

**MULTIŚRODOWISKOWE ZAGROŻENIA BEZPIECZEŃSTWA GLOBALNYCH  
ŁAŃCUCHÓW DOSTAW**  
**MULTI-ENVIRONMENTAL SAFETY THREATS FOR GLOBAL SUPPLY CHAINS**

**Krzysztof FICON**  
krzysztof.ficon@wp.pl

**Grzegorz KRASNODEBSKI**  
krasnodębski.grzegorz@wp.pl

Akademia Marynarki Wojennej  
Wydział Dowodzenia i Operacji Morskich

*Streszczenie: Tematem pracy jest bezpieczeństwo globalnych łańcuchów dostaw rozpatrywane z punktu widzenia zagrożeń generowanych przez 4 kluczowe środowiska bezpieczeństwa, tj. środowisko naturalne, geopolityczne, globalne i organizacyjne. Środowisko naturalne (przyrodnicze) i środowisko geopolityczne generują tzw. zagrożenia zewnętrzne, na które tylko w niewielkim stopniu możemy defensywnie oddziaływać. Środowiska globalne (rynkowe) i organizacyjne generują zagrożenia wewnętrzne, na które w dużym stopniu możemy ofensywnie oddziaływać i skutecznie minimalizować prawdopodobieństwo ich wystąpienia oraz negatywne ich skutki. Każde środowisko zostało szczegółowo scharakteryzowane pod kątem wpływu na kształtowanie bezpieczeństwa globalnych łańcuchów dostaw.*

*Abstract: The topic of work is the security of global supply chains considered from the point of view of threats generated by 4 key security environments, i.e. the natural, geopolitical, global and organizational environment. The natural (natural) environment and the geopolitical environment generate the so-called external threats that we can only defuse to a small degree. Global (market) and organizational environments generate internal threats, to which we can have an offensive influence and effectively minimize the likelihood of their occurrence and their negative effects. Each environment has been detailed in terms of its impact on shaping the security of global supply chains.*

*Słowa kluczowe: bezpieczeństwo, geopolityka, łańcuch dostaw, organizacja, przyroda, rynek, ryzyko, środowisko.*

*Keywords: security, geopolitics, supply chain, organization, nature, market, risk, environment.*

## **WPROWADZENIE**

Wiek XXI to faza dynamicznie rozwijającej się gospodarki globalnej, której symbolem są transgraniczne, prowadzone na wielką światową skalę przepływy towarów, usług, kapitału i pracy, bazujące na błyskawicznych strumieniach informacyjnych determinowanych przez współczesną technologią komputerową. Jedną z wielu definicji (Słownik, 2007, s. 106) globalizację określa jako: „(...) tworzenie strategii międzynarodowych przez organizacje mające na celu ekspansję zagraniczną i działanie na skalę światową”. Bardziej ogólna definicja mówi, że globalizacja oznacza umiędzynarodowienie wszelkich stosunków – politycznych, gospodarczych, społecznych, a nawet personalnych, co dodatkowo akcentuje rolę multimedialnych i multimodalnych strumieni niematerialnych i materialnych obiegających bez przeszkód całą kulę ziemską.

Globalny łańcuch dostaw przebiegający w ogólności w światowym wymiarze czasoprzestrzennym jest potencjalnie narażony na rozmaite zagrożenia i niebezpieczeństwa, będące skutkiem wielu czynników obiektywnych i subiektywnych, losowych i przypadkowych, a także zamierzonych i niezamierzonych (Jażdżewska-Gutta, 2013). W transgranicznych, międzykontynentalnych przepływach logistycznych i biznesowych występuje szereg zdarzeń, które mogą zakłócać precyzyjnie zaplanowany strumień łańcucha dostaw. Sytuacja ta rodzi kategorię ryzyka, będącą wymierną postacią niepewności, które może być kwantyfikowane – jako miara jakościowa lub ilościowa. Ryzyko będące pochodną zagrożeń i niepewności, jako miara wymierna może być przedmiotem racjonalnego zarządzania, co pozwala na skuteczne sterowanie globalnym łańcuchem dostaw, np. według kryterium maksymalnej skuteczności i bezpieczeństwa (Konecka, Stajniak, Szopik-Depczyńska, 2016). Globalne łańcuchy dostaw są stosunkowo silnie narażone na działanie różnych niepożądanych czynników i przeciwności powodujących wzrost ryzyka związanego z przepływami fizycznymi. Zakłócone przepływy fizyczne mogą generować rozmaite skutki natury organizacyjno-technicznej i przede wszystkim natury ekonomicznej oznaczające w tym przypadku dodatkowe koszty i nakłady i związane z tym straty (Brdulak, 2012).

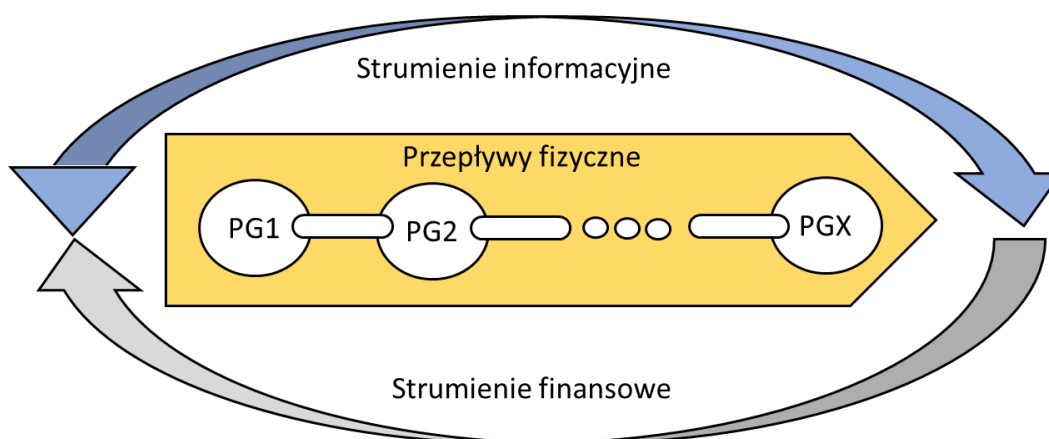
Celem pracy jest scharakteryzowanie podstawowych kategorii zagrożeń i związanego z nimi ryzyka, jakie towarzyszy globalnym łańcuchom dostaw i wskazanie ewentualnych dróg jego minimalizacji, celem ograniczenia potencjalnych strat. Zaproponowane sposoby mogą posłużyć menedżerom szczebla strategicznego do skutecznego antycypowania nadmiernego ryzyka i zachowania względnej płynności i sprawności łańcucha dostaw w warunkach potencjalnych zagrożeń na globalnych rynkach światowych.

## **1. POJĘCIE I ATRYBUTY BEZPIECZEŃSTWA ŁAŃCUCHÓW DOSTAW**

Intensywność współczesnych strumieni handlu światowego (wymiany międzynarodowej) cechuje wielka dynamika, której podstawą są szeroko rozumiane łańcuchy dostaw, obejmujące przepływy dóbr materialnych od pierwotnych źródeł pozyskania (naturalnych lub sztucznych) poprzez liczne ogniwa pośrednie, aż do końcowego odbiorcy (konsumenta). Słownik terminologii logistycznej (2016, s. 93) pojęcie łańcucha dostaw definiuje binarnie jako: „(...) 1) proces – sekwencja zdarzeń w przemieszczaniu dóbr zwiększająca ich wartość lub 2) struktura (organizacja) – grupa przedsiębiorstw realizująca wspólne działania niezbędne do zaspokojenia popytu na określone produkty w całym łańcuchu przepływu dóbr – od pozyskania surowców od dostawców do ostatecznego odbiorcy”. W obu przypadkach podstawą efektywnego przepływu dóbr materialnych jest

skuteczne zarządzanie zarówno dynamicznym procesem przebiegającym na osi czasu, jak też statyczną organizacją (strukturą) zajmującą się realizacją tego procesu (Rutkowski, 1999).

Z kolei M. Christopher (1998, s. 18) łańcuch dostaw definiuje jako: „(...) sieć powiązanych i współzależnych organizacji, które – działając na zasadzie wzajemnej współpracy – wspólnie kontrolują, kierują oraz usprawniają przepływy rzeczowe i informacyjne od dostawców do ostatecznych użytkowników”. Zbliżone podejście reprezentuje J. Witkowski (2003, s. 17), kiedy definiuje łańcuchy dostaw jako: „(...) współdziałające w różnych obszarach funkcjonalnych firmy wydobywcze, produkcyjne, handlowe, usługowe oraz ich klienci między którymi przepływają strumienie produktów, informacji i środków finansowych”. W tym sensie łańcuch dostaw to, z jednej strony, zbiór podmiotów gospodarczych realizujących skutecznie określone cele biznesowe, z drugiej, towarzyszące mu przepływy fizyczne dóbr i towarów, które są sterowane za pomocą strumieni informacyjno-decyzyjnych według ekonomicznych kryteriów finansowych (rys. 1).



Rys. 1. Idea funkcjonowania łańcucha dostaw

Źródło: Opracowanie własne.

Formalnie łańcuch dostaw (*LD*) możemy zdefiniować za pomocą następującego wyrażenia:

$$LD: \quad PG_i \times PG_{i+1} \rightarrow PF \times SI \times SF; \quad i = \overline{1, I} \quad (1)$$

gdzie:

$PG_i$  – *i*-ty podmiot gospodarczy,

$PF$  – przepływy fizyczne towarów i usług,

$SI$  – strumień informacyjno-decyzyjny,

$SF$  – strumień finansowy.

Pojęcie skuteczności na gruncie prakseologii T. Pszczołowski (1978, s. 219) definiuje jako: „(...) działania prowadzące od osiągnięcia zamierzonego celu”. Jeśli wytyczony cel nie zostanie osiągnięty określone działania są nieskuteczne. W przypadku łańcuchów dostaw tym celem jest harmonijna i efektywna realizacja sekwencji zdarzeń (transakcji handlowych) należących do danego łańcucha, gwarantująca spełnienie jego misji, czyli zaspokojenie popytu końcowego klienta, zgodnie z określonymi standardami obsługi klienta (Tarasiewicz, 2014). Jedną z istotnych cech skuteczności jest bezpieczeństwo działań prowadzących do osiągnięcia zamierzonego celu. Realizacja każdego celu w szczególności misji globalnego łańcucha dostaw może być w różnym stopniu zagrożona i zakłócona przez rozmaite czynniki zewnętrzne i wewnętrzne. Pierwotnym źródłem niepewności realizacji celu są więc zagrożenia, które w przypadku globalnego łańcucha dostaw są szczególnie rozbudowane i wielowątkowe (Jażdżewska-Gutta, 2013). Bez trudu można wyobrazić sobie spektrum potencjalnych zagrożeń w procesie spedycji międzynarodowej z udziałem m.in. drogi morskiej, przekraczającej różne systemy polityczne, granice państwowe, kultury biznesowe, strefy klimatyczne itp.

Kluczowe pojęcie bezpieczeństwa powszechnie jest definiowane jako stan braku zagrożeń i w mowie potocznej oznacza pewnego rodzaju dobrostan pozwalający na stabilne funkcjonowanie i perspektywiczny rozwój – człowieka, grupy społecznej, a także organizacji czy państwa, a nawet świata. Bezpieczeństwo posiada dualny statyczno-dynamiczny charakter, gdyż z jednej strony jest chwilowym stanem, z drugiej zmiennym procesem, najczęściej stochastycznym (Ficoń, 2007). O dynamice bezpieczeństwa decyduje szerokie spektrum zagrożeń generowanych przez bliższe i dalsze otoczenie badanego podmiotu (przedmiotu). Wiązka rozmaitych zagrożeń jest strumieniem ciągłym, dlatego stan bezpieczeństwa jest stanem zmiennym i chwilowym. Aby zachować pożądane standardy bezpieczeństwa konieczne jest świadome i nieustanne zarządzanie przestrzenią zagrożeń we wszystkich jej wymiarach (Ficoń, 2015). Niestety nie wszystkie rodzaje i spektra nieustannych zagrożeń dają się precyzyjnie identyfikować, prognozować i skutecznie zarządzać. Bardziej formalnie można powiedzieć, że bezpieczeństwo jest funkcją zagrożeń, które zawsze symbolizuje niepewność:

$$B = f(Z) \rightarrow Np \quad (2)$$

gdzie:

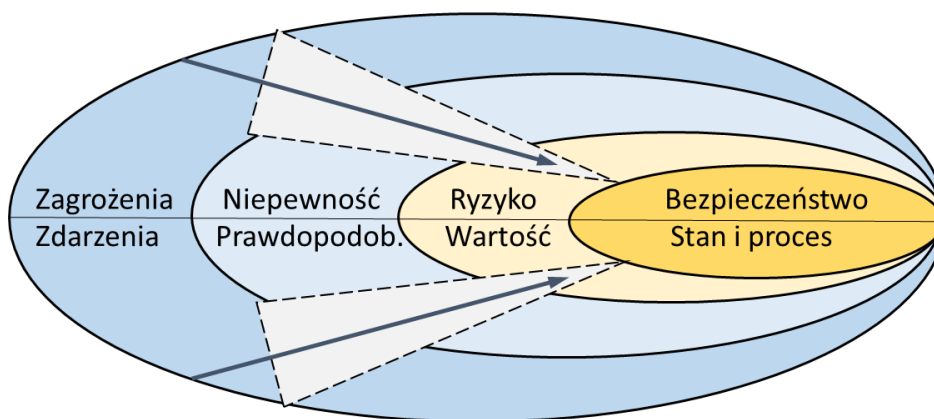
$B$  – bezpieczeństwo,  $Z$  – zagrożenia,  $Np$  – niepewność.

Wszechobecne zagrożenia mogą mieć charakter obiektywny lub subiektywny, systematyczny lub katastroficzny, prognozowany lub losowy, a ich skutki mogą być bardziej lub mniej szkodliwe i tragiczne. Zagrożeniom zawsze towarzyszy stochastyczna niepewność, która jako kategoria filozoficzna jest jakościowa i niewymierna. Prakseologiczna transformacja niepewności, to wymierne ryzyko, czyli statystyczna miara niepewności, losowości i pewnego rodzaju chaosu.

J. Wolanin (2005, s. 35) bezpieczeństwo definiuje jako: „(...) stan otoczenia cywilizacyjnego i naturalnego określonego przez poziom jego całkowitego ryzyka”. Tak rozumiane ryzyko służy więc do syntetycznego zobrazowania niepewności w postaci analitycznego wskaźnika, którym formalnie można zarządzać i celowo sterować w stronę zamierzonych wartości. Prakseologiczny ciąg przekształceń zagrożeń w stan bezpieczeństwa można przedstawić w następujący sposób:

$$Z \xrightarrow{\text{Losowość}} Np \xrightarrow{\text{Kategoryzacja}} R \xrightarrow{\text{Zarządzanie}} B \quad (3)$$

Dzięki wymiernej formule ryzyka ( $R$ ) jest możliwe świadome sterowanie i zarządzanie szerokim spektrum zagrożeń pod kątem zamierzonych standardów bezpieczeństwa. Ryzyko, które formalizuje kategorię niepewności umożliwia praktyczne zarządzanie bezpieczeństwem i kształtowanie go na pożądanym poziomie (rys.2).



Rys. 2. Przesłanki bezpieczeństwa łańcucha dostaw

Źródło: Opracowanie własne.

Ryzyko jest ilościową miarą niepewności, która jest naturalnym atrybutem wszelkiej działalności gospodarczej, polegającej formalnie na nieustannym podejmowaniu różnych decyzji biznesowych. Decyzje te z uwagi na niepełne i nieprecyzyjne informacje wejściowe

oraz niezwykle turbulentne, a środowisko ich wdrażania (konkurencja rynkowa) jest zawsze obdarzona pewnym pierwiastkiem błędu, przypadkowości i ograniczonej wiarygodności. Dopuszczalny margines tej niepewności nauka usiłuje zobrazować przy pomocy kategorii ryzyka, które jest miarą wymierną i deterministyczną.

Ryzyko formalnie można zdefiniować jako: „(...) iloczyn prawdopodobieństwa zajścia danego zdarzenia i skutków jego oddziaływania na procesy w organizacji” (Bizon-Górecka, 2007, s. 8). Jedną z wielu tzw. inżynierskich definicji ryzyka określa jako (POLRISK, 2010): „(...) cecha zdarzenia, zjawiska lub działania zdefiniowana kombinacją prawdopodobieństwa zdarzenia i jego skutków, które może wpłynąć pozytywnie lub negatywnie na osiągnięcie przez organizację jej nadrzędnych celów”. Wyraźnie negatywny wyraz ryzyka w działalności gospodarczej przypisuje J. Penc (2007, s. 388), kiedy twierdzi, że: „(...) ryzyko to prawdopodobieństwo poniesienia strat przez podmiot gospodarczy w następstwie podjęcia określonej decyzji”. Najbardziej popularna tzw. definicja obliczeniowa ryzyka ( $R$ ) występuje w następującej postaci:

$$R = p \times \$ \rightarrow \mathfrak{R}^+ \quad (4)$$

gdzie:

$R$  – ryzyko (obliczeniowe, inżynierskie),

$p \in [0,1]$  – prawdopodobieństwo wystąpienia zdarzenia,

$\$ \in (0, \infty)$  – prognozowane skutki tego zdarzenia,

$\mathfrak{R}^+$  – zbiór liczb rzeczywistych.

Prowadzenie rynkowej działalności gospodarczej jest obciążone różnymi rodzajami zagrożeń, mającymi charakter obiektywny, naturalny, przyrodniczy, a także subiektywny, społeczny, cywilizacyjny czy świadomy i celowy. Zagrożenia te implikują określone kategorie niepewności wyniku, czyli rozmaite ryzyka. Ryzyko, stanowiące stały czynnik każdej działalności gospodarczej w szczególnym stopniu ujawnia się w dynamice procesów logistycznych, cechujących się wysokim poziomem ekspozycji na różne zagrożenia (Brdulak, 2012). Naturalna dynamika procesów logistycznych realizowanych w wysoce zmiennych warunkach gospodarki rynkowej, pod nieustanną presją czynnika czasowego, na wysokim poziomie konkurencyjności przyczynia się do ciągłego powiększania katalogu zagrożeń i wzrostu poziomu ryzyka logistycznego (Ficoń, 2013).

Problematyka bezpieczeństwa łańcuchów dostaw ze względu na kluczowe znaczenie w gospodarce globalnej posiada bardzo bogatą teorię i praktykę i doczekała się wielu użytecznych aplikacji systemowych, takich jak, np. (Wieteska, 2011):

- system zarządzania ryzykiem w łańcuchu dostaw SCRM (*Supply Chain Risk Management*),
- system zarządzania bezpieczeństwem łańcucha dostaw SCSM (*Supply Chain Security Management*),
- system zarządzania ciągłością działania w łańcuchu dostaw BCMSC (*Business Continuity Management for Supply Chain*).

## 2. TYPOLOGIA PODSTAWOWYCH ZAGROŻEŃ

Ogólnoświatowy charakter globalnych łańcuchów dostaw oznacza ich światową rozległość przestrzenną, wymagającą pokonania wiele stref klimatycznych, granic państwowych, kultur administracyjnych i wiele specyficznych rynków biznesowych. Rozległość czasoprzestrzenna globalnego łańcucha dostaw generuje bardzo poważne problemy dla organów zarządzających jego funkcjonowaniem, odpowiedzialnych m.in. za bezpieczeństwo przepływów fizycznych i efektywność ekonomiczną realizowanej transakcji biznesowej (Konecka, 2011). Bardzo duży wpływ na skalę i zasięg rozmaitych zagrożeń ma wielkość, struktura i styl zarządzania łańcuchem dostaw. Porządkując podatność łańcuchów dostaw na zagrożenia można stwierdzić, że najmniejszą wrażliwością odznaczają się krótkie i zwarte łańcuchy lokalne (wewnętrzne), w których czas reakcji organów zarządzających jest natychmiastowy a wynik tych działań skuteczny (Rutkowski, 1999). Im dłuższy i bardziej rozbudowany jest łańcuch dostaw, tym większe jest spektrum potencjalnych zagrożeń, a ich skutki mogą być odpowiednio bardziej groźne. Łańcuchy zewnętrzne w miarę powiększania się ich wielkości (liczby podmiotów), skali realizowanych transakcji i zasięgu przestrzennego stają się coraz bardziej podatne na oddziaływanie różnych kategorii zagrożeń. Przykładowo możemy zbudować pewien typoszereg podatności łańcuchów dostaw (*LD*) na potencjalne zagrożenia obejmujący rosnąco:

$$LD = \langle LW \rangle LB \rangle LR \rangle LM \rangle LG \rangle \cap LV \quad (5)$$

gdzie:

*LW* – łańcuchy i wewnętrzne (lokalne),

*LB* – łańcuchy branżowe i korporacyjne,

- LR* – łańcuchy regionalne i krajowe,
- LM* – łańcuchy międzynarodowe i kontynentalne,
- LG* – łańcuchy globalne i światowe,
- LV* – łańcuchy wirtualne.

Według G. Wieteska (2011, s. 115) źródłem ryzyka płynącego z otoczenia dla łańcuchów dostaw jest:

- otoczenie makroekonomiczne, związane z sytuacją gospodarczą, polityczną, zjawiskami przyrodniczymi, stanem prawnym,
- otoczenie mikroekonomiczne, obejmujące sytuację gospodarczą w sektorze i przedsiębiorstwie, współpracę z dostawcami i odbiorcami, poziom konkurencji rynkowej,
- koniunkturalny popyt rynkowy wynikający z różnych czynników zewnętrznych i wewnętrznych, tylko w niewielkim stopniu podlegający prognozowaniu.

Natomiast *World Economic Forum* (2011) bezpieczeństwo globalnych łańcuchów dostaw lokuje w pięciu obszarach obejmujących: środowisko ekonomiczne, geopolityczne, przyrodnicze, społeczne i technologiczne. Jednocześnie jako najpoważniejsze zagrożenia gospodarcze dla firm pochodzące z otoczenia w roku 2010 zostały uznane: zmiany klimatyczne, katastrofy naturalne, kryzysy finansowe, ekstremalne wahania cen energii oraz dysproporcje społeczno-gospodarcze krajów i społeczeństw.

Dla dalszych analiz ogół czynników rzutujących na bezpieczeństwo i efektywność globalnych łańcuchów dostaw ( $SB_{LD}$ ) zostanie podzielonych na 4 zasadnicze kategorie dotyczące szerokich uwarunkowań środowiskowych:

$$SB_{LD} = \{S_N, S_P, S_G, S_O\} \quad (6)$$

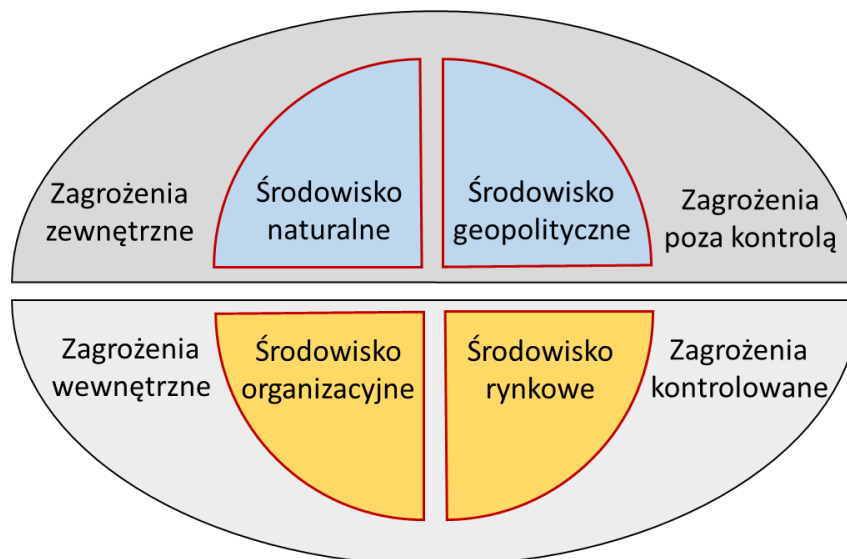
gdzie:

- $S_N$  – środowisko naturalne, warunki przyrodnicze i klimatyczne,
- $S_P$  – środowisko geopolityczne, stosunki międzynarodowe i społeczne,
- $S_G$  – środowisko globalne i relacje biznesowe,
- $S_O$  – środowisko organizacyjne (wewnątrzorganizacyjne).

Udział poszczególnych kategorii środowiskowych w kształtowaniu poziomu zagrożeń, a tym samym bezpieczeństwa łańcuchów dostaw jest wielce zróżnicowany i zależy od



specyfiki i charakteru danego łańcucha, konwencji jego umowy handlowej i ogólnie podatności na oddziaływania zagrożeń środowiskowych (Konecka, Stajniak, Szopik-Depczyńska, 2016). W trakcie tej specyfikacji celowo operujemy szerokim pojęciem środowiska, aby ograniczyć udział czynników okazjonalnych i przypadkowych (rys. 3).



Rys. 3. Środowiskowe obszary zagrożeń bezpieczeństwa globalnych łańcuchów dostaw  
Źródło: Opracowanie własne.

Biorąc pod uwagę misję i cele łańcuchów dostaw centralnym i pierwszoplanowym środowiskiem jest środowisko rynkowe, dla potrzeb którego został sformułowany dany łańcuch. Najważniejszym elementem bezpieczeństwa środowiskowego jest biznesowe środowisko rynkowe, będące naturalną platformą realizacji przepływów fizycznych i prowadzenia wszelkich transakcji handlowych (Huczek, 2015). W tym środowisku realizowane są wszystkie koncepcje strategiczne i bieżące procesy operacyjne warunkujące funkcjonowanie łańcuchów dostaw, niezależnie od ich rodzaju, zasięgu i wykonywanych zadań. W środowisku rynkowym przebiegają wszystkie działania biznesowe i procesy logistyczne stanowiące cel i istotę łańcuchów dostaw (Szymonik, 2010). Jakiegokolwiek wyeliminowanie środowiska rynkowego oznacza zanik danego łańcucha dostaw i jego upadłość.

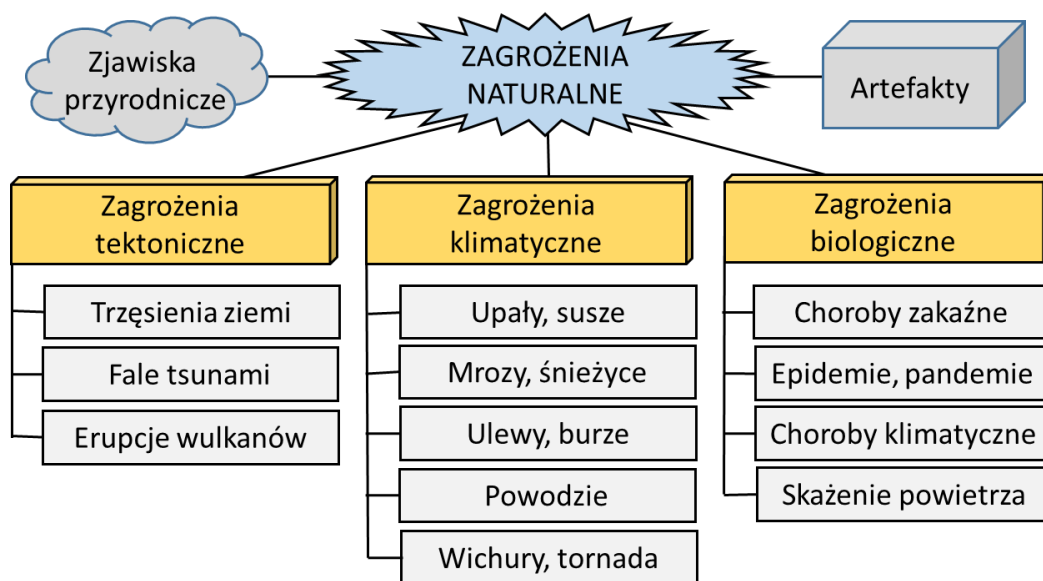
Ze środowiskiem rynkowym jest bezpośrednio związane środowisko menedżerskie reprezentujące organa kierownicze i zarządzające danym łańcuchem dostaw. W tym środowisku podejmowane są wszystkie decyzje rzutujące na istnienie, funkcjonowanie i standardy danego łańcucha. Inaczej można powiedzieć, że środowisko rynkowe i menedżerskie są warunkiem koniecznym funkcjonowania każdego łańcucha dostaw,

natomiast środowisko naturalne, polityczne i infrastrukturalne to warunki dostateczne, które stanowią o jakości i sprawności działania łańcucha dostaw.

### 3. ZAGROŻENIA W OBSZARZE ŚRODOWISKA NATURALNEGO

Środowisko naturalne obrazuje siły przyrody, które pomimo olbrzymiego postępu naukowo-technicznego skrywa ciągle wiele tajemnic i nie do końca przewidywalnych reakcji. Tylko niektóre zachowania przyrody możemy z pewnym prawdopodobieństwem prognozować i przewidywać ich skutki. Gwałtowność i nieprzewidywalność zjawisk przyrodniczych stanowi poważną kategorię ryzyka należącego do klasy ryzyka obiektywnego, niestety często katastroficznego. Głównymi zagrożeniami przyrodniczymi o różnej częstotliwości i intensywności działania mających wpływ na bezpieczeństwo praktycznie wszystkich rodzajów łańcuchów dostaw są: zagrożenia tektoniczne, klimatyczne i biologiczne (Ficoń, 2007). Najbardziej powszechne zagrożenia tektoniczne to: trzęsienia ziemi, erupcje wulkanów, fale tsunami oddziałujące głównie na elementy infrastruktury krytycznej państwa i logistycznej w ogólności. Mniej groźne w swoich skutkach są zagrożenia klimatyczne, takie jak: powodzie głównie obszarowe, lawiny błotne, susze, upały, zapy śnieżne i oblodzenia, a także tornada, huragany i burze atmosferyczne. Mniej powszechne, ale szczególnie niebezpieczne dla ludzi są zagrożenia biologiczne takie, jak: choroby zakaźne, epidemie i pandemie, choroby klimatyczne oraz skażenie wody i żywności (rys. 4).

Zagrożenia ze strony środowiska przyrodniczego należą do kategorii zagrożeń systematycznych, z którymi człowiek zmaga się od początku swoich dziejów. Spektakularne klęski żywiołowe i kataklizmy nie należą do rzadkości, a ich skutki dla integralności i sprawności globalnych łańcuchów dostaw są znane powszechnie i w jakimś stopniu kalkulowane w ryzyko podróży (transakcji). Ryzyko zdarzeń przyrodniczych jest ryzykiem obiektywnym i systematycznym, z którym najbardziej skutecznie walczy się na drodze transferu tego ryzyka na podmioty trzecie, czyli na towarzystwa ubezpieczeniowe. Oprócz trudnych dla światowych przepływów towarowych przypadków unikania przedsięwzięć (tras, regionów, pór roku) wysoce ryzykownych polisa ubezpieczeniowa jest podstawowym sposobem zwiększania bezpieczeństwa globalnych łańcuchów dostaw kosztem odpowiedniej składki ubezpieczeniowej. Relatywny rachunek ekonomiczny obejmujący realne koszty ubezpieczeń i hipotetyczne straty jest główną strategią defensywną liderów globalnych łańcuchów dostaw.



Rys. 4. Zagrożenia naturalne bezpieczeństwa globalnych łańcucha dostaw

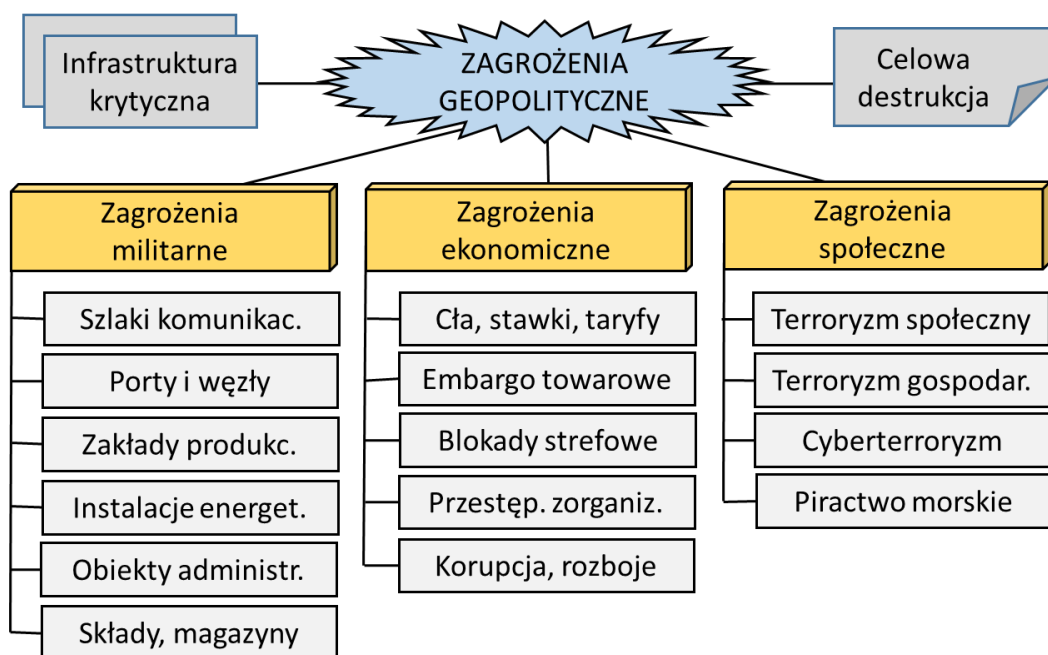
Źródło: Opracowanie własne.

Środowisko naturalne generuje obiektywne, zewnętrzne spektra zagrożeń, które w niewielkim stopniu mogą być antycypowane przez menedżerów biznesowych, a podatność globalnych łańcuchów dostaw na szlakach światowych na ich skutki jest stosunkowo duża (Jażdżewska-Gutta 2013). Systematyczne analizowanie różnego rodzaju – nie zawsze wiarygodnych prognoz i odpowiednie postępowanie ze stwierdzonym ryzykiem jest jedną z bardziej skutecznych metod minimalizowania niebezpieczeństwa pochodzącego ze strony sił natury.

#### 4. ZAGROŻENIA ZE STRONY ŚRODOWISKA GEOPOLITYCZNEGO

Zagrożenia generowane przez szeroko rozumiane środowisko geopolityczne szacowane są za pomocą ryzyka będącego następstwem celowej działalności człowieka (sił zbrojnych, organizacji przestępczych, grup społecznych, grup etnicznych, organów państwowych) i innych struktur i organizacji nieformalnych. Środowisko geopolityczne może generować trzy zasadnicze kategorie zagrożeń o charakterze stricte politycznym czy policyjnym, oraz zagrożenia natury ekonomicznej i społecznej. Najczęściej zagrożenia geopolityczne przybierają formę konfliktów o charakterze militarnym, ekonomicznym lub etnicznym, które zakłócają lub przerywają czasowo lub na stałe ciągłość łańcuchów dostaw (Kaczmarek, Ćwiek 2009). Działania militarne z reguły skierowane są na niszczenie lub wyłączenie z użytkowania elementów tzw. infrastruktury krytycznej rejonu objętego walką, takich jak: porty lotnicze i morskie, węzły kolejowe i drogowe, drogi i szlaki komunikacyjne,

mosty i wiadukty, instalacje energetyczne i paliwowe, zakłady produkcyjne, składy i obiekty magazynowe. W toku intensywnych działań wojennych niszczone są także obiekty i centra administracji publicznej, centra logistyczne i inne obiekty mające wpływ na obronność danego rejonu (kraju). Podczas działań wojennych paraliżowany jest w maksymalny sposób wszelki transport, komunikacja i łączność, systemy produkcyjne i systemy dystrybucyjne. Zagrożenia związane z konfliktami militarnymi obejmują różnego rodzaju restrykcje, embarga, blokady i ograniczenia w zakresie swobodnego przepływu towarów, co bezpośrednio godzi w ciągłość działania łańcuchów dostaw (Kaczmarek, Ćwiek 2009). Ogromne niebezpieczeństwo dla działalności logistycznej rodzi zanik organów władzy publicznej i struktur państwowych i standardów praworządności. Ich miejsce zajmuje zorganizowana przestępczość i związana z nią szczególnie groźna dla działalności gospodarczej korupcja, wymuszenia i różnego rodzaju rozboje (rys. 5).



Rys. 5. Zagrożenia geopolityczne bezpieczeństwa globalnych łańcucha dostaw

Źródło: Opracowanie własne.

Ogromne wyzwania dla działalności biznesowej i logistycznej generuje terroryzm i piractwo, głównie morskie. O ile konflikty zbrojne w skali lokalnej i piractwo morskie są w pewnym sensie lokalizowane przestrzennie i przewidywalne, i mogą być częściowo w różny sposób antycypowane, o tyle terroryzm ma wymiar globalny i jest praktycznie nieprzewidywalny. Irracjonalne ataki terrorystyczne w zależności od jego formy mogą być skierowane na różne obiekty, instytucje, a także pojedyncze osoby – często jako ślepe cele,

bez żadnego kryterium wyboru. Zupełnie odmienną kategorię zagrożeń generuje współczesna cywilizacja i technologie społeczeństwa informacyjnego (Ciesielski, 2011). Powszechność tych technologii zrodziła spektakularne zagrożenia pochodzące ze sfery tzw. cyberprzestrzeni, jako popularne cyberataki, skierowane na wszelkie zasoby i media informacyjne. Cyberataki mogą bardzo skutecznie zakłócać ciągłość i harmonię przepływów fizycznych na wszystkich etapach łańcucha dostaw (Kaczmarek, Ćwiek 2009). Reasumując należy zaważyć, że ekspozycja globalnych łańcuchów dostaw na środowisko geopolityczne jest szczególnie duża i dość często zagraża ich integralności i ekonomicznej efektywności (Tarasiewicz, 2014). Praktycznie nie ma możliwości aktywnego zwalczania tych zagrożeń, wobec tego pozostaje strategia unikania niebezpiecznych obszarów i silnego ubezpieczania prowadzonej w tych rejonach transakcji.

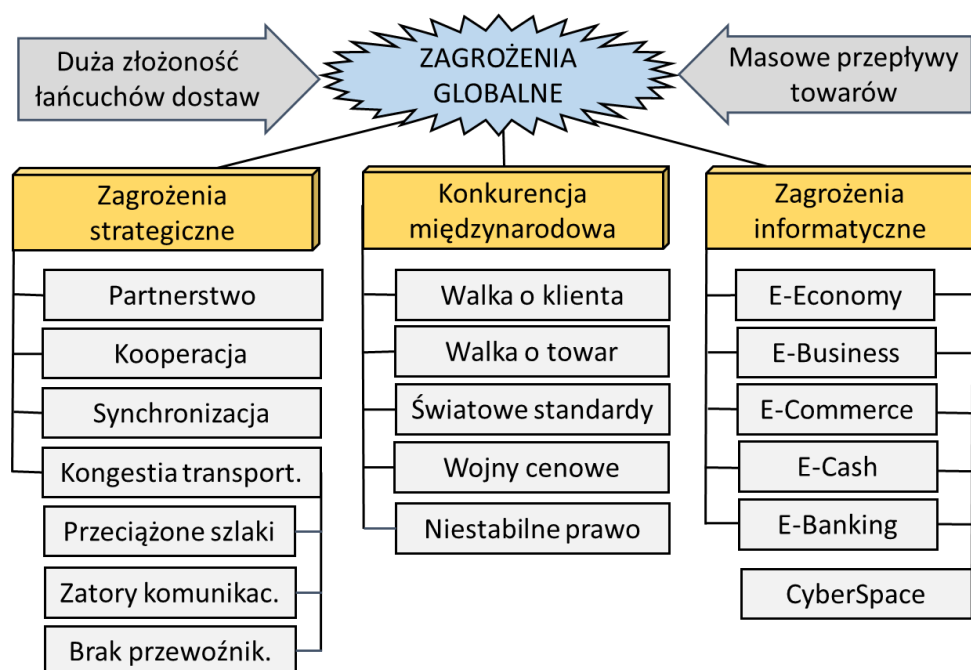
## 5. ZAGROŻENIA Z KIERUNKU ŚRODOWISKA GLOBALNEGO

Globalne otoczenie rynkowe to naturalna platforma realizacji działalności gospodarczej, w tym także procesów logistycznych. W warunkach globalizacji gospodarki łańcuchy dostaw stają się niezwykle rozbudowane i skomplikowane. Komplikuja się relacje biznesowe między partnerami, wydłużają się drogi transportowe oraz wolumen i ilość przewożonych towarów. Spełnienie warunku partnerstwa wywołuje konieczność pokonania granic państwowych, różnych barier politycznych, administracyjnych oraz prawnych, a także działania w zmiennych warunkach klimatycznych i cywilizacyjnych. Globalizacja oprócz silnego wpływu na koncepcje strategiczne biznesu i warunki działań operacyjnych – stała się jednym z głównych źródeł zagrożeń i pochodnych czynników ryzyka. Ryzyko jakie powstaje w tym obszarze ma charakter systematyczny i pozostaje tylko w niewielkiej części w dyspozycji zainteresowanych podmiotów gospodarczych (Jażdżewska-Gutta, 2013).

Dla efektywności globalnego łańcucha dostaw kluczowe znaczenie ma sprawne zarządzanie i kooperacja z podmiotami zewnętrznymi warunkująca realizację wielu funkcji biznesowych często na różnych kontynentach, np. za pośrednictwem specjalnych agentów. W procesie koordynacji wszystkich interesariuszy łańcucha dostaw podstawową rolę odgrywa skuteczność zarządzania, czyli kompetencje i profesjonalizm kadr menedżerskich, które odpowiadają za bieżące zarządzanie operacyjne w skali całego łańcucha. Kadry menedżerskie muszą posiadać aktualną wiedzę rynkową, np. o wielkości stawek i taryf transportowych, o obciążeniu poszczególnych przewoźników, a także o wysokości stóp procentowych, aktualnych kursach walut. W tym temacie bardzo groźne są zjawiska kongestii na szlakach komunikacyjnych i w punktach modalnych sieci transportowej, które mogą wynikać m.in.

z przyczyn systematycznych takich, jak sezonowe przeciążenie szlaków drogowych, świąteczne przerwy i wyłączenia z działalności biznesowej. Sytuacje te mogą generować różne zatory transportowe i opóźnienia, skutkujące dodatkowymi kosztami.

Dominującą rolą technologii komputerowych we współczesnych systemach zarządzania (gospodarowania) sprawia, że oprócz ewidentnych zalet i korzyści niesie ona także szereg zagrożeń również na wysokich szczeblach zarządzania strategicznego. Pierwzoplanowe znaczenie informacji w sterowaniu wieloczołowym, rozległym łańcuchem dostaw wymaga wielkiej sprawności wszelkich procedur informacyjno-decyzyjnych kierujących całym łańcuchem dostaw. Funkcjonują one na zasadzie sprzężenia zwrotnego – dziś z udziałem kanałów internetowych, podatnych niestety na rozmaite zakłócenia losowe i przypadkowe. Dzięki interaktywnej, internetowej komunikacji ze wszystkimi ogniwami łańcucha dostaw równoważone są rynkowe strumienie podaży i popytu, co skutkuje minimalizacją zapasów i ograniczeniem wszelkiego marnotrawstwa. Nowoczesne aplikacje teleinformatyczne, z jednej strony, pozwoliły na pełną synchronizację procesów logistycznych w całym łańcuchu dostaw, z drugiej, uzależniły te łańcuchy od sprawności i niezawodności sektora IT (*Information Technology*), coraz bardziej narażonego na cyberataki. Współczesna globalizacja wyrosła dzięki nowoczesnej technologii komputerowej, a kluczowymi jej technologiami są obecnie: e-Economy, e-Business, e-Commerce, e-Cash, e-Banking i wiele innych (Ciesielski, 2011). Dla potrzeb obsługi gospodarki globalnej powstała nowa gałąź inżynierii finansowej i potężny światowy sektor bankowy.



Rys. 6. Zagrożenia globalne bezpieczeństwa globalnych łańcuchów dostaw

Źródło: Opracowanie własne.

Analizując otoczenie rynkowe należy zwrócić szczególną uwagę na poziom konkurencji rynkowej i standardy obsługi klienta reprezentowane przez lokalne podmioty (Jażdżewska-Gutta, 2013). Silna konkurencja rynkowa oznacza ekonomiczną walkę o każdego klienta i każdy towar, który może trafić na dany rynek, co stanowi duże wyzwanie dla pojawiających się obcych przepływów fizycznych, także w strukturze globalnych łańcuchów dostaw. Konkurencja rynkowa to również szansa na pozyskanie bardziej korzystnych ofert ze strony miejscowych kontrahentów, umożliwiającą korzystne zrealizowanie określonej transakcji handlowej. Wdać tu dualność kategorii ryzyka – zagrożenie i szansa, którą menedżerowie ryzyka powinni racjonalnie wykorzystać.

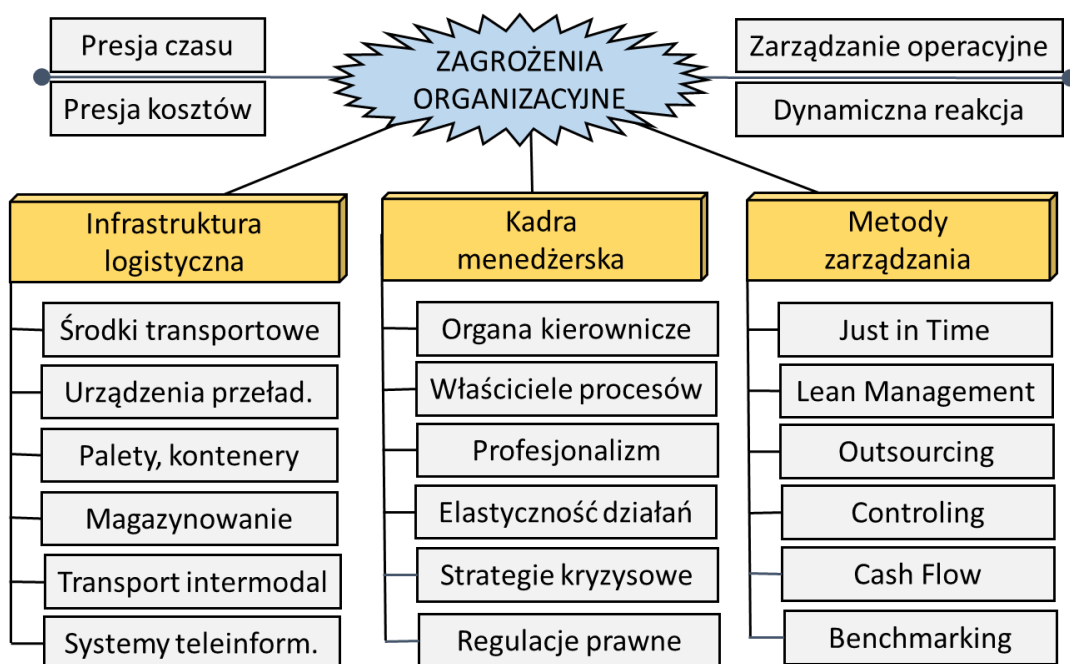
## **6. ZAGROŻENIA Z OBSZARU ŚRODOWISKA ORGANIZACYJNEGO**

Środowisko organizacyjne reprezentuje najbliższe otoczenie biznesowe łańcucha dostaw, który musi być sprawnie i efektywnie zarządzany w sposób zcentralizowany, według nowoczesnych standardów zarządzania menedżerskiego (Tarasiewicz, 2014). W tym obszarze najważniejsze są efektywne systemy zarządzania i odpowiednio szybka i skuteczna reakcja na pojawiające się z różnych kierunków i środowisk zagrożenia. Powstające tam ryzyko zaliczane jest do kategorii ryzyka operacyjnego, ściśle związanego z realizowanymi procesami gospodarczymi. Najczęściej jest efektem nietrafionych decyzji menedżerskich i mało skutecznych strategii przeciwdziałania pojawiającym się zagrożeniom wewnętrznym i rynkowym (Ficoń, 2015).

Głównymi domenami tego środowiska są organa menedżerskie pełniące funkcje kontrolno-sterujące, właściciele poszczególnych podmiotów gospodarczych lub procesów biznesowych, dostępna infrastruktura techniczna, głównie transportowo-magazynowa oraz rozmaite podmioty i procesy pomocnicze. Szczególną rolę pełni nieodzowna w XXI wieku technologia teleinformatyczna będąca podstawą procesów informacyjno-decyzyjnych (Ciesielski, 2011).

W zależności od konfiguracji i wielkości łańcucha dostaw w jego strukturze może, choć nie musi być wyróżniony lider pełniący funkcje kierownicze, odpowiedzialny za sprawność, niezawodność i skuteczność realizowanych transakcji handlowych. Oprócz wytyczania linii strategicznej łańcucha dostaw zobowiązany jest on do zagwarantowania pełnego bezpieczeństwa operacyjnego wszystkim procesom gwarantującym zrealizowanie przyjętego zlecenia zgodnie z odpowiednią umową handlową. Lider realizuje w sposób ciągły procedury zarządzania operacyjnego obsługiwanego łańcucha dostaw posługując się nowoczesnymi metodami menedżerskimi. W tym celu powszechnie stosuje się dziś takie

metody i procedury jak: *Just in Time*, *Lean Management*, *Outsourcing*, *Benchmarking*, *Controlling*, *Cash Flow* i inne. Na szczególną uwagę zasługuje *Outsourcing* wspierający koncepcję *Lean Management*, który polega na zleceniu procesów drugorzędnych i pomocniczych zewnętrznym podwykonawcom. Powoduje to dodatkowe rozczłonkowanie łańcucha dostaw i konieczność dodatkowej koordynacji tych podmiotów (rys. 7).



Rys. 7. Zagrożenia organizacyjne bezpieczeństwa globalnych łańcuchów dostaw

Źródło: Opracowanie własne.

Zagrożenia generowane przez wewnętrzne środowisko organizacyjne w dużej części wynikają z uwarunkowań techniczno-technologicznych jakimi dysponuje szeroko rozumiana infrastruktura. Sprawne funkcjonowanie łańcuchów dostaw wymaga posługiwania się bardzo różnymi urządzeniami technicznymi, takimi jak środki transportowe, systemy magazynowe, urządzenia przeładunkowe, systemy opakowaniowe i inne. Operowanie skomplikowanymi i ciężkimi systemami technicznymi powoduje powstanie różnych awarii i zdarzeń nadzwyczajnych, niosących ryzyko dla procesów technologicznych, a także dla ludzi obsługujących te urządzenia. Ogromną rolę w przepływach fizycznych odgrywają dziś opakowania, głównie zbiorcze typu palety i kontenery, którym ruch w łańcuchu dostaw jest automatycznie monitorowany. Opakowania jednostkowe generują wielkie problemy związane z odpadami i tzw. ekologią. Konieczność zachowania wymaganych prawem standardów ekologicznych znacząco rzutuje na wielkość kosztów związanych z przepływami fizycznymi, które muszą być bilansowane w skali superorganizacji zarządzającej łańcuchem dostaw.



Szczególnym elementem infrastruktury logistycznej jest technologia informatyczna, której użytkowanie może powodować rozmaite zagrożenia, głównie w sferze informacyjnej, takie jak: nielegalny dostęp do informacji, celowa lub przypadkowa dezinformacja, awarie nośników i systemów informatycznych, ataki hakerów na zasoby informacyjne itp.

W sferze zagrożeń wewnątrzorganizacyjnych funkcjonuje ciągła presja czasu i kosztów, wynikająca z wielkiej dynamiki łańcuchów dostaw (Rutkowski, 1999). Wiąże się ona ze stylem zarządzania i profesjonalnym zachowaniem się menedżerów w krytycznych sytuacjach decyzyjnych. Bardzo ważnym elementem bezpieczeństwa wewnętrznego są kompetencje i profesjonalizm oraz stabilność kadry kierowniczej i lojalność wszystkich pracowników na różnych szczeblach hierarchii zawodowej.

Należy podkreślić, że ryzyko wewnętrzne łańcucha dostaw musi być postrzegane i skorelowane w szerokiej perspektywie z ryzykiem gospodarczym każdego podmiotu uczestniczącego w danym łańcuchu, a nawet z ryzykiem macierzystej branży, jeśli są to łańcuchy branżowe. Minimalizacja ryzyka wewnętrznego łańcucha dostaw nie może być przeprowadzona bez kontrolowania ryzyka gospodarczego całej organizacji zarządzającej tym łańcuchem (Ficoń, 2013). Wskazane jest także, aby wszystkie podmioty uczestniczące w strukturze łańcucha dostaw kontrolowały według zbliżonej metodyki indywidualnie swoje ryzyka wewnętrzne i wzajemnie informowały się o poziomie tego ryzyka, celem wypracowania ogólnej strategii zarządzania ryzykiem wewnętrznym w całej superorganizacji.

Ryzyka powstające w środowisku organizacyjnym są stosunkowo podatne na różne strategie zarządzania, także stwierdzonym ryzykiem. Poprzez odpowiednie decyzje menedżerskie możemy bezpośrednio wpływać zarówno na przyczyny różnych zagrożeń, jak też na ich skutki (Ficoń, 2015). Zgodnie ze strategią zarządzania ryzykiem redukowanie ryzyka zaczyna się od źródła, czyli minimalizacji prawdopodobieństwa wystąpienia zdarzenia krytycznego, gdyż skutki są efektem wtórnym zaistniałego zdarzenia.

## **PODSUMOWANIE I WNIOSKI KOŃCOWE**

Globalne łańcuchy dostaw są w sposób naturalny narażone na szerokie spektrum rozmaitych zagrożeń, generujących określone ryzyka i niebezpieczeństwa, których dynamika jest ogromna. Wynika to z faktu globalnego zakresu funkcjonowania współczesnych łańcuchów dostaw, ich światowej rozległości przestrzenno-czasowej oraz wielkiej intensywności przepływów fizycznych we współczesnym świecie. Zagrożenia te są skierowane głównie na zakłócanie, a niekiedy na dezintegrację przepływów fizycznych, będącą skutkiem dezinformacji i różnych tendencyjnych oddziaływań na strumienie

informacje, godzącą de facto w skuteczność i sprawność zarządzania (Huczek, 2015). W efekcie końcowym zagrożenia środowiskowe powodują zwiększenie kosztów operacyjnych, a tym samym zmniejszenie ekonomicznej efektywności globalnych łańcuchów dostaw. Rozwijająca się globalizacja będzie potęgować te tendencje i dlatego należy precyzyjnie badać te trendy, aby możliwie skutecznie można byłoby im się przeciwstawić.

Wyniki badań diagnostycznych tych problemów zostały zaprezentowane w powyżej pracy, której głównym celem była specyfikacja i ogólna charakterystyka szerokiego spektrum zagrożeń, jakie generują dla bezpieczeństwa globalnych łańcuchów dostaw cztery skategoryzowane środowiska bezpieczeństwa – środowisko przyrodnicze, geopolityczne, rynkowe i organizacyjne. Kompleksowo postrzegane multiśrodowisko oddziałuje w sposób przypadkowy lub celowy przede wszystkim na trzy kluczowe strumienie – przepływy fizyczne, informacyjne i finansowe powodując tym samym destrukcję globalnego łańcucha dostaw i zaniżanie jego bezpieczeństwa.

Dwa pierwsze środowiska – przyrodnicze i geopolityczne implikują dla bezpieczeństwa globalnych łańcuchów dostaw zagrożenia obiektywne, których zaistnieniu trudno jest się przeciwstawić, a można jedynie zwalczać ich ewentualne skutki i następstwa. Skuteczne zarządzanie bezpieczeństwem globalnych łańcuchów dostaw w tym przypadku jest dość ograniczone i ma charakter wybitnie defensywny. Tylko w szczególnych przypadkach zagrożenia ze strony przyrody i szerokiej geopolityki można antycypować i profilaktycznie zwalczać. Pozostałe dwa rodzaje środowisk – globalne i organizacyjne generują zagrożenia o charakterze subiektywnym, mniej lub bardziej celowe, które są relatywnie prognozowane i podatne na skuteczne zwalczanie poprzez racjonalne zarządzanie np. antykrzysowe. W ogólności można powiedzieć, że zagrożenia te są wynikiem świadomej lub nieświadomej działalności człowieka i jego artefaktów. Pierwszoplanową rolę odgrywa w tym przypadku celowo zorganizowany system zarządzania, czyli kierownictwo i menedżerowie szczebla operacyjnego odpowiedzialni m.in. za bezpieczeństwo łańcuchów dostaw rozpatrywanych w różnej skali.

Skuteczne zarządzanie globalnym łańcuchem dostaw wymaga zbudowania komplementarnego systemu bezpieczeństwa obejmującego, z jednej strony, wszystkie środowiska będące źródłem potencjalnych zagrożeń, z drugiej, wszystkie podmioty uczestniczące w strukturze organizacyjno-funkcjonalnej tego łańcucha, ponoszące skutki tych zagrożeń. W tym kontekście ważne jest zachowanie wysokiego bezpieczeństwa na poziomie nawet najmniejszych ogniw globalnego łańcucha dostaw biorących udział w międzynarodowej wymianie towarowej.

Reasumując, można sformułować generalny wniosek, że problematyka bezpieczeństwa globalnych łańcuchów dostaw jest w dużym stopniu podatna na skuteczne zarządzanie ze strony kierownictwa strategicznego (lidera) danego łańcucha. Sama kwestia kierownictwa – przywództwa i lidera globalnego łańcucha dostaw jest zagadnieniem dość złożonym i nie zawsze jednoznacznym. Z drugiej strony, profesjonalne zarządzanie globalnym łańcuchem dostaw wymaga wysokich kompetencji menedżerskich, aktualnej wiedzy biznesowej i doskonałej znajomości światowej branży TSL – transport, spedycja, logistyka (Ciesielski, 2011). Dlatego bezpieczeństwo globalnych łańcuchów dostaw musi być rozpatrywane jako wielokryterialny problem decyzyjny, obejmujący jednocześnie konceptualny szczebel strategiczny i wykonawczy szczebel operacyjny. Prakseologicznym elementem tej procedury jest analiza i ocena ryzyka, dająca wymierne kryteria walidacji różnych zdarzeń krytycznych i sytuacji kryzysowych, co pozwala na wypracowanie bezpiecznego scenariusza zarządzania globalnym łańcuchem dostaw w konkretnych uwarunkowaniach multiśrodowiskowych.

## LITERATURA

1. Bizon-Górecka J. (red.) (2007). *Strategie zarządzania ryzykiem w przedsiębiorstwie – zarządzanie ryzykiem projektu*, Wyd. TNOiK: Bydgoszcz.
2. Brdulak H. (2012). *Logistyka przyszłości*. PWE: Warszawa.
3. Brdulak, H., (2001). *Zarządzanie ryzykiem a zarządzanie wiedzą w sieciach dostaw*. *Gospodarka Materiałowa i Logistyka*, nr 11/2001.
4. Christopher M. (1998), *Logistics and supply chain management. Strategies for reducing costs and improving service*. Financial Times Management London.
5. Ciesielski M. (red.) (2011). *Zarządzanie łańcuchami dostaw*. PWE: Warszawa.
6. Fertsch M. (red.) (2016). *Słownik terminologii logistycznej*. ILiM: Poznań.
7. Ficoń K. (2007). *Inżynieria zarządzania kryzysowego. Podejście systemowe*. BEL Studio: Warszawa.
8. Ficoń K. (2013). *Źródła i kategorie ryzyka logistycznego występujące w strukturze logistycznych łańcuchów dostaw*. ZN WSAiB nr 20/2013.
9. Ficoń K. (2015). *Dobre praktyki zarządzania przedsiębiorstwem w sytuacjach kryzysowych*. *Przedsiębiorstwo w Otoczeniu Globalnym*. UG ITiHM Gdańsk.
10. *Global Risk 2011*. World Economic Forum Report. January 2011.
11. <http://polrisk.pl/polrisk/zarzadzanie-ryzykiem/sloownik> (dostęp: 10.11.2017)

12. Huczek M. (2015). *Bezpieczeństwo łańcucha dostaw*. ZN WSH Zarządzanie 4/2015.
13. Jażdżewska-Gutta M. (2013). *Globalny i lokalny wymiar bezpieczeństwa w łańcuchu dostaw z perspektywy polskich przedsiębiorstw* ZN UG: Gdańsk.
14. Kaczmarek T. T., Ćwiek G. (2009), *Ryzyko kryzysu a ciągłość działania*. Difin: Warszawa.
15. Konecka S., Stajniak M., Szopik-Depczyńska K. (2016). *Bezpieczeństwo łańcucha dostaw*. Autobusy 11/2016.
16. Konecka, S. (2011). *Typologia łańcuchów dostaw*, Logistyka, nr 5.
17. Penc J. (1997), *Leksykon biznesu*, Agencja wyd. Placet: Warszawa.
18. Pszczołowski T. (1978). *Mała encyklopedia prakseologii i teorii organizacji*. Wyd. Narodowe Ossolineum: Wrocław-Warszawa-Kraków-Gdańsk.
19. Rutkowski, K. (red.), (2000). *Zintegrowany łańcuch dostaw. Doświadczenia globalne i polskie*. Wyd. SGH: Warszawa.
20. *Słownik pojęć ekonomicznych*. (2007). Tom 9. Ser. Biznes WN PWN: Warszawa.
21. Szymonik A. (2010). *Logistyka i zarządzanie łańcuchem dostaw*. Difin: Warszawa.
22. Tarasiewicz R. (2014). *Jak mierzyć efektywność łańcuchów dostaw*. Oficyna wyd. SGH: Warszawa.
23. Wieteska G. (2011). *Zarządzanie ryzykiem w łańcuchu dostaw na rynku B2B*. Difin: Warszawa.
24. Witkowski J. (2003). *Zarządzanie łańcuchem dostaw*. PWE: Warszawa.
25. Wolanin J. (2005). *Zarys teorii bezpieczeństwa obywateli*. DANMAR: Warszawa.