



Magdalena Jazdzewska-Gutta

Uniwersytet Gdański
Wydział Ekonomiczny
Instytut Handlu Zagranicznego
ekomjg@ug.edu.pl

ZMIANY W OBSZARZE BEZPIECZEŃSTWA ŁAŃCUCHA DOSTAW W LATACH 2001-2016

Streszczenie: Celem opracowania jest przedstawienie zmian w zakresie bezpieczeństwa w latach 2001-2016, ze szczególnym uwzględnieniem nowych wyzwań pochodzących z otoczenia łańcuchów dostaw, takich jak wzrost zagrożenia terrorystycznego czy kryzys migracyjny, które miały znaczny wpływ na państwa europejskie, a tym samym również na działające w nich przedsiębiorstwa. Analiza opiera się na danych statystycznych pochodzących z międzynarodowych baz danych oraz raportów organizacji międzynarodowych, dotyczących wybranych zagrożeń wobec łańcuchów dostaw, a także na wynikach badań ankietowych na temat bezpieczeństwa przeprowadzonych techniką wspomaganą komputerowo wywiadów telefonicznych wśród polskich eksporterów oraz importerów w 2013 i 2016 roku. Dzięki porównaniu danych i wyników badań z różnych okresów możliwe jest wykazanie dynamicznego charakteru bezpieczeństwa.

Słowa kluczowe: bezpieczeństwo łańcucha dostaw, terroryzm, piractwo, bezpieczeństwo transportu, zagrożenia.

JEL Classification: F50, L20, R49.

Wprowadzenie

Badania nad bezpieczeństwem łańcucha dostaw są prowadzone od 2001 roku. Bódcem do rozwoju tej tematyki były ataki terrorystyczne w Nowym Jorku oraz późniejsze w Londynie czy Madrycie. W otoczeniu prawnym zainteresowanie bezpieczeństwem łańcucha dostaw zaowocowało stworzeniem wielu regulacji mających na celu zabezpieczenie transportu oraz działań w zakresie kompetencji służb celnych. W kolejnych latach miały miejsce pojedyncze wyda-

rzenia związane z działalnością terrorystyczną, a pod koniec pierwszej dekady XXI w. nasilił się problem piractwa morskiego. Jednakże kolejne lata względniego spokoju mogły uspić czujność przedsiębiorców. W latach 2013-2016 nastąpiły zmiany polityczne na świecie związane z kryzysem rosyjsko-ukraińskim, wzrostem organizacji terrorystycznej pn. Państwo Islamskie oraz wojną domową w Syrii, co miało znaczny wpływ na państwa europejskie, a tym samym również na przedsiębiorstwa w nich działające. Wspomniane zagrożenia były nie tylko szeroko komentowane w mediach, ale wywierały również wpływ na postrzeganie problemu bezpieczeństwa łańcucha dostaw przez przedsiębiorców oraz na ich działania w tym zakresie.

Celem niniejszego opracowania jest określenie zmian, jakie zaszły w obszarze bezpieczeństwa łańcucha dostaw. Realizacji tego celu służy analiza danych statystycznych na temat zagrożeń dla łańcuchów dostaw, a także danych empirycznych pochodzących z badań ankietowych przeprowadzonych wśród polskich eksporterów i importerów.

1. Opis problemu

Bezpieczeństwo łańcucha dostaw jest bardzo złożonym pojęciem, zatem przytoczenie jednej definicji wiązałoby się z pominięciem wielu jego aspektów. W celu usystematyzowania jego znaczenia zostały wyodrębnione trzy płaszczyzny, według których bezpieczeństwo łańcucha dostaw można interpretować jako:

- a) stan niezagrożenia, co jest de facto celem łańcucha dostaw oraz wszystkich podmiotów w nim uczestniczących,
- b) działania przedsiębiorstw, organizacji lub instytucji publicznych, takie jak wszelkiego rodzaju procedury i środki ochrony zmierzające do osiągnięcia stanu bezpieczeństwa określonego w punkcie a) [Closs, McGarrel, 2004; Sternberg i in., 2012],
- c) polityka (element całościowej polityki bezpieczeństwa państwa).

W celu przeprowadzenia dalszej analizy najbardziej odpowiednie będzie przyjęcie pierwszej interpretacji. Według Ivanova i Sokolova, bezpieczeństwem łańcucha dostaw można określić ogólną właściwość systemu polegającą na niezakłóconym funkcjonowaniu łańcucha dostaw, umożliwiającą osiągnięcie jego celów pod ochroną przed zewnętrznymi zagrożeniami celowymi [Ivanov, Sokolov, 2010]. Takie zagrożenia celowe obejmują wszelkiego rodzaju zamierzone działania człowieka, które są związane z działalnością przestępczą [Hints, 2010]. Właśnie ta cecha pozwala odróżnić dwa aspekty bezpieczeństwa. Pierw-

szy wywodzi się od angielskiego pojęcia *security* i oznacza ochronę łańcucha dostaw przed działalnością przestępczą, a drugi dotyczy angielskiego pojęcia *safety*, czyli zdarzeń związanych z wypadkami, katastrofami naturalnymi i innymi nieumyślnymi działaniami ludzi.

Mimo że dany stan określa się raczej dla danych okoliczności w danym czasie, bezpieczeństwo ma charakter dynamiczny. Zmienia się w czasie w zależności od dwóch czynników – zagrożenia oraz wrażliwości (podatności) na zagrożenia, co można przedstawić za pomocą poniższej funkcji [Hofreiter, 2012]:

$$S(t) = f\{ T(t) \times V(t) \}$$

gdzie:

S – bezpieczeństwo (ang. *security*),

T – zagrożenie (ang. *threat*),

V – wrażliwość (podatność) na zagrożenia (ang. *vulnerability*),

t – czas.

Zagrożeniem można nazwać zdarzenie będące wynikiem umyślnego działania człowieka, w wyniku którego poczucie bezpieczeństwa maleje lub zanika. Wrażliwość z kolei oznacza ekspozycję łańcucha dostaw na zagrożenia i składa się z prawdopodobieństwa wystąpienia zdarzenia oraz zasięgu jego potencjalnych konsekwencji. Wrażliwość można zmniejszyć dzięki wdrożeniu przez uczestników łańcucha dostaw różnego rodzaju działań prewencyjnych i procedur bezpieczeństwa [Svensson, 2002]. Zarówno same zagrożenia, jak i środki ochrony łańcucha dostaw podlegają ciągłym zmianom w czasie. Uwzględniając zatem dynamiczny charakter bezpieczeństwa, należy zwrócić uwagę na konieczność prowadzenia badań w tym zakresie.

Zagrożenia wobec łańcucha dostaw można podzielić ze względu na motywację, jaką kierują się sprawcy przestępstw [Burns, 2016]. W przypadku przestępstw motywowanych finansowo może nią być chęć osiągnięcia osobistej korzyści, najlepiej materialnej. Z kolei przestępcy motywowani względami ideologicznymi najczęściej za cel stawiają sobie spowodowanie znacznej szkody, utraty życia oraz zastraszenie społeczeństwa. To zamierzenie z reguły jest realizowane za pomocą działalności terrorystycznej. Od tak rozumianej motywacji często zależy przedmiot ataku. Jeżeli sprawca kieruje się osobistą, finansową korzyścią, najczęściej skupi swoją uwagę na podmiotach gospodarczych, natomiast przestępcy, którym przyświecają względy ideologiczne, zaatakują przede wszystkim ludność cywilną i władze państw, a łańcuchy dostaw są ich celem dopiero w drugiej kolejności. Działalność przestępcza może przybierać różne formy. Często zdarza się, że obok legalnych łańcuchów dostaw funkcjonują ich nielegalne odpowied-

niki, wzdłuż których następuje przepływ fałszowanych bądź nielegalnych towarów, w tym również różnych rodzajów broni, która może być następnie wykorzystywana do prowadzenia działalności terrorystycznej. Wykorzystywane są te same szlaki transportowe, porty morskie czy przejścia graniczne, a oba systemy różni jedynie cel i sposób konfiguracji [Basu, 2013]. Niezwykle istotne jest zatem rozpoznanie wszelkiego rodzaju zagrożeń, a także ich ocena i stały monitoring, aby było możliwe przygotowanie odpowiednich środków ochrony.

Bezpieczeństwo łańcucha dostaw jest pojęciem bardzo złożonym, zatem jego analiza powinna uwzględniać wiele zagadnień, takich jak: bezpieczeństwo transportu, bezpieczeństwo dystrybucji, bezpieczeństwo logistyczne, bezpieczeństwo korporacyjne, ochrona obiektów i infrastruktury, bezpieczeństwo publiczne, bezpieczeństwo narodowe, zarządzanie awarią czy zarządzanie kryzysowe. Badania powinny uwzględniać różne ogniwa i przepływy w łańcuchu dostaw, w tym przepływ informacji. Należy jednak podkreślić, że obecnie wymiana informacji w większości następuje drogą elektroniczną, a jej bezpieczeństwo zależy w dużej mierze od jakości systemów informatycznych, co stanowi przedmiot badań innych dziedzin nauki.

2. Analiza danych statystycznych

Szczegółowej analizie poddano trzy wybrane zagrożenia, które najczęściej pojawiają się w literaturze dotyczącej bezpieczeństwa łańcucha dostaw, tj. kradzieże, terroryzm oraz piractwo morskie.

Dane statystyczne dotyczące zagrożeń wobec łańcucha dostaw są trudne do pozyskania, ponieważ nie prowadzi się ich stałego monitoringu, a wiele zdarzeń nie jest zgłaszanych odpowiednim służbom bądź następuje ich błędna klasyfikacja. Bazę danych dotyczącą kradzieży ładunków w Europie prowadzi stowarzyszenie TAPA EMEA [2015], jednakże raportowanie do tej bazy jest nadal niekompletne ze względu na trudności w identyfikacji odpowiednich zdarzeń w policyjnych rejestrach. Pomimo tego z roku na rok jest zgłaszanych coraz więcej zdarzeń. Raport za 2014 rok uwzględniał aż o 42,5% więcej przypadków kradzieży niż w 2013 roku. W kolejnym roku wzrost wyniósł 37,4%, natomiast dane za I kwartał 2016 roku wskazują na wzrost rzędu 115,5% w stosunku do pierwszego kwartału 2015 roku.

Ciekawych informacji dostarcza analiza danych dotyczących typu najczęściej zgłaszanych incydentów. W 2014 r. aż 48,6% wszystkich przypadków stanowiły kradzieże ładunku z pojazdu. W dalszej kolejności znalazły się kradzieże

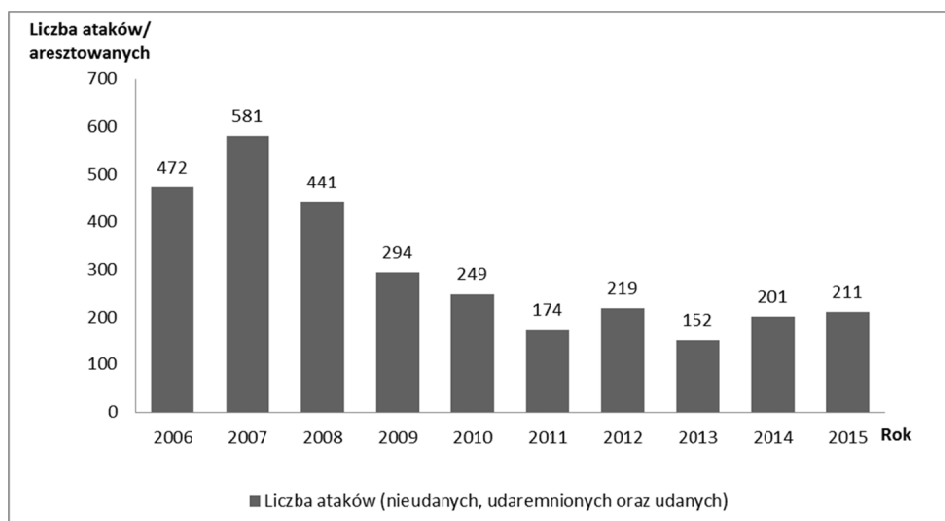
dokonane na terenie przedsiębiorstwa (17,5%) oraz kradzieże całych pojazdów (16,8%). Niepokojący może być fakt, że niemal 10% przypadków stanowiły porwania, które niejednokrotnie wiążą się z agresją sprawców. Zauważono, że kradzieże dokonywane w Stanach Zjednoczonych wiążą się z mniejszą przemocą niż w Europie ze względu na wysokość kar za popełnienie tego typu przestępstw, a także lepsze zabezpieczenie transportu na kontynencie europejskim, co wymusza na przestępcach konieczność stosowania przemocy w celu osiągnięcia zamierzonych korzyści [Burges, 2013].

Kolejnym ważnym zagrożeniem, często pomijanym przez przedsiębiorców, jest terroryzm. Zjawisko to było bodźcem i najważniejszym motorem rozwoju całej koncepcji bezpieczeństwa łańcucha dostaw. Jednakże terroryzm jest pojęciem nieprecyzyjnym, a także, głównie z przyczyn politycznych, właściwie niezdefiniowanym, czego następstwem są trudności w gromadzeniu statystyk. Kolejną cechą tego zagrożenia jest jego nieprzewidywalność, która wynika z relatywnej rzadkości tego zjawiska i wiąże się z brakiem możliwości jego prognozowania za pomocą metod statystycznych.

Niektórzy eksperci podkreślają, że zjawisko terroryzmu ulega transformacji, rozróżniając przy tym tzw. stary i nowy terroryzm [Laqueur, 1999; Hoffman, 2006; Neumann, 2009]. Według cytowanych autorów koncepcja nowego terroryzmu charakteryzuje się m.in. brakiem struktur, ponadnarodowym zasięgiem, finansowaniem pochodzącym z działalności przestępczej, bezkrytyczną przemocą [Matusitz, 2013], a także znacznie mniej wyraźnie zdefiniowanymi celami, takimi jak bliżej nieokreślona wrogość, przede wszystkim wobec Stanów Zjednoczonych, lub chęć zemsty, niejednokrotnie podsycana radykalizmem religijnym [Hoffman, 2006], podczas gdy inspiracją starego terroryzmu były raczej świeckie koncepcje nacjonalistyczne i separatystyczne. Współczesnym terrorystom zależy przede wszystkim na jak największych zniszczeniach i dużej liczbie ofiar, co ma im zapewnić rozgłos oraz zastraszyć społeczeństwo. Zwraca się uwagę, że współcześnie terroryści, szczególnie ci fanatycznie nastawieni, mogą nawet dążyć do wykorzystania broni masowej zagłady [Laqueur, 1999]. Chęć ochrony społeczeństwa przed tego typu zagrożeniami znalazła odzwierciedlenie w koncepcjach bezpieczeństwa przyjmowanych przez rządy państw i organizacje międzynarodowe. O ile idea rozróżnienia tych dwóch postaci terroryzmu jest relatywnie stara i przez niektórych badaczy krytykowana [Copeland, 2001; Duyveteyn, 2004; Spencer, 2014], o tyle aktualne statystyki wydają się ten podział potwierdzać.

Na rysunku 1 przedstawiono liczbę ataków terrorystycznych na terenie Europy w okresie od 2006 do 2015 roku. Od 2007 roku wyraźny jest znaczący

spadek liczby tego typu zdarzeń, z niewielkim jednorazowym wzrostem w 2012 roku. Wynika to przede wszystkim z ograniczenia działalności organizacji terrorystycznych o podłożu separatystycznym. Niepokojącym zjawiskiem jest natomiast fakt, że wzrasta zagrożenie związane z terroryzmem motywowanym względami religijnymi, ponieważ przekłada się to na zakres szkód oraz liczbę ofiar zamachów.



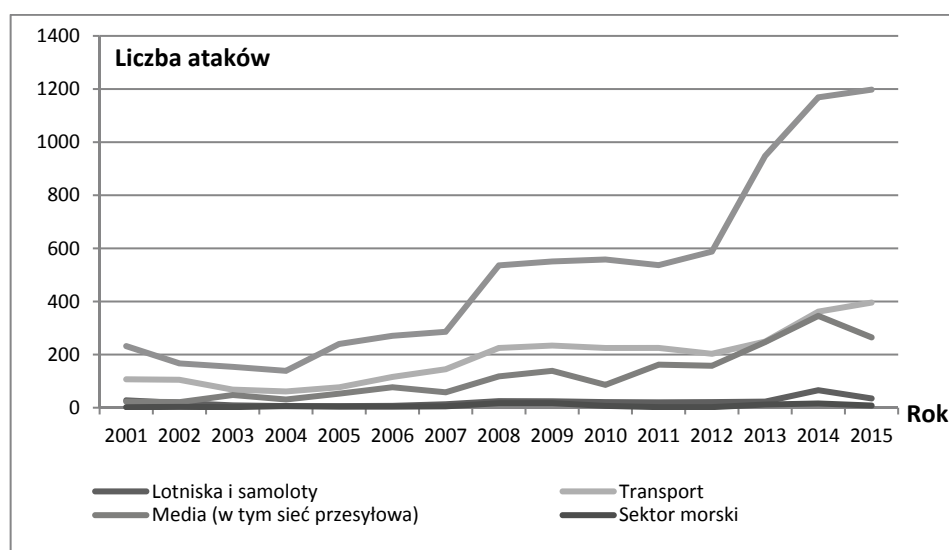
Rys. 1. Liczba ataków terrorystycznych w krajach Unii Europejskiej w latach 2006-2015

Źródło: Opracowanie własne na podstawie: Europol [2016].

Obszerną bazę danych na temat ataków terrorystycznych oferuje amerykański Departament Bezpieczeństwa we współpracy z Uniwersytetem Maryland [START, 2016]. Na jej podstawie została przeprowadzona analiza zjawiska terroryzmu. Ataki terrorystyczne są najczęściej skierowane przeciw celom prywatnym, tj. przeciw ludziom i ich mieniu. W okresie od 2001 do 2015 roku stanowiły one łącznie ponad 30% wszystkich zdarzeń. Drugą grupę z udziałem rządu 9,1% stanowił sektor biznesu. Jest to zarazem najbardziej liczna grupa spośród pięciu celów, które wyodrębniono ze względu na ich związek z funkcjonowaniem łańcuchów dostaw (rys. 2). Można zauważyć, że w latach 2012-2015 nastąpił znaczny wzrost liczby ataków na cele biznesowe (liczba ataków wzrosła dwukrotnie) oraz inne cele związane z łańcuchami dostaw. Największy wzrost, o ponad 200%, nastąpił w przypadku ataków na lotniska i samoloty.

Warto zauważyć, że udział ataków na cele biznesowe wśród łącznej liczby zdarzeń terrorystycznych różni się w zależności od regionu. W Stanach Zjedno-

czonych oraz Europie Zachodniej jest on około trzykrotnie wyższy niż średnio dla całego świata. Znaczne zagrożenie wiąże się również z transportem, przy czym w Stanach Zjednoczonych sektor ten jest rzadziej obierany jako cel ataku, natomiast częściej przeprowadza się tam ataki na lotniska i samoloty. Relatywnie mało zdarzeń dotyczy transportu morskiego, ponieważ ataki na statki częściej kwalifikuje się jako działalność piratów, a nie terrorystów. Niepokojący jest również wzrost ofiar terroryzmu. Dane z lat 2013 i 2014 wskazują na wzrost liczby ofiar śmiertelnych o 80% do ponad 14 tys. osób w 2014 roku [START, 2016].



Rys. 2. Liczba ataków terrorystycznych na świecie według wybranych celów ataku w latach 2001-2015

Źródło: Opracowanie własne na podstawie: START [2016].

Ostatnim zagrożeniem poddanym bardziej szczegółowej analizie jest działalność piratów morskich. Artykuł 101 Konwencji Narodów Zjednoczonych o prawie morza wyraźnie definiuje piractwo jako wszelkiego rodzaju nielegalne akty przemocy, przetrzymania bądź grabieży popełnione dla celów osobistych przez załogę lub pasażerów prywatnego statku bądź samolotu skierowane przeciwko statkowi morskiemu i powietrznemu lub osobom i mieniu na pokładzie takiego statku albo samolotu popełnione na pełnym morzu bądź w miejscu niepodlegającym jurysdykcji żadnego państwa. Za piractwo uznaje się również akt dobrowolnego udziału w korzystaniu ze statku morskiego lub powietrznego, jeżeli jego sprawca miał wiedzę co do pirackiego charakteru tego statku. Piractwem jest również podżeganie i celowe ułatwianie tego typu działalności [United Nations, 1982].

Piratów od terrorystów odróżnia przede wszystkim motyw działania. Ci pierwsi kierują się głównie chęcią osiągnięcia korzyści finansowej, natomiast terroryści – motywacją ideologiczną oraz chęcią wywołania strachu i zawirowań społecznych. Warto jednak podkreślić, że istnieje pewien związek między tymi zjawiskami, ponieważ piractwo jest często źródłem finansowania działalności terrorystycznej [Burns, 2016]. Najwięcej ataków piratów morskich odnotowano w latach 2000-2003 oraz 2009-2011, kiedy ich liczba często przekraczała 400 incydentów rocznie. W pierwszym z podanych okresów najczęściej zdarzeń miało miejsce na wodach Azji Południowo-Wschodniej, natomiast pod koniec pierwszej dekady XXI w. problem ten dotyczył przede wszystkim działalności piratów somalijskich u wybrzeży Afryki. Zagrożenie udało się zmniejszyć dzięki podjęciu wspólnych działań przez marynarki wojenne wielu krajów zrzeszone w ramach EU NAVFOR, NATO i Combined Task Force, przy wsparciu niezależnych sił z Chin, Indii, Japonii, Korei Południowej i Rosji. Z kolei w latach 2013-2015 ponownie nasiliła się działalność piratów u wybrzeży Indonezji i w rejonie cieśniny Malakka. Oprócz wspomnianych regionów piractwo występuje również w innych miejscach, m.in. na wodach Zatoki Gwinejskiej. W polskich mediach w 2015 roku głośna była sprawa porwania członków załogi statku Szafir, należącego do armatora EuroAfrica. Z uwagi na takie wydarzenia, jak również narastające zagrożenie terrorystyczne, może się zmieniać ocena bezpieczeństwa łańcuchów dostaw ze strony ich uczestników. Jest to przedmiotem analizy w kolejnej części niniejszego opracowania.

Analiza danych statystycznych potwierdza dynamiczny charakter bezpieczeństwa łańcucha dostaw. Najbardziej widoczną w ostatnich latach zmianą jest znaczący wzrost zagrożenia terrorystycznego. Jest to zjawisko szczególnie niepokojące, ponieważ spośród analizowanych zdarzeń terroryzm charakteryzuje się z reguły największym zasięgiem konsekwencji (strat), a także małym prawdopodobieństwem wystąpienia, co sprawiało, że przez wiele lat przedsiębiorcy je ignorowali w swoich planach zarządzania ryzykiem, a walka z terroryzmem była jak dotąd domeną państw. Dopiero wzrost zagrożenia w ostatnich latach doprowadził do tego, że coraz więcej firm dostrzeże takie niebezpieczeństwo i zgłasza potrzebę współpracy z rządami i organizacjami międzynarodowymi w celu zabezpieczenia międzynarodowych łańcuchów dostaw.

W przypadku zagrożeń charakteryzujących się większym prawdopodobieństwem wystąpienia, a także mniejszymi skutkami, takich jak kradzieże, przedsiębiorcy często muszą działać samodzielnie, ponieważ zarówno wsparcie ze strony państwa (np. w zakresie budowy monitorowanych parkingów), jak i otoczenie regulacyjne są w tym przypadku niewielkie.

3. Opis metody badawczej

Badanie ankietowe zostało przeprowadzone za pomocą techniki CATI (wspomaganych komputerowo wywiadów telefonicznych) latem 2013 roku [Jazdzewska-Gutta, 2015] oraz wiosną 2016 roku. Badaniem objęto odpowiednio 600 oraz 605 polskich eksporterów i importerów towarów, zajmujących się handlem wewnątrz Unii Europejskiej, jak również poza nią. Większość badanych firm zajmuje się zarówno eksportem, jak i importem towarów. Przedsiębiorstwa te są zróżnicowane pod względem wielkości, przy czym największą grupę stanowią mikro (2013 – 18,8%, 2016 – 23,3%), małe (2013 – 37,7%, 2016 – 38,7%) i średnie (2013 – 31%, 2016 – 28,9%) przedsiębiorstwa, natomiast udział dużych przedsiębiorstw wyniósł odpowiednio 12,5% oraz 9,1%. Respondenci reprezentują różne branże – handel hurtowy, produkcja mebli, maszyn i urządzeń, żywności, elektroniki, handel hurtowy itd. W zależności od struktury organizacyjnej oraz wielkości przedsiębiorstwa odpowiedzi na pytania udzielali właściciele lub osoby zarządzające firmą bądź menedżerowie lub specjaliści z działów logistyki, transportu, eksportu itd., czyli osoby bezpośrednio zaangażowane w realizację procesów transportowo-logistycznych.

4. Analiza wyników badania ankietowego

Analiza danych wskazuje, że w 2016 roku ponad 75% respondentów oceniło poziom bezpieczeństwa ich procesów transportowo-logistycznych jako wysoki lub bardzo wysoki, co stanowiło aż o 15 punktów procentowych więcej niż w 2013 roku. Z kolei w 2013 roku dwukrotnie więcej respondentów uznało, że poziom bezpieczeństwa jest niski lub bardzo niski. W 2016 roku wartość ta wyniosła około 6%. Większość firm jest usatysfakcjonowana poziomem zabezpieczenia łańcuchów dostaw i nie widzi potrzeby wprowadzania w tym zakresie dodatkowych procedur, regulacji czy środków ochrony. Mimo tego, że ogólny poziom bezpieczeństwa został oceniony jako wysoki, bardziej szczegółowe dane wskazują, iż respondenci dostrzegają zagrożenia ze strony otoczenia wobec ich łańcuchów dostaw.

Kolejne pytanie dotyczyło oceny zagrożeń wobec łańcucha dostaw. Respondenci zostali poproszeni o stwierdzenie, czy dane zdarzenie stanowi zagrożenie dla łańcucha dostaw firmy, a następnie o ocenę stopnia zagrożenia. Na podstawie danych zaprezentowanych w tab. 1 można zauważyć, że ranking zagrożeń nie uległ poważnym zmianom. Nadal dla większości firm największym zagrożeniem są kradzieże ładunku. Najbardziej istotną zmianą, odzwierciedlającą

cą dynamiczny charakter bezpieczeństwa, jest znaczne zwiększenie liczby respondentów, którzy rozpoznają dane zagrożenie. Niektóre z tych wartości zwiększyły się dwu-, trzy-, a nawet czterokrotnie, np. w przypadku terroryzmu, piractwa i przemytu broni masowego rażenia. Jednocześnie zmniejszyła się jednak średnia ocena ciężaru tych zagrożeń.

Tabela 1. Ocena zagrożeń wobec łańcuchów dostaw

Zagrożenie	Ocena* zagrożenia 2013	Ocena* zagrożenia 2016	Liczba respondentów uznających zdarzenie za zagrożenie dla ich łańcucha dostaw – 2013 rok	Liczba respondentów uznających zdarzenie za zagrożenie dla ich łańcucha dostaw – 2016 rok
Kradzieże ładunków i środków transportu w czasie transportu	2,91	2,26	168	210
Kradzieże towarów w magazynach, terminalach i na placach składowych	2,84	2,22	119	162
Naruszenie bezpieczeństwa informacji	3,23	2,14	57	151
Przejęcie ładunku przez fałszywych przewoźników lub spedytorów	3,02	2,15	50	145
Porwanie ładunku/środka transportu dla okupu	3,08	2,15	62	142
Wykorzystanie ładunku i/lub środka transportu, w którym znajdował się ładunek, w celu przemytu rzeczy lub osób	2,83	2,12	47	141
Przemyt broni masowego rażenia w kontenerze	2,90	2,07	29	135
Kradzież wartości niematerialnych i prawnych, podróbki towarów	2,94	2,07	50	135
Atak terrorystyczny	3,28	2,10	29	134
Działalność piratów morskich	3,11	2,14	27	120

* W kolumnie znajduje się średnia ocena danego zagrożenia, gdzie 1 oznacza zagrożenie bardzo małe, a 5 – bardzo poważne. Stopień zagrożenia był oceniany tylko przez respondentów, którzy uznali dane zdarzenie za zagrożenie dla łańcucha dostaw firmy.

Źródło: Opracowanie własne na podstawie badań ankietowych.

Respondentów zapytano również o to, czy w ich łańcuchach dostaw w ostatnich 5 latach wystąpiły zdarzenia wynikające z działalności przestępczej. Najczęściej zgłaszanymi zagrożeniami były kradzieże ładunku w czasie transportu (około 6% respondentów), celowe zniszczenie ładunku (3%) oraz oszustwo nierzetelnego dostawcy (2,5%). Warto podkreślić, że w poprzedniej edycji badania wartości te były czasem znacznie wyższe. Spośród wymienionych zagrożeń za najbardziej realne w ocenie przedsiębiorców można uznać ryzyko kradzieży

ładunku lub całego pojazdu w trakcie transportu, gdyż najwięcej osób (6% respondentów) wskazało, że takie zdarzenie dotyczyło ich firmy w ciągu ostatnich pięciu lat. Najczęściej wymienianym skutkiem takich kradzieży były straty finansowe.

W badaniu zostały również poruszone aktualne zagadnienia związane z bezpieczeństwem łańcucha dostaw, takie jak wpływ zagrożenia terrorystycznego i kryzysu migracyjnego na funkcjonowanie łańcuchów dostaw. W wyniku zagrożenia terrorystycznego w związku z zamachami w Paryżu i Brukseli poniesienie strat zadeklarowało 11 respondentów. Najczęściej wymieniane straty dotyczyły opóźnienia dostaw, ale w jednym przypadku wiązało się to nawet z żądaniem od przewoźnika większej opłaty za realizację przewozu. Straty wynikające z kryzysu migracyjnego zadeklarowało dwukrotnie więcej respondentów. Dotyczyły one utrudnień w związku z transportem do Wielkiej Brytanii, opóźnień na granicach oraz zniszczenia bądź kradzieży ładunku lub próby sforsowania pojazdu przez migrantów przebywających w tymczasowym obozie w Calais. Ewentualną konsekwencją całego szeregu zagrożeń mogłaby być likwidacja strefy Schengen. Co ciekawe, jedynie 35,5% respondentów uznało, że spowodowałoby to utrudnienia w realizacji ich eksportu bądź importu. W kilku przypadkach deklarowano nawet, że w celu zwiększenia bezpieczeństwa łańcucha dostaw należy zwiększyć kontrole na granicach oraz portach morskich i lotniczych.

Wyniki badań ankietowych pozwalają również na wskazanie zmian, jakie nastąpiły w obszarze działań przedsiębiorstw mających na celu zapewnienie bezpieczeństwa łańcuchów dostaw. Eksporterzy i importerzy zostali zapytani o stosowanie wybranych procedur i środków bezpieczeństwa. Lista tych działań została określona na podstawie analizy literatury oraz międzynarodowych raportów. Dane pozyskane z ankiet przedstawiono w tab. 2.

Tabela 2. Działania podejmowane przez przedsiębiorców w celu ochrony łańcucha dostaw

Działania	Liczba firm deklarujących stosowanie danego działania w 2013 roku	Udział firm (w %) deklarujących stosowanie danego działania w 2013 roku	Liczba firm deklarujących stosowanie danego działania w 2016 roku	Udział firm (w %) deklarujących stosowanie danego działania w 2016 roku
1	2	3	4	5
Śledzenie ładunku	120	20,0	254	42,0
Ochrona informacji i systemów informatycznych przed dostępem niepowołanych osób	24	4,0	204	33,7
Stała współpraca z naszymi dostawcami i/lub odbiorcami i innymi partnerami w ramach łańcucha dostaw na rzecz poprawy bezpieczeństwa	68	11,3	185	30,6

cd. tabeli 2

1	2	3	4	5
Kontrola i analiza ryzyka dostawców	73	12,2	159	26,3
Kontrola i analiza ryzyka przewoźników, spedytorów i innych podwykonawców	36	6,0	150	24,8
Wytyczne dla przewoźników co do korzystania ze strzeżonych parkingów	55	9,2	150	24,8
Kontrola procesu załadunku towaru w celu wyeliminowania możliwości przemytu	34	5,7	133	22,0
Systemy monitoringu wizyjnego	53	8,8	123	20,3
Przeszkolenie i instrukcje dla pracowników w zakresie stałego monitoringu bezpieczeństwa	69	11,5	119	19,7
Kompleksowa identyfikacja i ocena ryzyka w łańcuchu dostaw (audyty bezpieczeństwa)	16	2,7	119	19,7
Analiza profili kandydatów do pracy pod kątem bezpieczeństwa	42	7,0	51	8,4
Plomby, inteligentne kontenery itp.	123	20,5	48	7,9
Stała współpraca z organami publicznymi na rzecz poprawy bezpieczeństwa	22	3,7	38	6,3
Niezapowiedziane ćwiczenia i treningi na wypadek wystąpienia zakłócenia w łańcuchu dostaw	9	1,5	16	2,6

Źródło: Opracowanie własne na podstawie badań ankietowych.

W przypadku większości wymienionych procedur w 2016 roku nastąpił wzrost liczby przedsiębiorców deklarujących ich stosowanie. Liczba firm, w których wprowadzono elementy analizy ryzyka oraz ochrony informacji, w ciągu trzech lat wzrosła nawet kilkukrotnie. Może to oznaczać, że przedsiębiorcy, dostrzegając zagrożenia płynące z otoczenia, coraz chętniej samodzielnie podejmują działania zmierzające do zabezpieczenia ich łańcuchów dostaw. Najwięcej przedsiębiorców deklarowało śledzenie ładunku, ochronę informacji i systemów informatycznych oraz stałą współpracę z dostawcami. Można również zauważyć, że przedsiębiorcy nie doceniają roli człowieka w zapewnieniu bezpieczeństwa, co przejawia się m.in. w relatywnie mniejszym zainteresowaniu szkoleniami, a także niewielkim udziałem firm, w których przeprowadza się okresowe ćwiczenia lub analizy kandydatów do pracy pod kątem bezpieczeństwa.

Można również zaobserwować, że w istotny sposób zmieniły się opinie przedsiębiorców na temat podmiotów, które powinny być odpowiedzialne za bezpieczeństwo łańcuchów dostaw. W 2013 roku ponad połowa respondentów

uznała, że przedsiębiorcy powinni sami zadbać o bezpieczeństwo (52,3%), a potrzebę współpracy przedsiębiorstw z rządami państw wyraziło jedynie 36,8% ankietowanych. Z kolei odpowiedzialność państw i rządów wskazało jedynie 14,2% przedsiębiorców¹, natomiast organizacji międzynarodowych 9,5% ankietowanych [Jażdżewska-Gutta, 2015]. W badaniu przeprowadzonym w 2016 roku zdecydowana większość respondentów była zdania, że za bezpieczeństwo łańcucha dostaw odpowiadają organizacje międzynarodowe (67,9%) oraz państwa i rządy (64,3%). Ponad połowa badanych uznała, że firmy powinny współpracować w tym zakresie z rządami państw, natomiast samodzielne działania przedsiębiorców preferuje jedynie 6,4% z nich.

W wyjaśnieniu powodów wspomnianych zmian pomocna może być przeprowadzona analiza opinii respondentów na temat zagrożeń wobec łańcucha dostaw. Zaobserwowany przez nich wzrost zagrożenia związanego z terroryzmem, przemytem i działalnością piratów morskich może prowadzić do wniosków, iż sami przedsiębiorcy nie będą w stanie ochronić łańcuchów dostaw, w związku z czym konieczne jest zaangażowanie rządów i organizacji międzynarodowych, jak również ściślejsza współpraca pomiędzy biznesem i administracją.

5. Bezpieczeństwo łańcucha dostaw jako element polityki państw

Kompleksowa analiza zmian w obszarze bezpieczeństwa łańcucha dostaw wymaga również uwzględnienia działań podejmowanych przez rządy państw oraz organizacje międzynarodowe, niejednokrotnie w ramach realizacji polityki bezpieczeństwa. W latach 2001-2016 powstało wiele regulacji oraz dokumentów strategicznych dotyczących bezpieczeństwa. Znaczna część działań była inspirowana przez Organizację Narodów Zjednoczonych, która skupiła się przede wszystkim na zwalczaniu terroryzmu, głównie w zakresie jego finansowania, walki z przemytem broni masowego rażenia oraz ochrony przed zamachami terrorystycznymi realizowanymi z użyciem materiałów wybuchowych, jednak nie są to działania bezpośrednie, a najczęściej jedynie nieskoordynowane zalecenia oraz deklaracje podjęcia takich działań, które mają znaczenie symboliczne. Więcej inicjatyw podejmują agencje wyspecjalizowane, takie jak Organizacja Międzynarodowego Lotnictwa Cywilnego (ICAO) czy Międzynarodowa Organizacja Morska (IMO). Aktywna działalność obu wymienionych organizacji skutkuje szeregiem regulacji w zakresie bezpieczeństwa, odnoszących się zarówno do transportu morskiego, jak i lotniczego.

¹ W pytaniu o podmioty odpowiedzialne za bezpieczeństwo można było wskazać więcej niż jedną odpowiedź.

Na arenie międzynarodowej szczególną aktywność w obszarze polityki bezpieczeństwa łańcucha dostaw wykazują Stany Zjednoczone i Unia Europejska. Z porównania ich działań jednoznacznie wynika, że Stany Zjednoczone zdołały wypracować bardziej spójne rozwiązania, natomiast działania podejmowane w ramach Unii Europejskiej są bardziej chaotyczne, przy czym taki stan rzeczy można tłumaczyć koniecznością osiągnięcia w tym zakresie zgody wielu państw członkowskich UE. W Stanach Zjednoczonych już w 2001 roku zadeklarowano, że bezpieczeństwo łańcucha dostaw jest elementem szerszej strategii bezpieczeństwa narodowego [Williams, Lueg, LeMay, 2008]. W kolejnych latach uchwalono m.in. takie dokumenty, jak: *Narodowa Strategia Bezpieczeństwa Transportu* (2005 rok), *Strategia zwiększenia międzynarodowego bezpieczeństwa łańcucha dostaw* (2007 rok) oraz *Narodowa strategia bezpieczeństwa łańcucha dostaw* (2012 rok). Za najbardziej kompleksowy dokument można uznać strategię z 2012 roku. Wyznaczono w niej dwa podstawowe cele, tj. promowanie sprawnego i bezpiecznego przepływu towarów oraz wspieranie sprężystych łańcuchów dostaw, odpornych na zmieniające się zagrożenia i szybko odzyskujących sprawność [National Strategy..., 2012]. Strategia obejmuje wszystkie gałęzie transportu i różne zagrożenia oraz zakłada współpracę międzynarodową i krajową ze wszystkimi interesariuszami. Należy podkreślić, że dokument ten skupia się nie tylko na ochronie łańcuchów dostaw, ale również na ich szybkim powrocie do pierwotnego stanu w przypadku wystąpienia zagrożenia.

W Unii Europejskiej, ze względu na rozproszenie kompetencji pomiędzy różnymi instytucjami oraz państwami członkowskimi, mimo podjętych prób nie powstał żaden kompleksowy dokument odnoszący się do bezpieczeństwa łańcucha dostaw. Powstało natomiast wiele dokumentów poruszających tę tematykę, jednakże ich znaczna część ma jedynie formę komunikatów Komisji Europejskiej, które nie są dokumentami wiążącymi. Najbardziej kompleksowe podejście zaprezentowano w Unijnym Kodeksie Celnym z 2013 roku. W dokumencie tym podkreślono, że wiodącą rolę w zakresie bezpieczeństwa łańcuchów dostaw powinny pełnić organy celne oraz sprecyzowano ich zadania i kompetencje w tym obszarze.

Analiza regulacji powstałych po 2001 roku w Stanach Zjednoczonych i Unii Europejskiej pozwala stwierdzić, że ewolucja Stanów Zjednoczonych w kierunku bardziej kompleksowego podejścia jest bardziej korzystnym zjawiskiem, ponieważ umożliwia koordynację działań poszczególnych służb i organów administracyjnych, co powinno się przyczynić do lepszej ochrony poszczególnych ogniw i przepływów w łańcuchach dostaw.

W kontekście wyników badania ankietowego można przyjąć, że obserwowany przez respondentów wzrost zagrożeń wobec łańcuchów dostaw, w szczególności takich, przed którymi przedsiębiorcy nie są w stanie samodzielnie zapewnić sobie ochrony, wpłynie na wzrost akceptacji działań rządów, instytucji administracji publicznej oraz organizacji międzynarodowych zmierzających do zwiększenia poziomu bezpieczeństwa, nawet kosztem dodatkowych nakładów ze strony przedsiębiorców.

Biorąc pod uwagę obecne środowisko regulacyjne, należy stwierdzić, że priorytetem polityki bezpieczeństwa powinna być koordynacja i harmonizacja działań. Wiele elementów, np. kwestie związane z kradzieżami ładunków, pozostaje nieuregulowanych, podczas gdy w niektórych obszarach, takich jak transport lotniczy czy morski, występuje nadmiar regulacji, niejednokrotnie dotyczących tego samego zakresu [Jażdżewska-Gutta, 2015]. Badania ankietowe wykazały, że przedsiębiorcy oczekują od rządów państw programów certyfikacji zaufanych podmiotów, takich jak AEO, przy czym warto podkreślić, że osiągnięcie pełnych korzyści z tego typu inicjatyw będzie możliwe dzięki ich harmonizacji i wzajemnym uznawaniu w skali międzynarodowej [Grottel, 2015], a także opartej na zaufaniu współpracy przedsiębiorstw i administracji.

Z dużym prawdopodobieństwem można stwierdzić, że pojawianie się nowych zagrożeń dla międzynarodowych łańcuchów dostaw będzie w przyszłości skutkowało powstaniem kolejnych regulacji, które będą miały na celu zapewnienie bezpieczeństwa, jednakże nowe przepisy trzeba tworzyć w przemyślny sposób. Niemal 95% respondentów uznało, że od rządów państw oczekują współpracy w zakresie tworzenia programów ochrony transportu i logistyki. Oznacza to, że przedsiębiorcy są otwarci na nowe inicjatywy ze strony rządów państw i organizacji międzynarodowych, ale oczekują również, że będą mogli wziąć udział w procesie decyzyjnym, a następnie czerpać korzyści z przywilejów nadanych zaufanym podmiotom.

Podsumowanie

Przeprowadzone analizy potwierdzają, że bezpieczeństwo ma dynamiczny charakter. Wzrost zagrożeń wobec łańcuchów dostaw można zaobserwować zarówno na podstawie danych statystycznych, jak i w opiniach przedsiębiorców, którzy coraz częściej rozpoznają różnego rodzaju niebezpieczeństwa, w tym również nowe zjawiska wynikające m.in. z kryzysu migracyjnego. Największy wzrost zaobserwowano w przypadku zagrożenia terroryzmem, piractwem i prze-

mytem broni masowego rażenia, co może być wynikiem szeroko komentowanych w mediach zdarzeń, w tym ataków terrorystycznych w latach 2014-2016. Wcześniej wielu przedsiębiorców ignorowało tego typu ryzyko, skupiając się przede wszystkim na ochronie przed zdarzeniami cechującymi się większym prawdopodobieństwem wystąpienia, takimi jak kradzieże. Wzrost zagrożenia w wymienionych obszarach może prowadzić do wniosków, że do jego zwalczania konieczna jest współpraca przedsiębiorstw z rządami państw i organizacjami międzynarodowymi oraz kompleksowe podejście do problemu bezpieczeństwa. Godne uwagi są skoordynowane działania podejmowane w tym zakresie przez rząd i administrację Stanów Zjednoczonych. Nie należy jednakże bezpośrednio kopiować przyjętych tam rozwiązań, przede wszystkim ze względu na odmienny charakter zagrożeń występujących w Stanach Zjednoczonych i Europie.

Wyniki ankiet pokazały również, że polscy przedsiębiorcy są skłonni do współpracy z organami publicznymi oraz do poniesienia dodatkowych kosztów w celu zapewnienia bezpieczeństwa, jednakże konieczne są harmonizacja i koordynacja różnych działań, aby uniknąć sytuacji nakładania się kompetencji różnych służb oraz regulacji dotyczących tych samych obszarów łańcucha dostaw.

Literatura

- Basu G. (2013), *The Role of Transnational Smuggling Operations in Illicit Supply Chains*, "Journal of Transportation Security", Vol. 6, s. 315-328.
- Burges D. (2013), *Cargo Theft, Loss Prevention, and Supply Chain Security*, Butterworth-Heinemann, Oxford.
- Burns M. (2016), *Logistics and Transportation Security: A Strategic, Tactical, and Operational Guide to Resilience*, Taylor & Francis Group, Boca Raton.
- Closs D.J., McGarrel E.F. (2004), *Enhancing Security Throughout the Supply Chain*, The IBM Center for the Business of Government.
- Copeland T. (2001), *Is the "New Terrorism" Really New? An Analysis of the New Paradigm for Terrorism*, "The Journal of Conflict Studies", Vol. XXI, No. 2.
- Duyvesteyn I. (2004), *How New Is the New Terrorism*, "Studies in Conflict & Terrorism", Vol. 27, No. 5, s. 439-454.
- Europol (2016), *European Union Terrorism Situation and Trend Report (TE-SAT) 2016*, <https://www.europol.europa.eu/> (dostęp: 10.03.2017).
- Grottel M. (2015), *The Safety and Security of International Trade as a Determinant of the Business Strategy of the Polish Customs Service*, "European Integration Studies", No. 9, s. 139-154.
- Hintsa J. (2010), *A Comprehensive Framework for Analysis and Design of Supply Chain Security Standards*, "Journal of Transportation Security", Vol. 3, Iss. 2, s. 105-125.

- Hoffman B. (2006), *Inside Terrorism*, Columbia University Press, New York.
- Hofreiter L. (2012), *Wstęp do studiów bezpieczeństwa*, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego, Kraków.
- Ivanov D., Sokolov B. (2010), *Adaptive Supply Chain Management*, Springer Verlag, London.
- Jążdżewska-Gutta M. (2015), *Niedoskonałości w zakresie bezpieczeństwa międzynarodowych łańcuchów dostaw*, „Zeszyty Naukowe Uniwersytetu Gdańskiego. Ekonomia Transportu i Logistyka” (Modelowanie Procesów i Systemów Logistycznych), cz. 14, nr 56, s. 53-69.
- Laqueur W. (1999), *The New Terrorism: Fanaticism and the Arms of Mass Destruction*, Oxford University Press, New York.
- Matusitz J. (2013), *Terrorism and Communication. A Critical Introduction*, Sage Publications, Los Angeles-London-New Delhi-Singapore-Washington DC.
- National Strategy for Global Supply Chain Security (2012), The White House, Washington.
- Neumann P.R. (2009), *Old and New Terrorism. Late Modernity, Globalization and the Transformation of Political Violence*, Polity Press, Cambridge.
- Spencer A. (2014), *The myth of ‘New Terrorism’* [w:] S. Gottlieb (ed.), *Debating Terrorism and Counterterrorism: Conflicting Perspectives on Causes*, Sage Publications, Los Angeles-London-New Delhi-Singapore-Washington DC.
- START (2016), *Global Terrorism Database*, A Center of Excellence of the U.S. Department of Homeland Security and University of Maryland, <https://www.start.umd.edu> (dostęp: 24.08.2016).
- Sternberg H., Nyquist C., Nilsson F. (2012), *Enhancing Security through Efficiency Focus – Insights from a Multiple Stakeholder Pilot Implementation*, “Journal of Business Logistics”, No. 33(1), s. 64-73.
- Svensson G. (2002), *A Conceptual Framework of Vulnerability in Firms’ Inbound and Outbound Logistics Flows*, “International Journal of Physical Distribution & Logistics Management”, Vol. 32, Iss. 2, s. 110-134.
- TAPA EMEA (2015), *The Cargo Crime Landscape in EMEA. Annual Report 2014*.
- United Nations (1982), *United Nations Convention on the Law of the Sea done in Montego Bay, 10.12.1982*, United Nations Treaty Series, Vol. 1833.
- Williams Z., Lueg J.E., LeMay S. (2008), *Supply Chain Security: An Overview and Research Agenda*, “The International Journal of Logistics Management”, Vol. 19, No. 2, s. 254-281.

**THE CHANGES IN THE AREA OF SUPPLY CHAIN SECURITY
IN 2001-2016**

Summary: The aim of this paper is to present the changes in the area of supply chain security in the years 2001-2016, with the emphasis on the new challenges from the environment of the supply chains, such as the increase of terrorist threat and migration crisis, which had a significant impact on the European countries and thus also on the companies operating in these countries. The analysis is based on statistical data from international databases and reports of international organizations on selected threats to supply chains, as well as on the results of surveys on supply chain security conducted using CATI (computer-aided telephone interviews) method, among Polish exporters and importers in 2013 and 2016. By comparing data and research results from different periods, it is possible to demonstrate the dynamic nature of security.

Keywords: supply chain security, terrorism, piracy, transportation security, threats.