

Aby przedstawić dezinformację, która obecnie coraz częściej stanowi właśnie cyberzagrożenie w sposób jak najbardziej jasny w opinii autorów, posłużyli się przykładem zarządzania łańcuchem dostaw. Jest to jeden z głównych, często realizowanych i bardzo ważnych, zwłaszcza w aspekcie działań zbrojnych i procesów logistycznych. Przykładów na słuszność tej tezy nie brakuje. W czasie II wojny światowej cele, zasięg oraz czas trwania operacji oraz ofensyw były uzależnione w dużej mierze od sprawności i bezpieczeństwa łańcucha dostaw dla nacierających związków taktycznych i operacyjnych. Niemal całkowite zatrzymanie pochodu Aliantów zachodnich jesienią 1944 r. było spowodowane kłopotami w łańcuchu dostaw. Nie dość, że początek łańcucha dostaw znajdował się nad północnym, francuskim wybrzeżem, to pojawiło się wiele niebezpieczeństw na każdym z jego

ogniw. Równocześnie w środkowej Polsce stanęła ofensywa w ramach operacji *Bagration*. Ten przymusowy postój również w dużej mierze spowodowany był wydłużeniem o kilkaset kilometrów łańcucha dostaw, a także koniecznością odnalezienia odbiorców dostaw i ustalenia, co, komu, ile i gdzie trzeba dostarczyć.

W tym miejscu zasadne wydaje się podkreślić, że jak zauważają Z. Piątkowski oraz W. Żebrowski, należy rozumieć, że logistyka w sferze zaopatrzenia dotyczy przepływów surowców, materiałów, detali, części, półproduktów od dostawców do magazynów zaopatrzeniowych lub magazynów przyjęcia w przedsiębiorstwie lub bezpośrednio do procesu produkcyjnego (Piątkowski, Żebrowski, 2008). Definicji samego łańcucha dostaw w literaturze przedmiotu zawiera wiele. Jest on bardzo często definiowany w kreślonych kontekstach prowadzonych badań. Inaczej definiuje się w aspekcie militarnym, przedsiębiorstw prywatnych, towarów niebezpiecznych czy produktów cyfrowych. W odniesieniu do pojęcia zarządzania również nie brakuje definicji tego procesu w licznych jego kontekstach. Najlepszą formą zdefiniowania procesu zarządzania łańcuchem dostaw, w odniesieniu do cyberzagrożeń i cyberbezpieczeństwa, wydaje się być następujące stwierdzenie. Zarządzanie łańcuchem dostaw to proces planowania, realizacji zaplanowanych działań oraz kontroli tych działań, mających na celu efektywny i wydajny przepływ towarów, surowców, zapasów w drodze oraz niezbędnej informacji i wiedzy z punktu wyjścia do punktu dostawy w celu zaspokojenia potrzeb i wymagań odbiorcy (Janczewski, 2018).

Łańcuch dostaw jest elementem logistyki. Prowadząc rozszerzone rozważania na temat logistyki w aspekcie poznawczym, jak i praktycznym, pominięcie zagadnienia łańcucha dostaw stanowiłoby kardynalne niedopatrzenie. Posiadanie ważnych, aktualnych, wiarygodnych oraz na bieżąco weryfikowanych informacji zdaje się być jednym z głównych narzędzi do ochrony bezpieczeństwa podmiotu. Zarówno w aspekcie zagrożeń tradycyjnych, jak i cyberzagrożeń. W tym momencie rozważań należy uwidocznić, w jaki sposób dezinformacja stanowi obecnie broń w podjętym temacie.

Dezinformacja to zjawisko, element komunikacji werbalnej i niewerbalnej, a także broń. Nie sposób określić moment w dziejach ludzkości, w którym pierwszy człowiek przekazał fałszywą informację w celu umyślnego wprowadzenia kogoś w błąd, a w konsekwencji samemu osiągając

zamierzone korzyści. Można pokusić się o stwierdzenie, iż dezinformacja stanowi stały element stosunków społecznych (w tym również biznesowych), bowiem jest mocno zakorzeniona w przeszłości, obecnie wykorzystywana na skalę jak nigdy wcześniej oraz prognozowanie jej udziału w szeroko pojętej przestrzeni informacyjnej jest raczej słuszne (Dela, 2022). Właśnie demokratyczny dostęp do przestrzeni informacyjnej innego przedsiębiorstwa logistycznego, zwłaszcza w obszarze cyber i poprzez Internet, daje możliwość upubliczniania w niej dowolnego rodzaju treści skierowanych do innych realizatorów łańcucha dostaw oraz innych procesów logistycznych, co stanowi narzędzie *par excellence* dla eskalacji skuteczności dezinformacji (Mogilnicki, 2024).

Dezinformację można rozumieć zarówno jako stan, jak i proces. Można ją stosować z wykorzystaniem różnorakich metod, zarówno oddzielnie, jak i synchronicznie (Brühl, 2019). Wszystko zależy od tego, zarówno w stanie, jak i w procesie, która forma jest bardziej korzystna. Proces dezinformowania, mający doprowadzić do stanu dezinformowania, wymaga stosowania dezinformacji jako działań (Osiecki, 2023): zaplanowanych, sprowadzających się do spreparowania i dostarczania odbiorcom informacji lub innego rodzaju danych częściowo lub w pełni fałszywych, realizowanych w cyberprzestrzeni, rozumianej jako obszar przetwarzania, publikowania i wymiany informacji z wykorzystaniem odpowiednich urządzeń i oprogramowania, posiadającej ukryty, znany tylko twórcy dezinformacji, cel.

W kontekście cyberbezpieczeństwa w logistyce i bezpieczeństwa łańcuchów dostaw te dwie opcje rozumienia dezinformacji, jawią się następująco. Dezinformacja jako stan odnosiła się do sparaliżowania zarządzania łańcuchem dostaw oraz innych procesów logistycznych w przeszłości. Innymi słowy, ten paraliż już się dokonał i trwa. Natomiast dezinformacja jako proces to wszystkie działania realizowane w czasie teraźniejszym jak i te zaplanowane na przyszłość. Są one ukierunkowane na doprowadzenie do przerwania łańcucha dostaw oraz uniemożliwienie zarządzania nim. Żadne z wielu pojedynczych działań nie spowoduje tego, lecz ujęte w zorganizowanych procesach dezinformowania już tak. Zarówno w aspekcie tradycyjnych zagrożeń bezpieczeństwa, jak i w aspekcie cyberzagrożeń.

Dezinformacja obecnie stanowi poważne zagrożenie dla skutecznego zarządzania łańcuchem dostaw, a także dla logistyki. Współczesność, jak

dowodzi praktyka, nie ograniczyła się jeszcze do działań jedynie w domenie cybernetycznej, ale ta domena odgrywa i będzie odgrywać coraz większą i ważniejszą rolę. W systematycznym budowaniu przewagi niekinetycznych cyfrowych form, metod i technik wykorzystania dezinformacji jako broni, pomaga wykorzystanie narzędzi opartych na sztucznej inteligencji. Aby przedstawić to zagadnienie, posłużono się opisami hipotetycznych, lecz bardzo prawdopodobnych sytuacji, jakie mogą mieć miejsce w rzeczywistości.

Po pierwsze, wykorzystanie dezinformacji może doprowadzić do przerwania łańcucha dostaw oraz spadku jego wydajności. W procesie działań dezinformacyjnych określone grupy dywersyjne mogą zniszczyć lub przestawiać znaki drogowe. To natychmiast i znacznie zakłóci zarządzanie łańcuchem dostaw i same dostawy, generując jednocześnie dodatkowe koszty, bo kierowcy będą spalać paliwo, aby wrócić na właściwą trasę przejazdu. W transporcie kolejowym lub lotniczym bardzo podobnie. Dodatkowo, jeśli maszynista otrzyma informację fałszywą (dezinformację), może ustawić lokomotywę na złym torze i zabrać zaopatrzenie przeznaczone dla odbiorcy „A", które zawiezie odbiorcy „B". Takie sytuacje wręcz paraliżują proces zarządzania łańcuchem dostaw oraz sam łańcuch. Opóźnienia oraz dodatkowe koszty mogą być gargantuiczne. Dodatkowo mogą mieć znaczny wpływ na wartości i cele najwyższe, takie jak bezpieczeństwo państwa. Zakłócenie lub paraliż łańcucha dostaw broni, amunicji, żołnierzy lub medykamentów do rejonu prowadzenia działań zbrojnych może mieć katastrofalne i nieodwracalne skutki.

Po drugie, wykorzystanie dezinformacji, w oparciu o sztuczną inteligencję może doprowadzić do likwidacji łańcucha dostaw, nawet przez podmiot od tegoż łańcucha uzależniony. Program o nazwie *Deepfake* zdaje się być jednym z obecnie najbardziej powszechnych oraz niebezpiecznych narzędzi. Ten program, który wykorzystuje sztuczną inteligencję, jest w stanie wytwarzać produkty audiowizualne, odtwarzające bardzo wiarygodnie wygląd oraz głos konkretnych osób. Wytworzenie np. filmu, w którym przedstawiciel podmiotu „A" zwraca się do przedstawiciela podmiotu „B" i wypowiada mu kontrakt na dostawy ekstremalnie ważnych surowców, urządzeń lub towarów. Utracenie dostaw w krótkim czasie doprowadzi do upadku podmiotu „A", który na dodatek będzie jeszcze musiał zapłacić karę

podmiotowi „B". Jeśli ktoś nie zorientowałby się, że to mistyfikacja i dywersja, doszłoby do wspomnianych skutków, a zorientowanie się wcale nie jest proste.

Po trzecie, dezinformacją można doprowadzić do przerwania łańcucha dostaw, poprzez samych jego realizatorów. Wszak w obecnym świecie, głównymi celami dezinformacji stały się społeczeństwa, które zajęły miejsce dowódców wojskowych, prominentnych polityków oraz wpływowych grup obywateli. Poprzez wykorzystanie sztucznej inteligencji do szerzenia informacji, można zasypać wręcz pracowników przedsiębiorstw logistycznych spreparowanymi treściami, które wywołają co najmniej strajk. Wykorzystanie trudnego okresu finansowego, żeby wtedy rozpowszechnić treści (np. wytworzone przez *Deepfake*), które informowałyby o lekkomyślnym rozporządzaniu aktywami przedsiębiorstwa, zamiast podnieść płace pracownikom, to recepta właśnie na to. Zasadnym wydaje się stwierdzić, że ochrona realizatorów łańcucha dostaw przed dezinformacją, to de facto ochrona samego łańcucha dostaw. Bezpieczeństwo informacyjne ludzi odpowiedzialnych za łańcuch, determinuje zarówno pośrednio, jak i bezpośrednio bezpieczeństwo łańcucha dostaw oraz innych procesów logistycznych.

Dezinformacja stanowi obecnie coraz poważniejsze zagrożenie dla bezpieczeństwa we wszystkich jego wymiarach, w tym także w branży logistycznej. To zagrożenie, choć powstało i wyewoluowało w prawdziwym świecie, obecnie jest spotykane głównie w przestrzeni cyfrowej. Sztuczna inteligencja to ogromne osiągnięcie techniki, ale też katalizator częstotliwości, kreatywności i liczby, z jaką dezinformacja jest szerzona. Dlatego warto się przyjrzeć, w jaki sposób może być wykorzystana w cyberbezpieczeństwie logistyki.

Sztuczna inteligencja w cyberbezpieczeństwie logistyki

Wskazano już, jak dużo zależy od bezpieczeństwa łańcucha dostaw, który jest elementem logistyki. O ile w tradycyjnym rozumieniu bezpieczeństwa logistyki i zagrożeń w logistyce trudno jest cokolwiek nowego wskazać, o tyle w aspekcie cyberbezpieczeństwa zdecydowanie tak. Tradycyjne, czyli kinetyczne, i inne już znane zagrożenia dla logistyki zostały już gruntownie zbadane. Zasadnym wydaje się wskazać, że mogą pojawić się nowe formy, lecz już nazwane i usystematyzowane typy zagrożeń logistycznych

stanowią prawie katalog zamknięty. Zupełnie inaczej ma się to w aspekcie zapewnienia cyberbezpieczeństwa w branży logistycznej, a także wykorzystania do tego sztucznej inteligencji. Bezpieczeństwo cyberprzestrzeni, czyli innymi słowy cyberbezpieczeństwo w ujęciu holistycznym, to brak ryzyka utraty danych lub informacji przechowywanych w cyberprzestrzeni (Pacek, Hoffmann, 2013). Można zatem stwierdzić, jak wykazuje praktyka, że jest to połączenie różnych narzędzi, technik oraz środków reagowania i ochrony danych nie tylko przed ich kradzieżą i utratą, ale też przed manipulowaniem ich treścią.

Zdaniem autorów, cyberbezpieczeństwo to stan braku zagrożeń utratą, kradzieżą oraz manipulacją danych przechowywanych trwale przez podmiot, a także brak zagrożenia manipulacją i kreowaniem własnej przestrzeni informacyjnej przez inny podmiot, za sprawą wykorzystania do tego narzędzi, metod oraz technik cyfrowych w przestrzeni cybernetycznej. Stan ten osiągany jest w wyniku realizacji procesów okresowych oraz ciągłych, mających na celu zbudowanie zdolności ochrony przed cyberzagrożeniami, a także stałe monitorowanie przestrzeni informacyjnej w poszukiwaniu destrukcyjnych i innych niepożądanych działań w tejże przestrzeni.

A zatem cyberbezpieczeństwo w logistyce należy rozumieć jako stan, w którym procesy logistyczne, cyfrowe dane niezbędne do niezakłóconej ich realizacji, a także ich planowania oraz ich kontrolowania pozostają wolne od zagrożeń, zarówno tych typowo cybernetycznych, jak i innych, które mogą być wywołane działaniami w cyberprzestrzeni (Microsoft, b.d.).

Tak jak wspomniano wcześniej, sztuczna inteligencja (AI) może generować i być narzędziem do wytwarzania zagrożeń dla cyberbezpieczeństwa w logistyce, a też może wspomagać utrzymywanie i polepszanie tego wymiaru bezpieczeństwa jako stanu. Obecnie coraz częściej powstają nowe programy, algorytmy oraz sposoby wykorzystania sztucznej inteligencji w procesie dbania o cyberbezpieczeństwo. Niektóre z nich ukierunkowane są na wykrywanie i zwalczanie pojawiających się zagrożeń, nawet stosując metaforyczny ogień kontrbateryjny, czyli niszcząc zdolności innego dezinformacyjnego programu czy algorytmu. Jednakże wykorzystanie sztucznej inteligencji, zwłaszcza w logistyce, nie ogranicza się jedynie do tego. Może być ona równie pożytecznie wykorzystywana w bieżącej obsłudze centrów logistycznych oraz np. w zarządzaniu łańcuchami dostaw. W kontekście

centrów logistycznych, znajduje ona zastosowanie np. w optymalizacji przestrzeni magazynowej, zarządzaniu zapasami zgromadzonymi w magazynach centrów logistycznych, przydzielaniu zadań pracownikom centrów logistycznych oraz poprawie efektywności tras na terenie samego magazynu, co przekłada się na efektywniejsze i bezpieczniejsze funkcjonowanie całego łańcucha dostaw. Natomiast w kontekście zarządzania łańcuchem dostaw, korzyści zastosowania sztucznej inteligencji, zdają jawić się następująco: ułatwia rutynową komunikację, zarówno w komunikacji wewnętrznej oraz z podmiotami zewnętrznymi, może udzielać automatycznie odpowiedzi na zapytania, które wprowadzane do systemu zintegrowanego z nią pojawiają się dość często, a odpowiedzi na nie zazwyczaj są podobne, potwierdza zamówienia i aktualizuje statusy dostaw, co skutecznie usprawnia komunikację i ogranicza opóźnienia w procesach, przyspiesza planowanie przepływów logistycznych w różnych horyzontach czasowych i przekrojach, skuteczniej koordynuje procesy logistyczne oraz inne operacje oraz prowadzi stały monitoring procesów logistycznych (Mroczko, 2023).

Biorąc pod uwagę zawarte powyżej wybrane możliwości zastosowania sztucznej inteligencji w logistyce oraz zarządzaniu łańcuchem dostaw, zasadnym wydaje się wskazać, jakie korzyści dla przedsiębiorstwa logistycznego oraz procesu zarządzania łańcuchem dostaw płyną za sprawą wykorzystania tego cybernetycznego narzędzia. Oczywiście, zachowując kontekst niniejszego opracowania, autorzy wymieniają jedynie te, które mają wpływ na cyberbezpieczeństwo, ale oddziałują na kluczowe aspekty w logistyce determinujące jej skuteczność. A są to: wyeliminowanie błędu ludzkiego, przy planowaniu zagospodarowania przestrzeni magazynowej, wyeliminowanie błędu ludzkiego przy obliczeniach stanu zapasów zgromadzonych w magazynie, wyeliminowanie ryzyka korupcji pracowników odpowiedzialnych lub biorących udział w realizacji procesów logistycznych, która może skłonić nich do szeroko rozumianego sabotażu, przydzielanie zadań pracownikom, w oparciu o znajomość wszystkich ich kompetencji, odnotowanych w systemie cyfrowym, a także precyzyjny ich dobór po porównaniu ze sobą co najmniej dwóch pracowników o podobnych ale nieidentycznych kompetencjach, prowadzone przez sztuczną inteligencję pojazdy na terenie magazynu wykonują przewóz towarów efektywniej oraz z większą częstotliwością w badanym czasie, niż gdy prowadzi je człowiek, odciąża i nie marnuje

czasu pracowników odpowiedzialnych za komunikację i aktualizację statusu dostaw, samodzielnie obsługuje systemy i nie dopuszcza się metod ani czynności (wchodzenia na niebezpieczne strony internetowe służbowym komputerem), które generują ryzyko oddziaływania cyberzagrożeń, wykrywa odpowiedzi udzielne na zapytania kierownictwa do realizatorów łańcucha dostaw, które są niezgodne z ustalonymi standardami, przez co natychmiast może zaalarmować o nieprawidłowości odpowiednią komórkę organizacji, może szybko i trafnie przewidywać potencjalne zagrożenia dla planu realizacji konkretnego łańcucha dostaw, w oparciu o całą wiedzę globalnej sieci internetowej, do której jest podłączona, analizuje i koreluje dane dotyczące zdarzeń w cyberprzestrzeni i cyberzagrożeń z wielu źródeł, przekształcając je w jasne i praktyczne szczegółowe informacje używane przez analityków ds. zabezpieczeń do dalszego badania i ograniczania ryzyka cyberataków.

Przedstawione możliwości wykorzystania sztucznej inteligencji w zapewnianiu cyberbezpieczeństwa logistyki, procesu zarządzania łańcuchem dostaw oraz bieżącego prowadzenia działalności centrum logistycznego, rzecz jasna, nie zawierają wszystkich możliwych jej zastosowań. Jednakże zasadnym wydaje się wskazać, że zbiór możliwości tutaj zaprezentowany, może śmiało stanowić wstęp i punkt wyjścia do dalszych badań nad rolą sztucznej inteligencji w cyberbezpieczeństwie logistyki oraz zarządzania łańcuchem dostaw.

Przyszłość cyberbezpieczeństwa w logistyce

Stałą w obszarze obronności wielu państw świata jest to, że przygotowują się do odparcia ataku, prowadzenia wojny oraz zgromadzenia zapasów i produkcji bieżącej w takich ilościach, jakie były niezbędne ostatnio, tj. w czasie ostatniej wojny tych państw. Cyberbezpieczeństwo, choć stosunkowo niedawno usystematyzowane, jest znacznie starsze od sztucznej inteligencji. Mogłoby się tak wydawać, jeśli rozumiemy je jako brak zagrożeń i ryzyka utraty ważnych informacji danej organizacji drogą cyfrową. Wykorzystywanie najnowocześniejszych w danym momencie technologii w działalności przedsiębiorstw, np. logistycznych, czy w obronności państwa nie jest niczym nowym. Oczywiście, w kontekście ochrony przed nieuprawnionym dostępem do treści planów, raportów z realizacji zadań,

danych osobowych personelu organizacji i wielu innych podobnych, przełomowe i bezpieczne technologie już powstawały.

Zatem, odpowiadając na pytanie problemowe opracowania, należy wskazać dwa procesy, które wydają się niezbędne do przygotowania branży logistycznej w aspekcie bezpieczeństwa, pod kątem rozważań zawartych w tym opracowaniu.

Po pierwsze, należy uświadomić całą branżę w ujęciu personalnym, a także na etapie edukacji uświadamiać młodych adeptów logistyki, na temat zagrożeń cyberbezpieczeństwa logistyki oraz zarządzania łańcuchami dostaw. Świadomość istnienia, fundamentalnych zasad działania i najczęstszych celów stosowania konkretnych typów zagrożeń, to inherentna część systemu odporności przed nimi.

Po drugie, należy już na etapie projektowania nowych cyfrowych systemów planowania, realizacji oraz nadzoru procesów logistycznych przewidywać włączenie w ich obsługę sztucznej inteligencji. Zdecydowanie ergonomicznie jest obsługiwać i przebywać w pojazdzie opancerzonym, który ma przewidziane miejsce na ewentualny, np. karabin maszynowy, czyli coś długiego, o pewnej szerokości, wyrzucający przedmioty (łuski) tylko w jednym możliwym kierunku, i można się o to jeszcze oparzyć. Przewidzenie włączenia sztucznej inteligencji do obsługi systemów logistycznych nie tylko nie spowoduje zakłóceń, np. w zarządzaniu łańcuchem dostaw, ale również skróci czas, w którym pewne podmioty mogłyby przypuścić cyberatak w związku z niepoprawnym działaniem systemu podczas czas dostosowywania go do sztucznej inteligencji.

Po trzecie, należy zoptymalizować czynnik ludzki z cyfrowym, aby zarówno ludzie nie bali się sztucznej inteligencji w swojej pracy, jak i sztuczna inteligencja przewidywała pewną tolerancję błędu, gdyż nadzoruje nie inny system, ale ludzi. Należy zrównoważenie budować podejście do sztucznej inteligencji w branży logistycznej, aby ona i ludzie ze sobą współpracowali, a nie rywalizowali. Tutaj też trzeba nadmienić świadomość. Koniecznym wydaje się dążenie do takiego stanu, w którym personel rozumie i widzi, że sztuczna inteligencja skutecznie dba o bezpieczeństwo ich pracy, również w obszarze cyberbezpieczeństwa. Postrzeganie przez branżę logistyczną w ujęciu personalnym sztucznej inteligencji jako zagrożenia spowoduje zwalczanie jej poprzez próby sabotażu jej poleceń. W efekcie

ani personel ani sztuczna inteligencja nie będą efektywne. Ucierpi na tym organizacja jako całość. Jak wynika z doświadczeń wojennych, np. w naszym kraju, gdzie dwóch się bije, tam korzysta partyzant. W rozpatrywanym kontekście takie zwalczanie się wytworzy dogodne warunki do ataków zewnętrznych na organizację, w tym w obszarze cyber. Konflikty wewnętrzne, niepokoje społeczne oraz dysfunkcyjność to okoliczności par excellence dla dezinformacji oraz katalizatory jej skuteczności.

Do głównych strategii ochrony przed cyberzagrożeniami w logistyce, zdaniem autorów, należy zaliczyć: zwiększenie świadomości pracowników poprzez szkolenia z zakresu cyberbezpieczeństwa oraz stosowanie polityk dotyczących bezpiecznego korzystania z poczty e-mail i systemów IT, segmentację sieci IT/OT, czyli oddzielenie systemów operacyjnych (OT) od klasycznych systemów IT, w celu ograniczenia możliwości rozprzestrzeniania się ataków. Regularne aktualizacje i łatki bezpieczeństwa, najnowsze wersje oprogramowania oraz systemów operacyjnych, które eliminują luki w zabezpieczeniach, monitorowanie zagrożeń i szybka reakcja poprzez wdrażanie systemów detekcji anomalii i SIEM (Security Information and Event Management) w celu wykrywania podejrzanych aktywności. Zabezpieczenie dostępu do systemów logistycznych poprzez stosowanie uwierzytelniania wieloskładnikowego (MFA), silnych haseł oraz ograniczonego dostępu do kluczowych systemów oraz backup danych, czyli tworzenie regularnych kopii zapasowych i ich przechowywanie w sposób odseparowany od głównej infrastruktury IT.

Podsumowanie

Współczesna logistyka, oparta na cyfryzacji i integracji systemów IT, jest coraz bardziej narażona na cyberzagrożenia. Ataki mogą prowadzić do poważnych zakłóceń operacyjnych, strat finansowych oraz naruszenia poufności danych. Dlatego też przedsiębiorstwa logistyczne muszą nieustannie inwestować w strategie cyberbezpieczeństwa, szkolenia pracowników oraz zaawansowane systemy ochrony, aby minimalizować ryzyko ataków i zapewnić stabilność operacyjną łańcucha dostaw. Kluczowa wydaje się być świadomość cyberzagrożeń oraz ukierunkowanie sztucznej inteligencji nie tylko na bieżące wsparcie procesów logistycznych, ale też na wykrywanie i przeciwdziałanie cyberzagrożeniom. Jednym z głównych zagrożeń dla

współczesnej logistyki, poza atakami cybernetycznymi, zdaje się być dezinformacja. Zarówno dla logistyki cywilnej, jak i wojskowej. Zatem, aby osiągnąć cyberbezpieczeństwo w tym obszarze, charakteryzujące się wysokim stopniem doskonałości, należy podejmować wiele różnych oraz nowych działań, jakie zostały ukazane w tym opracowaniu. Pełna synergia personelu ze sztuczną inteligencją wydaje się być determinującym czynnikiem rozwoju i szerszego stosowania jej w branży logistycznej. Stanowić ona musi narzędzie wspomagające, a nie eliminujące czynnika ludzkiego. Tylko wtedy będzie możliwy do wykorzystania cały jej potencjał. Zarówno w aspekcie poznawczym, jak i praktycznym. Zaproponowane działania przygotowawczo-edukacyjne zdają się dowodzić hipotezy postawionej przez autorów. Lecz wymagają one dużej finezji oraz jeszcze większej wiedzy ich realizatorów. Powierzchowne i niedokładne ich zrealizowanie na pewno nie poprawi poziomu cyberbezpieczeństwa w logistyce.

Literatura

1. Arvato. (b.d.). *Logistyka kiedyś i dziś: Ewolucja czy rewolucja*? Pobrane z: https://blog.arvato.pl/logistyka-kiedys-i-dzis-ewolucja-czy-rewolucja (dostęp: 24.02.2026).
2. Barcik, R., Odlanicka-Poczobutt, M. (2020). *Logistyka 4.0 – wybrane zastosowania*. Politechnika Śląska.
3. Bartczak, K. (2022). Rodzaje cyberzagrożeń i prawne sposoby im przeciwdziałania w kontekście cyfrowych platform technologicznych w logistyce. *Autobusy: Technika, Eksploatacja, Systemy Transportowe, 23*(12), 123-128.
4. Bielecki, M. (2022). *Total logistic management: Logistyka i łańcuchy dostaw 4.0.* Uniwersytet Łódzki.
5. Brühl, M. (2019). Wiedza a dezinformacja w społeczeństwie. W: A. Szczygielska (red.), *Zarządzanie wiedzą w kontekście zapewnienia bezpieczeństwa państwa* (s. 129-142). Akademia Sztuki Wojennej.
6. Dela, P. (2022). Informacja jako narzędzie i obiekt ataku w cyberprzestrzeni. W: W. Scheffs (red.), *Konteksty teoretyczne i praktyczne informacji w organizacji* (s. 279-300). Akademia Kaliska.
7. Ivanov, D., Dolgui, A., Sokolov, B. (2019). The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics.

International Journal of Production Research, 57(3), 829-846. https://doi.org/10.1080/00207543.2018.1488086

8. Janczewski, J. (2018). Zarządzanie łańcuchem dostaw. *Zarządzanie Innowacyjne w Gospodarce i Biznesie, 1*(26), 163-179.
9. Kitler, W. (2022). Przygotowanie systemu kierowania bezpieczeństwem narodowym RP: Zadania i organizacja administracji rządowej szczebla centralnego. *Wiedza Obronna, 278*(1), 11-34.
10. Microsoft. (b.d.). *Co to jest AI dla cyberbezpieczeństwa*? Pobrane z: https://www.microsoft.com/pl-pl/security/business/security-101/what-is-ai-for-cybersecurity (dostęp: 24.02.2026).
11. Mogilnicki, M. (2024). Rosyjskie przygotowania dezinformacyjne do wojny z Ukrainą. *Cybersecurity and Cybercrime, 1*(4), 272-280.
12. Mroczko, F. Kowalczyk L., Mroczko F. (red.). (2023). *Prace naukowe Wyższej Szkoły Zarządzania i Przedsiębiorczości z siedzibą w Wałbrzychu*, *53.* Wyższa Szkoła Zarządzania i Przedsiębiorczości.
13. Netbe.pl. (b.d*.). Specyfika ataków na urządzenia IoT: Jakie zagrożenia wiążą się z Internetem Rzeczy?* Pobrane z: https://netbe.pl/specyfika-atakow-na-urzadzenia-iot-jakie-zagrozenia-wiaza-sie-z-internetem-rzeczy/ (dostęp: 24.02.2026).
14. Orłowska, M. (2023). SAP ERP software as a tool for managing the logistics subsystems of an enterprise. *Zeszyty NaukowebPolitechniki Śląskiej. Organizacja i Zarządzanie, XXX*, 515-526.
15. Orłowska, M., Orłowski, D. (2024). Wyzwania i możliwości zastosowania dronów w logistyce miejskiej. *Gospodarka Materiałowa i Logistyka, 76*(3), 69-79.
16. Osiecki, M. (2023*).* Dezinformacja jako źródło współczesnych cyberzagrożeń. W: M. Marczyk, M. Stolarz, B. Terebiński (red.), *Cyberbezpieczeństwo w teorii i praktyce: Wybrane aspekty* (s. 199-210). Akademia Sztuki Wojennej.
17. Pacek, B., Hoffmann, R. (2013). *Działania sił zbrojnych w cyberprzestrzeni*. Akademia Obrony Narodowej.
18. Piątkowski, Z., Żebrowski, W. (2008). Logistyka w sferze zaopatrzenia. *Postępy Techniki Przetwórstwa Spożywczego,18* (2), 115-121.
19. Płaczek, E. (2018). Logistyka w erze Industry 4.0. *Przedsiębiorczość i Zarządzanie, 19*(11.3), 55-66.

20. RedSteel. (b.d.). *Logistyka 4.0 – trudne wyzwanie czy szansa na rozwój*? Pobrane z: https://redsteel.pl/logistyka-4-0-trudne-wyzwanie-czy-szansa-na-rozwoj/ (dostęp: 24.02.2026).
21. Sokołowska, M. (2024). Logistyka 4.0: *Powiedzmy sobie, o co tak naprawdę chodzi.* Pobrane z: https://www.trans.eu/pl/blog/logistyka-4-0/logistyka-4-0-powiedzmy-sobie-o-co-tak-naprawde-chodzi/ (dostęp: 24.02.2026).
22. Tjahjono, B., Esplugues, C., Ares, E., Pelaez, G. (2017). What does Industry 4.0 mean to supply chain? *Procedia Manufacturing, 13*, 1175-1182. https://doi.org/10.1016/j.promfg.2017.09.191
23. Vault-Tech. (b.d.). *Supply chain attack: Tak ataki na dostawców zagrażają bezpieczeństwu firm*. Pobrane z: https://vault-tech.pl/cyberbezpieczenstwo/supply-chain-attack/ (dostęp: 24.02.2026).