INTERNET RZECZY W INTEGRACJI PROCESÓW LOGISTYCZNYCH W SYSTEMACH ZARZĄDZANIA KRYZYSOWEGO

INTERNET OF THINGS IN THE INTEGRATION OF LOGISTICS PROCESSES FOR CRISIS MANAGEMENT SYSTEMS

Piotr ZASKÓRSKI
piotr.zaskorski@wat.edu.pl

Michał JUREK
michal.jurek@student.wat.edu.pl

Wojskowa Akademia Techniczna
Wydział Cybernetyki
Instytut Organizacji i Zarządzania

Streszczenie: W dzisiejszym społeczeństwie informacyjnym szczególny nacisk kładziony jest na rozwój systemów wspomagających zarządzanie. Jednym z takich rozwiązań, o którym traktuje niniejsza praca jest wykorzystanie rozwiązania Internet of Things w usprawnianiu funkcjonowania systemów logistycznych w zarządzaniu kryzysowym. Rozważany jest ten aspekt w odniesieniu do szerszej perspektywy, jaką są systemy zarządzania kryzysowego. Rozwiązanie to posiada zarówno wady, jak i zalety, które są także przedmiotem dyskusji w tym artykule.
Abstract: In today's information society, emphasis is placed on the development of management support systems. One of the solutions that this study is about is the usage of the Internet of Things in improving the functioning of logistics systems in crisis management. This aspect has been considered in relation to the wider perspective of crisis systems management. This solution has advantages and disadvantages that are also included in this study.
Słowa kluczowe: Logistyka, Internet rzeczy, Zarządzanie kryzysowe, informatyka, systemy logistyczne
Key words: Logistics, Internet of Things, Crisis management, informatics, logistics system

WSTĘP

Szybki rozwój technologii informacyjnych i teleinformatycznych zaowocował powiększającym się wachlarzem możliwości wykorzystania rozwiązań i narzędzi technologicznych nie tylko dla biznesu, ale także w obszarze administracji publicznej. Dzisiejsze struktury państwa i podmiotów międzynarodowych są bardzo złożonymi systemami działania z szerokim spectrum różnego typu zagrożeń dla ich bezpieczeństwa oraz ciągłości działania w różnych stanach funkcjonowania. Jednym z istotnych wymiarów bezpieczeństwa jest wymiar zapewniania ciągłości procesów logistycznych. Stosując dość umowną analogię do przedsiębiorstw produkcyjno-usługowych, w których zapewnianie ich bezpieczeństwa, a w tym tzw. „bezpieczeństwa logistycznego" – można uznać za kryterium dominujące.

Szczególnym rodzajem interakcji państwa i obywatela (całego społeczeństwa) w wymiarze bezpieczeństwa jest zapewnienie ciągłości funkcjonowania systemów zarządzania i reagowania kryzysowego. Łączy się to nie tylko z zabezpieczeniem

odpowiednich sił i środków, lecz także z odpowiednim koordynowaniem działań tak, aby w sposób sprawny i efektywny przeciwdziałać zagrożeniom. Aspekt sprawności procesów logistycznych staje się więc dominującym wymiarem. Włączenie do modelu usprawnień procesów logistycznych w systemach zarządzania kryzysowego – możliwości technologii Internetu rzeczy może sprzyjać doskonaleniu aktualnych rozwiązań. Stąd próba odpowiedzi na pytania: „Jak oraz w jakim stopniu można usystematyzować i usprawnić procesy logistyczne w obszarze systemów zarządzania kryzysowego na różnych szczeblach zarządzania państwa. W przedstawionej koncepcji wykorzystano metodę analizy systemowej i analizę literatury oraz wybranych źródeł internetowych.

1. SYSTEM ZARZĄDZANIA KRYZYSOWEGO

W systemie bezpieczeństwa narodowego RP wyodrębniono dwa podstawowe komponenty:

- Podsystem militarny,
- Podsystem cywilny.

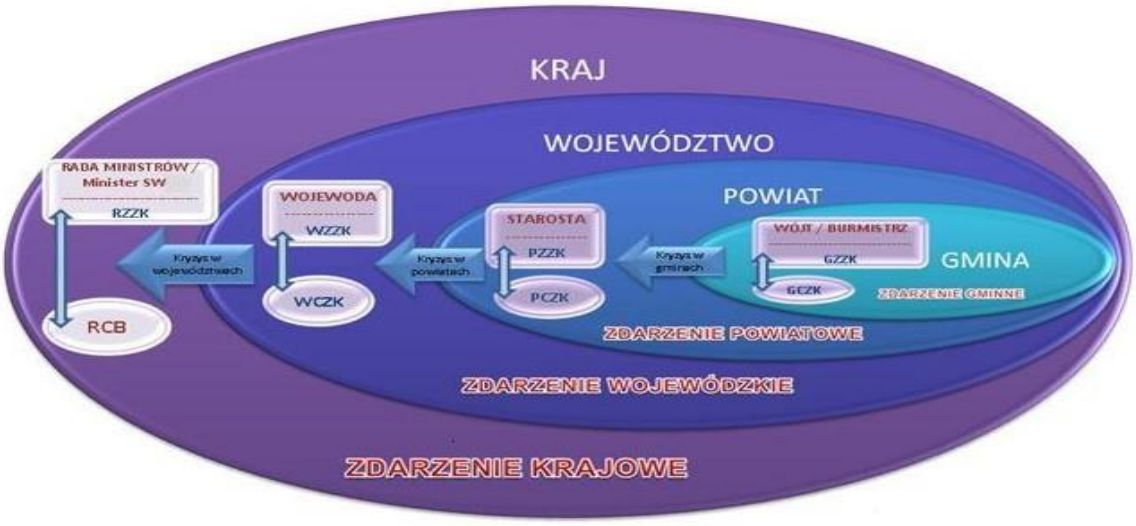
W skład komponentu militarnego wchodzą Siły Zbrojne Rzeczpospolitej Polskiej, które zobligowane są do obrony kraju przed zagrożeniami militarnymi/zbrojnymi. Utrzymywane siły i środki służą przede wszystkim realizacji takich zadań i celów. Procesy logistyczne związane z zapewnieniem odpowiednich zasobów maja charakter względnie autonomiczny. SZ RP uruchamiają swoją aktywność głównie w stanach nadzwyczajnego zagrożenia, które może mieć formę np. zbrojnej napaści na terytorium RP. Siły zbrojne stanowią więc ważny komponent komplementarny z podsystemem cywilnym na czas sytuacji kryzysowej z jej realizacją w postaci konfliktu zbrojnego.

Podsystem cywilny jest komponentem wzmacniającym system bezpieczeństwa narodowego poprzez wykorzystanie wszystkich służb pozamilitarnych (policja, straż pożarna, inne służby i straże), których celem głównym jest zapewnienie ludności cywilnej bezpieczeństwa podczas normalnego funkcjonowania państwa. Stan normalnego funkcjonowania można definiować jako brak zagrożeń, które mogłyby zagrozić wewnętrznej spójności państwa (na przykład atak terrorystyczny).

Szczególnym przypadkiem swoistego połączenia tych dwóch podsystemów jest System Zarządzania Kryzysowego, który został tak zaprojektowany i prawnie usankcjonowany, aby przy niedoborze sił i środków sektora cywilnego, za potwierdzeniem

odpowiednich osób decyzyjnych, mogły zostać użyte zasoby, którymi dysponuje część militarna. Nie może się to jednak przekładać na pogorszenie lub brak możliwości wykonywania pierwotnych zadań przez SZ RP.

W regulacjach ustawowych (prawnych) dotyczących Systemu Zarządzania Kryzysowego (SZK) RP eksponuje się podejście systemowe. Tak więc zarówno System Bezpieczeństwa Narodowego, jak i jego składowe, a w tym SZK i jego ważny komponent, jakim jest System Reagowania Kryzysowego w Polsce traktowane są holistycznie jako uzupełniające się komponenty z możliwością przenikania zadań i zasobów (Rysunek 1). Holizm związany jest tutaj przede wszystkim z takim rozmieszczeniem składowych, by te zapewniały spójność i ciągłość funkcjonowania całego systemu wyższej rangi (hierarchicznie szerszej odpowiedzialności).



Rysunek 1. Ogólna struktura Systemu Zarządzania Kryzysowego RP
Źródło: **http://rcb.gov.pl/zarzadzanie-kryzysowe/** (06.03.2018)

Warto tu nadmienić, że System Reagowania Kryzysowego jest podsystemem Zarządzania Kryzysowego bazującym na odpowiedniej współpracy i przepływie informacji pomiędzy służbami, a centrami zarządczymi oraz odpowiednim przygotowaniu zasobów do użycia w konkretnym działaniu (przy realizacji konkretnego zagrożenia i w celu przeciwdziałania ryzyku utraty logistycznej i informacyjnej ciągłości działania). Analizując działania wyżej wymienionych systemów i ich strukturę daje się zauważyć, że pomimo działania na tym

samym szczeblu, to w tym samym czasie - kompetentne służby i centra zarządzania kryzysowego – komunikują się dwutorowo. Informacja z miejsca zdarzenia musi najpierw dotrzeć do kierującego akcją ratowniczą, a dopiero później może zostać przesłana do osób odpowiedzialnych za zarządzanie kryzysowe na danym poziomie zarządzania w strukturze terytorialnej. Może to doprowadzić do chaosu informacyjnego przy szybkim tempie rozwoju sytuacji. Podczas monitorowania zagrożeń taka sytuacja może opóźnić dotarcie wiadomości do odpowiednich służb lub osób decyzyjnych, które mogą nie zareagować we właściwym czasie na zagrożenia, co może wiązać się z ryzykiem poniesienia większych strat.

Kolejnym problemem, który związany jest ze skutecznością procesów informacyjno-decyzyjnych w SZK jest dostępność informatycznych systemów zarządzania kryzysowego dla służb cywilnych i ich kompatybilność z rozwiązaniami w SZ RP oraz w państwach UE i NATO. Na dzień dzisiejszy użytkowany jest dedykowany dla problematyki zarządzania kryzysowego system informatyczny wspierający procesy reagowania kryzysowego o nazwie „System Wspomagania Reagowania Kryzysowego Alaska (SWRK Alaska)", który ma swoje źródło w resorcie Obrony Narodowej. System ten nie w pełni integruje przepływ informacji w zakresie uruchamiania i podejmowania działań w relacji przykładowo z systemem Państwowej Straży Pożarnej i z Centrami Zarządzania Kryzysowego (CZK). W aktualnym zbiorze rozwiązań dla służb cywilnych do wspomagania podejmowania decyzji jest coraz częściej wykorzystywana platforma sieci powszechnej typu Internet oraz serwisy internetowe takie jak Google Maps, Google Earth. W obszarze zarządzania zasobami logistycznymi w SZK można odwołać się do całej rodziny systemów klasy OLTP (On-Line-Transaction-Processing) oraz OLAP (On-Line-Analyzing-Processing), które mogą wspomagać m. in. procesy gospodarki materiałowej (w tym planowania zaopatrzenia i dostaw), serwisu i monitorowania transportów. Usługi informacyjne tej klasy są również dostępne na platformie Internetu i w tzw. chmurze obliczeniowej. Dodatkowo usługi te mogą być wzbogacone poprzez wykorzystanie tzw. Internetu Rzeczy (łączenia wszystkiego ze wszystkim, IoT - Internet of Things) dla zapewnienia kompleksowości działań i aktualnych danych o bieżącej sytuacji kryzysowej i stanie zabezpieczenia logistycznego.

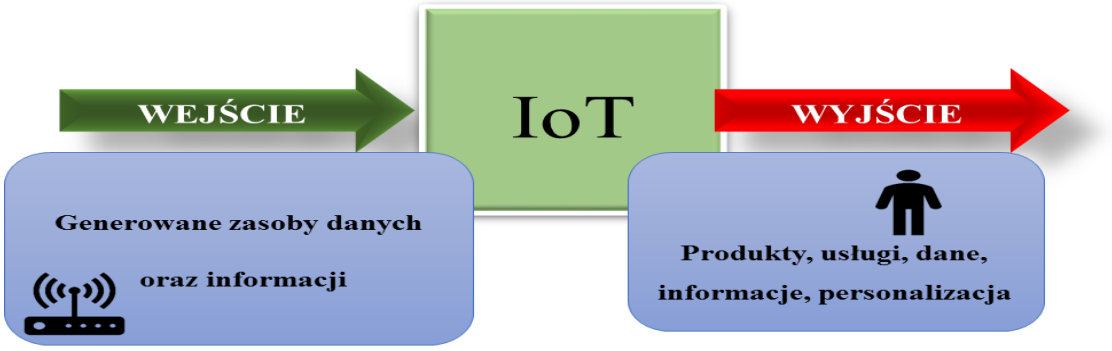
2. ISTOTA INTERNETU RZECZY

Internet rzeczy (IoT) odnosi się do zjawiska/platformy Internetu jako globalnej sieci, która łączy już bardzo dużą liczbę użytkowników poprzez połączenie miliardów urządzeń

(komputerów, tabletów czy smartfonów). Cały proces informacyjny realizowany jest za pomocą odpowiednio dobranych i przygotowanych składników tej sieci (Rysunek 2).

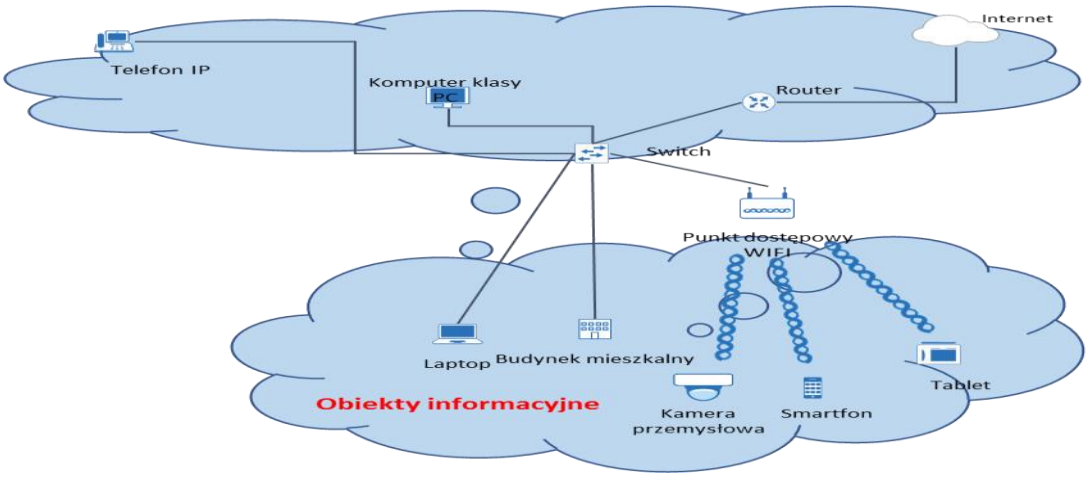
Rysunek 2. Ważniejsze komponenty sieci Internet
Źródło: Opracowanie własne

Internet rzeczy wykorzystuje platformę Internetu do łączenia w jej środowisku „rzeczy" wyposażonych w odpowiednie typy sensorów, czujników lub stanowiących całe obiekty i systemy w jedną spójną komunikacyjnie całość (IoT to sieć łącząca ze sobą „rzeczy", w tym również obiekty infrastruktury, środki transportu i wybrane zasoby materiałowe). Przyjmowane definicje IoT sugerują wyłączenie czynnika ludzkiego. W przypadku systemów zarządzania kryzysowego IoT stanowi niejako uzupełnienie działań ludzkich poprzez możliwość bieżącego monitorowania i zbierania aktualnej informacji o stanie sił i środków działania oraz o potrzebach z tym związanych. Można zatem stwierdzić, że Internet rzeczy jest siecią różnego rodzaju rzeczy i urządzeń, w której może nastąpić wymiana informacji pomiędzy nimi z możliwością ich udostępniania upoważnionemu użytkownikowi (Rysunek 3). Prawa dostępu do generowanej informacji są ważnym przesłaniem dla systemów operujących informacją wrażliwą. W wielu sytuacjach kryzysowych informacja o zasobach i procesach logistycznych może osiągać taki status.



Rysunek 3. Istota sieci IoT
Źródło: Opracowanie własne

Należy tu zwrócić uwagę, że Internet rzeczy w sensu stricto to techniczne połączenia pomiędzy urządzeniami i komunikacja między nimi. Ważnym ograniczeniem jest odpowiednia wielkość urządzeń/sensorów (kart sieciowych) monitorujących niejako zachowania i realizację funkcji przez obiekty/rzeczy połączonych w tej sieci. Zatem w sieci IoT mogą być monitorowane urządzenia elektroniczne, sprzęty medyczne, sprzęty domowe, środki transportu (samochody, samoloty), urządzenia automatyki obiektowej oraz całe budynki, miasteczka, miasta i obiekty/regiony rangi krajowej oraz międzynarodowej.



Rysunek 4. Ramowa architektura sieci IoT
Źródło: Opracowanie własne

Urządzenia stanowiące komponenty funkcjonalne Internetu rzeczy określa się mianem „inteligentnych". Należy jednakże zwrócić uwagę na to, że ich „inteligencja" nie jest cechą immamentną, lecz nabytą przez sposób analizy i wykorzystania danych dostarczanych przez obiekty/zasoby, z którymi współpracują. Tak więc w chwili obecnej elementy takie, jak

sensory, odbiorniki, procesory, smart-urządzenia i ich oprogramowanie coraz częściej stają się nierozerwalną składową szeroko rozumianych produktów (rzeczy). Posiadają ponadto same w sobie zdolności łączenia się z zewnętrzną warstwą infrastruktury IoT. Możliwości takie sprawiają, że następują swoiste zmiany w ich działaniu i w sposobie wykorzystaniu ich funkcji. Wszystko to daje nowe możliwości nie tylko wzrostu funkcjonalności różnego typu rozwiązań, ale także zapewniania ciągłości działania (Zaskórski, 2011) i przeciwdziałania sytuacjom kryzysowym, a w tym monitorowania stanu realizacji procesów logistycznych na dowolnym szczeblu zarządzania. Internet rzeczy może więc stać się integralnym elementem systemu ostrzegania oraz ograniczania asymetrii informacyjnej (Zaskórski, 2012) w zarządzaniu procesami logistycznymi w warunkach zagrożeń i kryzysów.

3. KONCEPCJA WYKORZYSTANIA IoT W PLANOWANIU PROCESÓW ZARZĄDZANIA KRYZYSOWEGO

Planowanie procesów zarządzania kryzysowego jest silnie warunkowane poziomem integracji systemu zarządzania kryzysowego i systemów reagowania kryzysowego, odzwierciedlających konkretne potrzeby działania. Wymaga to przede wszystkim usprawnienia przepływu informacji pomiędzy tymi systemami, co wpływa na zapewnienie ciągłości działania na każdym szczeblu (w danym rejonie działania) różnych obiektów występujących w danej konfiguracji. Można tu skorzystać z porównania do wprowadzonej przez firmę Microsoft funkcji Fast Boot w systemie Windows, która zapewnia wrażenie (niejako symulację) ciągłego korzystania z urządzenia klasy PC mimo pełnego zamknięcia systemu. Dla realizacji kryterium zapewniania informacyjnej ciągłości działania muszą zostać zabezpieczone odpowiednie zasoby wg uregulowań legislacyjnych oraz utworzona bądź zmodyfikowana odpowiednia infrastruktura (Tabela 1), a w tym wykonawstwo musi być kompetencyjnie przygotowane i uzasadnione (organy, instytucje). W obecnym porządku prawnym każda ze służb odpowiada za pewien wycinek działań przy określonej sytuacji kryzysowej, nawet jeśli ma to wymiar monitorowania. Ustawodawca musi zmienić obowiązujące akty prawne lub uchwalić nowe tak, aby regulowały istotne kwestie użycia infrastruktury bądź zasobów innych służb lub ogniw wykonawczych w celu realizacji specjalizowanych funkcji i obowiązków z zakresu zarządzania kryzysowego.

Odpowiednie organy (w tym służby logistyczne podmiotów działania na danym szczeblu) powinny zostać zobligowane do zapewnienia dostępu do infrastruktury, naprawy,

jej modernizacji, jak i usprawniania oraz doskonalenia. Może to być jednym z warunków niezakłóconego przebiegu wymiany informacji pomiędzy różnymi węzłami systemu oraz stworzenia podstaw do pracy ciągłej w różnych wymiarach: logistycznym, organizacyjnym, personalnym itp. Możliwość stałego monitorowania różnych obiektów nie tylko infrastruktury krytycznej, ale także elementów wykonawczych (w tym urządzeń i innych zasobów) może sprzyjać weryfikacji i urealnianiu bieżących planów działania/reagowania kryzysowego. Dostęp do bieżącej informacji pochodzącej bezpośrednio z obiektów monitorowanych, a często w jakiś sposób zagrożonych (sygnały z różnego rodzaju czujników np. temperatury, dymu, skażeń i innych) staje się ważną determinantą skuteczności realizacji procesów zarządzania kryzysowego i działań w systemie reagowania kryzysowego. Dane pobrane z centrów danych mogą wspomagać procesy planistyczne oraz w pewnym sensie automatycznie inicjować procesy reagowania kryzysowego.

Tabela 1. Wymagane środki do zapewnienia integracji technologiczno-informacyjnej

Zasoby	Legislacja	Infrastruktura
- pieniężne - ludzkie - intelektualne (oprogramowanie)	- zmiany ustaw i aktów wykonawczych - przyjęcie nowych aktów prawnych	- czujniki - stacje pomiarowe - centra danych - sieci teleinformatyczne

Źródło: opracowanie własne

Władza centralna i samorządowa poprzez swoje działania i gospodarowanie środkami budżetowymi może dysponować zasobami, zapewniającymi założony poziom bezpieczeństwa poprzez optymalne ich zużycie w operacjach i systemach zarządzania kryzysowego. Racjonalne planowanie zasobów ludzkich oraz ich wykorzystywanie jest warunkowane dostępem do bieżącej informacji o nich ze szczególnym uwzględnieniem stanów osobowych, kompetencji (np. kompetencji i umiejętności informatycznych) oraz dyspozycyjności. Skuteczne planowanie działań jest przedsięwzięciem wielowymiarowym, gdzie wszelkie zasoby informacyjne i wytwory intelektualne (wykonane oprogramowanie, systemy informatyczne) powinny być także chronione. Skuteczność to również niezawodność różnych narzędzi i ich wsad informacyjno-intelektualny. Ustalenie granic kompetencyjnych w ujęciu ról systemowych może sprzyjać klarownemu podziałowi odpowiedzialności np. za stan i bezpieczeństwo udostępnionej/planowanej do użycia infrastruktury (na przykład pomiarowej). Nieklarowność kompetencyjna może wpływać na nieokreśloność procedury planistycznej, szczególnie rozproszenie kompetencyjne wymusza tzw. ład informacyjny, gdzie każdy uczestnik procesu planistycznego zna swój obszar zadaniowo-kompetencyjny

i uprawnienia w dostępie do zasobów informacyjnych (np. walka kompetencyjna na kolei jest przykładem niespójności kompetencyjnej i odpowiedzialności, ponieważ inna firma odpowiada za tory, inna za sieć trakcyjną, a żadna z nich nie bierze odpowiedzialności za zaistniałe zdarzenie np. kradzież sieci trakcyjnej i niesprawność żądanej usługi). Stąd uporządkowanie informacyjne i dostęp do aktualnej informacji sytuacyjnej w połączeniu z informacją analityczno-historyczną może ograniczać wąskie gardło w opracowaniu i użytkowaniu jednolitych narzędzi i systemów informatycznych, wspomagających procesy podejmowania decyzji.

Wykorzystanie usług klasy IoT staje się w pewnym sensie gwarancją dostępu do aktualnych danych, uwzględniania w procesach planowania odniesienia do aktualnych potrzeb oraz dysponowanego stanu sił i środków. Przyjęta koncepcja integracji źródeł informacji z uwzględnieniem platformy IoT daje duże możliwości w przypadku realizacji zadań w sytuacji kryzysowej a więc pod silną presją czasu i jego stały deficyt. Poprawa przepływu informacji oraz wymiany danych i zastosowanie automatyzacji procesu zbierania danych i wymiany informacji w trybie on-line powinno poprawić wydajność oraz szybkość działań przygotowawczo-decyzyjnych i skuteczności realizacji procesów zabezpieczająco-wykonawczych, w tym procesów logistycznych. Stąd platforma IoT tworzy bazę do budowy modułowego, zintegrowanego systemu informatycznego wspomagającego proces zarządzania kryzysowego na wszystkich jego szczeblach. Takie oprogramowanie w obszarze bezpieczeństwa narodowego zarówno w podsystemie cywilnym, jak i militarnym staje się w dzisiejszych czasach bardzo potrzebne i wręcz obligatoryjne. Daje to możliwość wzrostu poziomu bezpieczeństwa także całego systemu zarządzania kryzysowego.

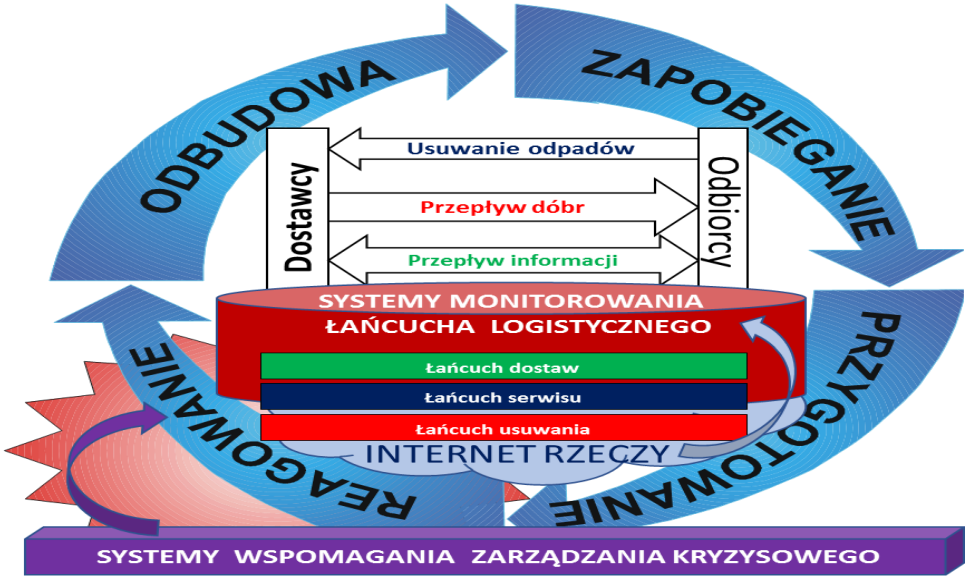
4. ZARYS MODELU WYKORZYSTANIA IoT W PLANOWANIU I MONITOROWANIU PROCESÓW LOGISTYCZNYCH

W planowaniu zarządzania kryzysowego obszar planowania logistycznego, a w szczególności planowania materiałowego zajmuje ważne miejsce. Współczesne systemy logistyczne próbują dostosowywać się do dynamicznie zmieniających się warunków. Główną determinantą efektywnego i skutecznego działania mogą być istniejące technologie teleinformatyczne. Wyzwania XXI wieku potwierdzają, że przejście do dynamicznych struktur procesowych staje się warunkiem koniecznym efektywności i sprawności procesów logistycznych. Dotyczyć to może problemów transportu, produkcji, gospodarki materiałowej,

magazynowania itp. Szybki obieg aktualnej informacji o bieżących, dynamicznie zmieniających się potrzebach i możliwościach logistycznych oraz wieloaspektowe analizy determinują skuteczność i ciągłość działania systemów zarządzania i reagowania kryzysowego. Współczesne systemy i procesy logistyczne są podatne na współdziałanie z otoczeniem. Każdy element tego systemu - jako ogniwo w łańcuchu łączącym dostawcę z odbiorcą (Pawelczyk, Zaskórski, 2014) - zorientowany jest w wyznaczonym czasie na realizację określonego procesu w kontekście celu całego systemu zarządzania kryzysowego. Podmioty i realizatorzy zadań z obszaru zarządzania kryzysowego (w tym reagowania kryzysowego) funkcjonując z dostępem do aktualnej, jednoznacznej, wspólnej i wiarygodnej informacji mogą zwiększyć realizowalność procesów i ich efektywność. Podejście systemowe w zarządzaniu logistyką w SZK zmienia strukturę wykonawczą procesów logistycznych. Coraz większego znaczenia nabierają wyspecjalizowane systemy logistyczne, które mogą pełnić rolę kompleksowych dystrybutorów i dysponentów zasobów.

Logistykę w SZK należy postrzegać jako proces zaopatrywania w zasoby i utrzymywanie ich sprawności tak, aby materiały i energia oraz towary były zawsze w dyspozycji we właściwym czasie, na właściwym miejscu i we właściwej ilości. W obszarze zarządzania procesami logistycznymi w SZK należy eksponować przede wszystkim funkcję planowania, koordynacji i sterowania w aspekcie czasowym i przestrzennym w danym systemie zarządzania lub reagowania kryzysowego. Analiza systemowa każe spojrzeć na łańcuch dostaw jako jeden z trzech bazowych elementów łańcucha logistycznego (Rysunek 5) i uwzględnić stałe relacje między odbiorcą a dostawcą z zapewnieniem dostępu do aktualnej informacji o stanie i przem ieszczaniu się zasobów poprzez proces stałego ich monitorowania. Zapewnienie ciągłości funkcjonowania łańcucha dostaw z wykorzystaniem infrastruktury IoT istotnie poprawia relacje z otoczeniem, gdzie konkretny element organizacyjny SZK jest tylko jednym z ogniw w łańcuchu przepływu rzeczy i informacji. Dzięki IoT łańcuch dostaw i relacje ogniw współdziałających mogą być stabilne.

W działaniach silnie warunkowanych czasowo ważnym komponentem staje się również łańcuch serwisu, który obejmuje procesy zapewnienia użyteczności poszczególnych produktów (obiektów/środków transportu/rzeczy). W łańcuchu tym mogą być zdalnie monitorowane i uruchamiane procesy kontroli poprawności funkcjonowania określonego produktu/obiektu z ewentualną jego naprawą lub wymianą itp. Łańcuch usuwania natomiast związany jest z procesami eliminacji produktów oraz odpadów powstających w procesach wykonawczych (np. reagowania kryzysowego).



Rysunek 5. Ogólny model integracji procesów logistycznych w SZK
Źródło: opracowanie własne na podstawie: Pisz I., Sęk T., Zielecki W., Logistyka w przedsiębiorstwie (2013), s. 0-41

W prezentowanym na rysunku 5 modelu integracji procesów logistycznych ważnym założeniem jest ujęcie systemowe, co oznacza, że uwzględniane są różnorakie relacje między dostawcą a odbiorcą i między różnymi poziomami zarządzania zasobami i systemami. Logistyka jest więc spójnym systemem wkomponowanym w pełny cykl zarządzania kryzysowego. Logistyka jako spójny i kompletny oraz kompleksowy system działania z jednoznacznie zdefiniowanymi procesami i relacjami (Tomaszewski i Zaskórski, 2013) zapewnić może wzrost efektywności procesów dostarczania zasobu do wyznaczonego miejsca, na czas i z kosztami na optymalnym poziomie w określonych warunkach działania.

Poziom realizacji tak zdefiniowanych celów jest determinowany możliwością bieżącego sterowania oraz wykorzystania właściwości sprzężenia zwrotnego poprzez monitorowanie i ewidencjonowanie wyników działań z wykorzystaniem platformy IoT. Spójność relacji pomiędzy poszczególnymi podsystemami (ogniwami) logistyki i operowanie wspólną bazą informacyjną (np. informacja o wymaganej ilości produktu może być równocześnie wykorzystywana przez różnych realizatorów procesu logistycznego z możliwością wspólnej reakcji na tę informację w całym łańcuchu logistycznym). Operowanie jednolitymi, aktualizowanymi on-line zasobami informacyjnymi wzmacnia wartość łańcucha dostaw. We wspomaganiu procesów zarządzania łańcuchami logistycznymi - szczególną rolę mogą

odgrywać systemy klasy Business Intelligence. Systemy te wymagają jednak zasileń z systemów bieżącego działania. Ten atrybut może być przypisany źródłom danych generowanych z platformy IoT, ze szczególnym uwzględnieniem możliwości monitoringu poszczególnych składowych w łańcuchu logistycznym (systemy satelitarne, systemy automatycznej identyfikacji RFID itp.) dla zapewnienia ciągłości działania i bezpieczeństwa (Zaskórski, 2011).

5. TENDENCJE ROZWOJOWE W WYKORZYSTANIU IoT SYSTEMACH REAGOWANIA KRYZYSOWEGO

Ciągły i intensywny rozwój techniki może zaowocować wytworzeniem nowych produktów, które w dużym stopniu przyczynią się do uproszczenia lub rozszerzenia wykorzystania technologii Internetu Rzeczy w systemach reagowania kryzysowego. Ważna przy tym staje się miniaturyzacja czujników lub też odpowiednia ich integracja z przedmiotami codziennego użytku jak na przykład telefon typu smartfon. Zjawisko to przyczyni się zapewne do sprawniejszego przeprowadzania akcji ratowniczych a przede wszystkim wpłynie na czas i sposób ich kompleksowego przygotowania do przeciwdziałania zidentyfikowanym zagrożeniom. Za postępem techniki musi jednak iść, a nawet wyprzedzać postęp legislacyjny. W obecnym stanie prawnym należy dążyć do wzbogacenia unormowań w zakresie tworzenia, wykorzystania i utrzymaniu systemów bazujących na IoT. Różne braki w tym zakresie mogą powodować pewne bariery w zakupie i wykorzystaniu sprzętu, a w tym:

- Ograniczenie możliwości zakupu odpowiedniego sprzętu (np. brak świadomości decydentów),
- Niewystarczające przygotowanie osób odpowiedzialnych za projektowanie i wdrożenie infrastruktury,
- W razie wystąpienia awarii lub też uszkodzenia (w tym też z winy osób postronnych) brak jest unormowań w zakresie kompetencji i odpowiedzialności za powstałe w ich wyniku szkody.

Wydaje się jednak, że pomimo różnych barier i pewnych niedogodności można prognozować zwiększanie się roli Internetu Rzeczy w systemach reagowania kryzysowego. Postępująca cyfryzacja i powszechny plan informatyzacji kraju owocuje już pewnymi rozwiązaniami, które podnoszą skuteczność funkcjonowania systemów zarządzania (szczególnie reagowania) kryzysowego i zapewniają ciągłość ich działania poprzez ciągłość zintegrowanych procesów logistycznych. Znajomość tych procesów to przede wszystkim

dążenie do zachowania kryterium ich kompletności i spójności. Korzystając z możliwości platformy IoT można doprowadzić do monitorowania krytycznych aktywności i ich realizatorów z przypisaną rolą, ustaloną wg zdolności wykonania tej roli. Sposób realizacji każdego procesu i poziom jakości jego wyników uzależniony jest od bieżącej, aktualnej informacji o potrzebach i możliwościach działania. Takie systemowe postrzeganie procesu umożliwia pełną identyfikację stanu każdego obiektu składowego oraz weryfikację i korektę planów działania (np. planów awaryjnych).

Rysunek 6. Ramowe warunki efektywnego procesu decyzyjnego
Źródło: Opracowanie własne

Analizując aktualny stan wykorzystania IoT oraz postrzegane tendencje rozwojowe można prognozować, że dynamika i elastyczność działań w systemach zarządzania będzie wymuszać konieczność bezpośredniego monitorowania całego systemu i procesów logistycznych, warunkujących jego ciągłość działania skorelowaną z funkcjonowaniem różnych komponentów. Determinantą osiągania takich celów jest niewątpliwie dostęp do uniwersalnych i dedykowanych narzędzi informatycznych (Rysunek 6). Szczególną rolę ma tu platforma Internetu, usług w chmurze obliczeniowej (CC/Cloud Computing) oraz Internet rzeczy. Wiele podmiotów administracji publicznej podobnie jak podmiotów biznesowych - zmierza dziś ku integracji i skoordynowaniu wewnętrznych procesów z procesami w ich otoczeniu. Widać więc, że informatyczne wsparcie łańcucha logistycznego eksponuje integrację wielu podmiotów w procesach przepływu dóbr czy realizacji usług logistycznych.

Poszczególne ogniwa łańcucha logistycznego wymagają skoordynowanych przepływów zasobów na bazie aktualnej informacji (Warszewski i Zaskórski, 2015). Szczegółowy obraz każdego procesu i sposób jego realizacji z odpowiednim odwzorowaniem informacyjnym mogą wzmacniać skuteczność i efektywność systemową. Większość z funkcji analityczno-prognostycznych może być realizowana z wykorzystaniem usług w tzw. chmurze

obliczeniowej (na platformie Internetu), z wykorzystaniem usług skalowalnych wg faktycznych potrzeb. Internet rzeczy będzie rozszerzał funkcjonalność źródeł informacji. Wśród systemów integrujących działanie różnych ogniw w realizacji procesów logistycznych i łańcucha dostaw modyfikowane będą systemy klasy SCM (Supply Chain Management/ Zarządzanie Łańcuchem Dostaw) w kierunku ich „inteligentnej" struktury. System ten jest kompleksowym narzędziem klasy ZSIZ i w połączeniu z zasileniami informacyjnymi z platformy IoT może generować nowe jakościowo rozwiązania w obszarze planowania, jak i oceny wyników realizacji procesów zarządzania kryzysowego, co daje także możliwość integracji i synchronizacji działań wielu podmiotów w łańcuchu (systemie) logistycznym.

PODSUMOWANIE

Zjawisko Internetu Rzeczy może być bardzo przydatne w kreowaniu efektywności procesów logistycznych w systemach zarządzania i reagowania kryzysowego. Niesie to jednak nie tylko nowe możliwości, lecz także zagrożenia, które mogą stanowić poważny problem we wdrażaniu różnego rodzaju systemów bazujących na urządzeniach IoT. Jednakże odpowiednie ich przygotowanie zabezpieczenie pozwoli na zwiększenie elastyczności, spójności i efektywności podejmowanych działań. Z perspektywy logistyki i funkcjonowania łańcuchów logistycznych - trend ten daje możliwość opracowania nowych systemów, które nie tylko usprawnią wdrożone rozwiązania, lecz też dadzą początek innym, bardziej innowacyjnym i przystępnym dla człowieka oraz środowiska. Zaprezentowany tu zarys koncepcji może być pewną przesłanką do utworzenia nowoczesnego systemu wspomagania działań logistycznych w SZK. System ten mógłby być wykorzystywany we wspomaganiu procesów decyzyjnych.

Współczesne procesy i łańcuchy logistyczne tworzą dziś globalną sieć logistyczną. Postrzeganie tego w kategoriach systemowych z uwzględnieniem możliwości bieżącego informowania o potrzebach i możliwościach działania – stwarza okazję do skuteczniejszego procesu decyzyjnego. Traktując samą logistykę jako złożony system działania, coraz częściej zwraca się uwagę na dynamikę zmian w otoczeniu. Dynamika we współdziałaniu różnych podmiotów może być kontrolowana poprzez informacyjną integrację procesów w całym łańcuchu logistycznym. Działania w dynamicznym środowisku wymagają jednak odpowiedniej bazy techniczno-technologicznej, a w tym odwołania się do zjawiska IoT.

LITERATURA

1. Bojarski, W.W. (2001). *Efektywność systemowa przedsięwzięć gospodarczych.* Warszawa: WSZZIP.
2. Champy, J. (2003). *X – Engineering przedsiębiorstwa*. *Przemyśl swój biznes w erze cyfrowej – procesy, propozycja, partycypacja, partnerstwo*. Warszawa: PLACET.
3. Durlik, I. (2007). *Inżynieria zarządzania. Strategie organizacji produkcji. Nowe koncepcje zarządzania.* Warszawa: PLACET.
4. Pawelczyk, K. Zaskórski, P. (2014). Ocena złożoności i wartości projektów w systemach logistycznych. *Systemy Logistyczne Wojsk, nr 40/2014,* 237—253
5. Pisz, I. Sęk, T. Zielecki, W. (2013). *Logistyka w przedsiębiorstwie*. Warszawa: PWE.
6. Zaskórski, P. (red.). (2011). *Zarządzanie organizacją w warunkach ryzyka utraty informacyjnej ciągłości działania.* Warszawa: WAT.
7. Skowronek, Cz. Sarjusz-Wolski, Z. (2012). *Logistyka w przedsiębiorstwie.* Warszawa: PWE.
8. Tomaszewski, Ł. Zaskórski, P. (2013). Strategia zarządzania logistyką w aspekcie bezpieczeństwa systemowego. *Systemy Logistyczne Wojsk, nr 39/2013,* 375-407
9. Warszewski, P. Zaskórski, P. (2015). Model zarządzania procesowego w doskonaleniu systemów logistycznych. *Gospodarka Materiałowa i Logistyka nr 5/2015,* 809-825
10. Zaskórski, P. (2012). Wirtualizacja organizacji w „chmurze" obliczeniowej. *Ekonomika i Organizacja Przedsiębiorstwa, nr 3/ 2012*, 24-33
11. Zaskórski, P. (2012). *Asymetria informacyjna w zarządzaniu procesami*. Warszawa: WAT.
12. Zaskórski, P. (2013). Systemy klasy BI platformą współczesnych organizacji. W: W. Gonciarski (red.), U. Ornarowicz (red.), *Współczesne zarządzanie: różnorodność prob lemów i sposobów ich rozwiązywania* (monografia, 233–246). Warszawa: WAT.
13. Miller, M. (2016). *Internet rzeczy. Jak inteligentne telewizory, samochody, domy i miasta zmieniają świat*. Warszawa: Wydawnictwo PWN.
14. http://csikgw.wp.mil.pl/pl/30_8.html (06.03.2018)
15. http://www.nowastrategia.org.pl/itwzk/ (06.03.2018)
16. https://niebezpiecznik.pl/post/ktos-zhackowal-156-miejskich-syren-alarmowych/ (06.03.2018)

17. https://maps.shodan.io/#16.720385051693988/3.515625/3/satellite/webcam (06.03.2018)
18. https://obywatel.gov.pl/dokumenty-i-dane-osobowe/mdokumenty (06.03.2018)