Nr 1 (167) 2013

NOWOCZESNE TECHNOLOGIE WYKRYWANIA I ELIMINACJI ZAGROŻEŃ STOSOWANE W ŁAŃCUCHACH DOSTAW

Wiktor BIERNIKOWICZ*

* *Instytut Dowodzenia, Wyższa Szkoła Oficerska Wojsk Lądowych*
e-mail: w.biernikowicz@wso.wroc.pl

Artykuł wpłynął do redakcji 05.11.2012 r., Zweryfikowaną i poprawioną wersję po recenzjach i korekcie otrzymano w styczniu 2013 r.

W artykule przedstawione zostały główne zagrożenia występujące we współczesnych łańcuchach dostaw oraz technologie służące do ich wykrywania i eliminowania. Szczególną uwagę zwrócono na możliwości techniczne i zastosowania poszczególnych rozwiązań oraz korzyści wynikające z ich wdrażania.

Słowa kluczowe: *transport, bezpieczeństwo, łańcuch dostaw, kontener, monitorowanie ładunków, skanowanie kontenerów, terroryzm*

WSTĘP

W opinii wielu organizacji i ośrodków badawczych na całym świecie, zajmujących się analizą i zarządzaniem ryzykiem w transporcie, a także doradztwem w tym zakresie, do najpoważniejszych zagrożeń dla bezpieczeństwa handlu zaliczana jest niewątpliwie groźba przeprowadzenia zamachu terrorystycznego. Na kolejnych miejscach uplasowały się między innymi: piractwo morskie oraz zorganizowana przestępczość (przemyt narkotyków, handel bronią, podrabiane towary).

Działalność różnych ugrupowań oraz organizacji terrorystycznych ukierunkowana jest na osiągnięcie światowego rozgłosu oraz wywołanie „fali strachu'', stąd też do najczarniejszych scenariuszy zaliczany jest atak z użyciem broni masowego rażenia (np. broni biologicznej[1]), którego rezultatem byłaby olbrzymia liczba ofiar oraz trudne do oszacowania straty materialne[2]. Przykładem może być fakt, iż bezpośrednio po ataku na World Trade Center oraz Pentagon[3] wstrzymany został całkowicie transport lotniczy

[1] W opinii specjalistów wykrycie takiej przesyłki z uwagi na brak odpowiednich urządzeń jest najtrudniejsze (o wiele łatwiej wykryć materiały promieniotwórcze – czujniki promieniowania, czy też broń konwencjonalną – skanery).

[2] Straty poniesione w wyniku ataku na World Trade Center, oszacowane wyłącznie dla miasta Nowy Jork, oscylują w granicach 83 miliardów USD (o czym mówi raport opracowany we wrześniu 2002 r. przez City's Comptroller).

[3] W wyniku ataku z dnia 11 września 2001 r., przeprowadzonego przez al-Kaidę zginęło około 3 tysięcy ludzi (terroryści uprowadzili cztery samoloty pasażerskie, które następnie wykorzystane zostały ja-

oraz zamknięto wszystkie przejścia graniczne, co wywołało kryzys oraz wstrząsnęło całą amerykańską gospodarką. Zaatakowanie w tak dotkliwy sposób największego światowego mocarstwa pokazało, że nikt nie może dzisiaj czuć się bezpieczny, a poprawa bezpieczeństwa powinna stać się nadrzędnym celem dla każdego państwa. Akty terroru mogą dotknąć każdą gałąź transportu, co w dużym stopniu ułatwia stale rozwijający się transport intermodlany.

1. GENEZA PROBLEMU

Każdy atak niesie za sobą poważne skutki, które wpływają na wzrost cen transportu i towarów (odbudowa zniszczonej infrastruktury, ubezpieczenia, nowe technologie zwiększające bezpieczeństwo), ponadto istnieje duże ryzyko paraliżu komunikacyjnego lub też czasowego wstrzymania ruchu, co może wpływać negatywnie na stan światowej gospodarki.

Biorąc pod uwagę złożoność istniejących dzisiaj globalnych łańcuchów dostaw (duża liczba podmiotów biorących udział w wymianie handlowej, brak światowych standardów w dziedzinie zabezpieczeń, wymiany danych itp.), szczególnie przewozy kontenerowe narażone są na liczne zagrożenia. Błyskawiczny rozwój konteneryzacji doprowadził do tego, że skontrolowanie każdej jednostki ładunkowej nie jest dzisiaj możliwe. W efekcie dochodzi do licznych prób wykorzystania tych urządzeń transportowych przez środowiska przestępcze oraz organizacje terrorystyczne, a do najczęściej wymienianych wariantów ich działania zaliczyć można dwa:

- przejęcie legalnego kontenera i umieszczenie w nim własnego ładunku;
- wykorzystanie kontenera (tzw. „koń trojański'') do przewiezienia w sposób legalny, ukrytego i niebezpiecznego towaru (np. ładunek wybuchowy, broń biologiczna), a następnie jego detonacja na pokładzie statku lub też po przybyciu do portu rozładunku.

Opublikowany w lipcu 2003 r. raport GAO[4] na temat bezpieczeństwa rynku przewozów kontenerowych szacuje, że całkowity koszt dla amerykańskiej gospodarki wynikający z zamknięcia na okres 12 dni jednego portu morskiego (informacja o ukrytej broni masowego rażenia) wyniósłby około 58 miliardów dolarów (4,8 miliarda dolarów dziennie), natomiast skutki detonacji takiego ładunku kosztowałyby około 1 biliona dolarów[5].

Brak właściwej kontroli pozwala bardzo łatwo przemycić na pokład statku kontener zawierający ładunek wybuchowy, który następnie można wykorzystać do zorganizowania zamachu. Zdarza się również, że aktów terroru dopuszczają się pracownicy (kierowcy, robotnicy portowi) lub członkowie załogi statku, samolotu będący terrorystami albo też przez nich opłacani.

Zagrożenie atakami terrorystycznymi, także przy wykorzystaniu kontenerów, nabrało szczególnego wymiaru po wydarzeniach z dnia 11 września 2001 r., doprowadzając do zaostrzenia procedur celnych (np. obowiązek skanowania ładunków przyby-

ko narzędzie zamachu: dwa do ataku na wieże World Trade Center, jeden do ataku na Pentagon, a czwarty, który rozbił się w Pensylwanii prawdopodobnie miał uderzyć w Kapitol lub Biały Dom).

[4] United States Government Accountability Office.

[5] *Container Security Initiative, 2006-2011 Strategic Plan,* [in:] *U.S. Customs and Border Protection*, Washington 2006, s. 31.

wających do USA) oraz powstania nowych inicjatyw legislacyjnych zmierzających do poprawy bezpieczeństwa w transporcie. Do najważniejszych z nich zaliczyć można między innymi:

- Partnerstwo branży handlowej i celnej przeciwko terroryzmowi (C-TPAT);
- Inicjatywa Bezpieczeństwa Kontenerowego (CSI);
- Międzynarodowy Kodeks Ochrony Statków i Obiektów Portowych (ISPS);
- Upoważniony Przedsiębiorca (AEO)[6].

2. PRZEGLĄD NAJWAŻNIEJSZYCH TECHNOLOGII WYKRYWANIA I ELIMINACJI ZAGROŻEŃ STOSOWANYCH W ŁAŃCUCHACH DOSTAW

Obecnie na świecie dostępny jest szeroki wachlarz rozwiązań i urządzeń używanych do wykrywania wszechobecnych w transporcie zagrożeń.

Do najważniejszych i najskuteczniejszych stosowanych obecnie rozwiązań zalicza się:

- skanowanie ładunków;
- elektroniczne plomby;
- inteligentne kontenery;
- monitorowanie i śledzenie ładunków.

Można dyskutować na temat ich zalet i wad, ale nie można kwestionować jednego, bez nich o wiele trudniej byłoby wykryć niebezpieczny ładunek czy zapobiec kolejnym aktom terroru. Znamiennym jest również fakt, że każdy kolejny zamach wpływa na coraz większe zyski firm sektora zabezpieczeń, a branża ta stale się rozwija.

2.1. Skanowanie ładunków

Analizując najczęściej stosowane sposoby przeprowadzania kontroli ładunków (kontenerów, pojazdów), możemy rozróżnić dwa podstawowe:

- tradycyjne (polegające na kontroli fizycznej) – inwazyjne, wymagające otwarcia kontenera oraz czasochłonne[7];
- przy użyciu skanerów – nieinwazyjne, pojazd (samochód, pociąg) może być w ruchu, a także zdecydowanie szybsze i dokładniejsze.

Biorąc pod uwagę dostępne obecnie na rynku modele skanerów, według kryterium wykorzystywanego do prześwietlania źródła promieniowania, możemy je podzielić na urządzenia wykorzystujące:

- promieniowanie gamma;
- promieniowanie rentgenowskie;
- wiązki neutronowe.

---

[6] W. Biernikowicz, T. Smal, *Nowe standardy bezpieczeństwa na rynku przewozów kontenerowych,* [w:] *Edukacja dla bezpieczeństwa*, WSB 2008, s. 491.

[7] Według różnych źródeł czas potrzebny na fizyczne skontrolowanie kontenera wynosi od 4-8 godzin i wymaga pracy kilku osób używających specjalistycznych narzędzi, podczas gdy jego skanowanie trwa zaledwie kilka minut.

Ponadto z uwagi na przeznaczenie oraz wydajność pracy dzielą się one na przenośne (mobilne) i stacjonarne.

Skanery wykorzystujące promieniowanie gamma oferowane są przez wielu producentów i znajdują szerokie zastosowanie z uwagi na dużą precyzję oraz stosunkowo niewielki koszt. Dodatkowo wykorzystują one mniejszą w porównaniu ze skanerami rentgenowskimi dawkę napromieniowania i są od nich szybsze. Ukazywany przez skaner obraz umożliwia operatorowi rozpoznanie kształt ładunku, co pozwala zauważyć ukryte w środku przedmioty. Dzięki swoim właściwościom skanery te dają 100 % gwarancję inspekcji całej powierzchni, bez pozostawiania tzw. „czarnych plam''. Urządzenia posiadają także zintegrowane czujniki promieniowania, co umożliwia wykrycie źródeł promieniowania. Biorąc pod uwagą przeznaczenie i możliwości tego typu skanerów, możemy je podzielić na :

- urządzenia mobilne (mobile systems) do prześwietlania pojazdów i kontenerów będących w ruchu;
- urządzenia stacjonarne (portal systems) – skanowanie kontenerów w portach morskich.

Jednym z największych producentów skanerów jest firma RAPISCAN Systems, producent między innymi urządzenia o nazwie Rapiscan GaRDS Portal, którego możliwości przedstawia poniższa tabela.

Tabela 1. Możliwości techniczne urządzenia RAPISCAN GaRDS Portal

RAPISCAN GaRDS Portal	
przepustowość	1-3 samochodów ciężarowych na minutę
prędkość skanowania	ok. 2 mile na godzinę
penetracja (stal)	do 190 mm
wydajność	do 120 pojazdów (kontenerów)/godzinę
źródło promieniowania	kobalt-60/ cez-137
maks. wymiary skanowanego pojazdu	wysokość - 4,5m, szerokość - 3m

Źródło: Opracowanie własne na podstawie danych producenta

Skanery wykorzystujące promieniowanie rentgenowskie służą, podobnie jak opisywane wcześniej urządzenia do prześwietlania cargo, pokazując różnice gęstości (kontrast wyświetlanego obrazu) przewożonych towarów. Skanowany obraz jest przetwarzany przez specjalne oprogramowanie komputerowe, co pozwala operatorowi na jego obróbkę, powiększenie oraz wydruk i archiwizację. Decydującym o skuteczności działania czynnikiem jest stopień wyszkolenia operatora, który musi być wyczulony na obserwowane zmiany i precyzyjnie je interpretować (w przypadku promieniowania gamma, analizą zawartości zajmuje się komputer, który alarmuje o ewentualnym zagrożeniu). Przykładem takiego skanera może być prezentowany poniżej skaner RAPISCAN Eagle M4500 (rys.1).

Skanery wykorzystujące wiązki neutronowe są urządzeniami do automatycznego wykrywania zagrożeń w postaci materiałów wybuchowych, źródeł promieniowania oraz sprawdzania zawartości jednostek ładunkowych. Pozwalają one wykryć zagrożenie niezależnie od kształtu niebezpiecznego przedmiotu (np. plastycznego materiału wybuchowego, który może zostać sformowany w dowolny kształt) oraz miejsca jego ukrycia, czym przewyższają opisywane wcześniej skanery. Emitowane przez urządzenie i wysy-

łane z różną prędkością wiązki neutronowe pobudzają skanowany ładunek i reagują na obecne źródła promieniowania gamma. Odebrane sygnały pozwalają wykryć ewentualne zagrożenie (porównanie z zagrożeniami opisanymi w bazie danych), ustalić dawkę promieniowania, rodzaj materiału oraz precyzyjnie zlokalizować jego położenie, tworząc w razie wykrycia zagrożenia trójwymiarowy obraz.

Urządzenia tego typu znajdują zastosowanie zarówno w portach morskich, jak i na lotniskach, a także na przejściach granicznych (np. granica amerykańsko-meksykańska). Niektóre instytucje rządowe oraz armie wykorzystują mobilne skanery (ukryte we wnętrzu zaparkowanego obok ulicy lub budynku pojazdu) do prześwietlania przejeżdżających obok pojazdów, co pozwala w sposób niezauważony podnieść bezpieczeństwo oraz zredukować ryzyko przeprowadzenia zamachu.

Rys. 1. Mobilny system Rapiscan Eagle M4500
Źródło: [online] [dostęp: 02.08.2010]. Dostępny w Internecie: http/www.rapiscansystems.com/datasheets/Rapiscan_EagleM4500 Series_Screen.Pdf

2.2. Elektroniczne plomby (e-seals)

Głównym zadaniem tych zabezpieczeń jest uniemożliwienie otwarcia kontenera przez osoby nieupoważnione (próba mechanicznego usunięcia plomby powoduje przerwanie obwodu elektronicznego i wysłanie powiadomienie o włamaniu), a także szybka identyfikacja kontenera. W porównaniu z tradycyjnymi plombami (np. z ołowiu), niezauważone usunięcie e- plomby nie jest możliwe.

Możemy wyróżnić następujące typy elektronicznych plomb:

- jednorazowego użytku (disposable) – najtańsze, zawierające jedynie takie informacje, jak przypisany seryjny numer ID oraz status bezpieczeństwa;
- wielokrotnego użytku (reusable) – droższe od jednorazowych, które zawierają oprócz wymienionych wcześniej danych, informacje na temat użytkownika, położenia, czasu, daty oraz wskaźnik zużycia baterii;
- zaawansowane technologicznie urządzenia do rejestrowania otwarcia drzwi kontenera oraz monitorowania zachodzących zmian środowiskowych, które umieszczane są wewnątrz kontenera (dodatkowo na zewnątrz stosowane są wytrzymałe plomby).

Jednocześnie dzięki połączeniu tej technologii z tagami RFID[8] oraz wykorzystaniu łączności satelitarnej i GPS możliwe jest monitorowanie położenia przesyłki oraz komunikowanie się z serwerem centralnym (zapewniony dostęp do internetu).

2.3. Inteligentne kontenery (smart containers)

Termin ten został zarezerwowany dla kontenerów, które wyposażono w szereg urządzeń i czujników pozwalających na monitorowanie zachodzących zmian środowiskowych (np. temperatury, wilgotności), reagujących i alarmujących o nieuprawnionym otwarciu drzwi oraz umożliwiających, dzięki technologii RFID/GPS/GSM, określenie pozycji oraz śledzenie położenie w ruchu.

Urządzenia te mogą się różnić pod względem posiadanych możliwości, ale zasadniczo zadaniem każdego ,,inteligentnego kontenera'' jest wykrywanie i rejestrowanie zmian (zjawisk) oraz powiadamianie o nich.

Bardziej zaawansowane modele będą informowały i raportowały w zakresie szerszych danych (zawartość kontenera – cargo manifest, dane nadawcy i odbiorcy, przewoźnika, położenie, odchylenie od trasy, przybycie do punktu przeznaczenia), natomiast te najprostsze przekażą jedynie informację o otwarciu drzwi.

Do podstawowych korzyści wynikających ze stosowania ,,inteligentnych kontenerów'' należą: ograniczenie liczby kradzieży, poprawa bezpieczeństwa łańcuchów dostaw, skrócenie czasu transportu. Ponadto ich użytkownicy mogą liczyć na przywileje w postaci łagodniejszego traktowania przez służby celne (szybsze odprawy celne, uproszczone procedury). Istnieją również raporty, które dowodzą, że rozwój tej technologii może w znaczący sposób zwiększyć bezpieczeństwo łańcucha dostaw, przynosząc z tego tytułu duże zyski. Według opracowanego przez The Homeland Security Research Group raportu, którego wyniki przytoczono poniżej (patrz rysunek nr 2) przewidywany jest intensywny rozwój technologii zwiększających bezpieczeństwo przewozów kontenerowych, a prognozowane dochody z tego typu działalności w przeciągu 7 lat (2006–2012) wzrosły z poziomu 70 milionów USD w 2006r. do około 4,2 miliarda USD w roku 2012[9].

Niektórzy operatorzy logistyczni, tacy jak Schenker, wdrażają i testują własne rozwiązania, np. Schenker Smartbox (wspólny projekt z Cisco oraz Intermec)[10]. Wyniki pierwszych testów przeprowadzonych w 2007 roku z udziałem 10 ,,inteligentnych kontenerów'', na trasie Hamburg – Hong Kong zaowocowały kolejnymi większymi wdrożeniami. Wykorzystywane przez tego niemieckiego operatora rozwiązanie służy do monitorowania parametrów ładunku oraz jego lokalizacji, łącząc w sobie możliwości zarówno RFID oraz GPS, co umożliwia przesyłanie w stałych interwałach czasowych informacji o kondycji ładunku (zmiany temperatury, wstrząsy) oraz szybką lokalizację. Tradycyjne plomby zostały zastąpione przez e-seals, gwarantując możliwość podjęcia odpowiedniej i szybkiej reakcji w razie otwarcia kontenera. Informacje na temat po-

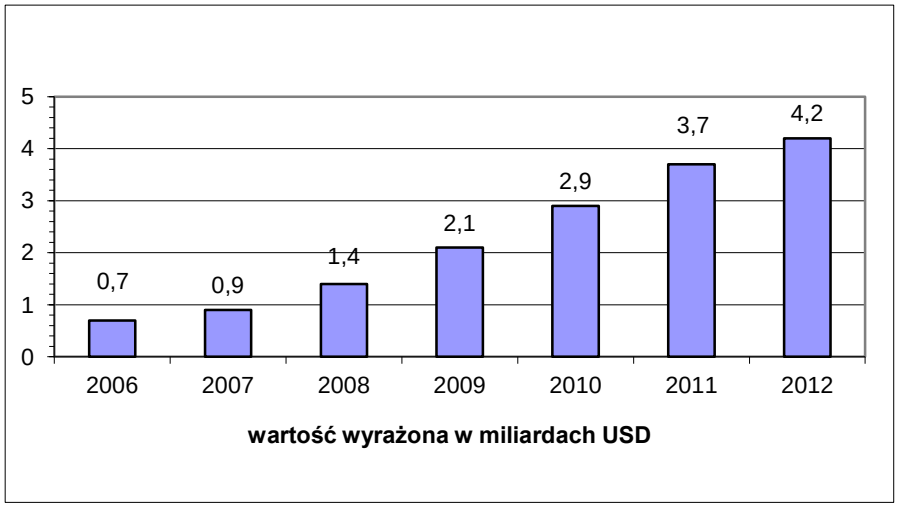
---

[8] Radio Frequency Identyfication (RFID) – system kontroli przepływu towarów w oparciu o zdalny zapis i odczyt danych (poprzez fale radiowe) z wykorzystaniem specjalnych układów elektronicznych (tagów) przytwierdzonych do monitorowanych towarów.

[9] J. Giermanski, *Tapping the Potential of smart containers,* [in:] *Supply Chain Management Review*, January/February 2008, s. 38.

[10] [online]. [dostęp: 04.02.2009r.]. Dostępny w Internecie: http://www.logasiamag.com/article-52-schenkerrfidgpscontainersecuritysolution-LogisticsAsia.html.

szczególnych kontenerów dostępne są poprzez portal internetowy, po wcześniejszym zalogowaniu.



Rys. 2. Rozwój rynku inteligentnych kontenerów w latach 2006-2012

Źródło: Opracowanie własne na podstawie raportu Homeland Security Research Group

Własne rozwiązanie do śledzenia przesyłki w czasie rzeczywistym oraz kontroli wybranych parametrów opracowali wspólnie inni potentaci (IMB oraz MAERSK Logistics). Urządzenie o nazwie TREC (Tamper-Resistant Embedded Controller), przymocowane jest do kontenera na podobnej zasadzie jak aktywny tag RFID, ale w przeciwieństwie do niego nie wymaga utworzenia całej sieci czytników rejestrujących sygnał. Zamiast tego komunikuje się wysyłając zakodowane dane wykorzystując w tym celu urządzenia bezprzewodowe (sieć satelitarna Iridium, sieć komórkowa, GPS). Pozostałe informacje rejestrowane są przez małe tagi RFID (ZigBee) połączone z różnymi sensorami, które współpracują z urządzeniem TREC, a następnie udostępniane użytkownikom kontenerów poprzez specjalny portal. Trwające miesiąc testy (10 kontenerów) zakończyły się próbą z udziałem 1000 urządzeń (testy trwały 4 miesiące), a następnie po przeanalizowaniu rezultatów zapadła decyzja o seryjnej produkcji gotowego produktu[11].

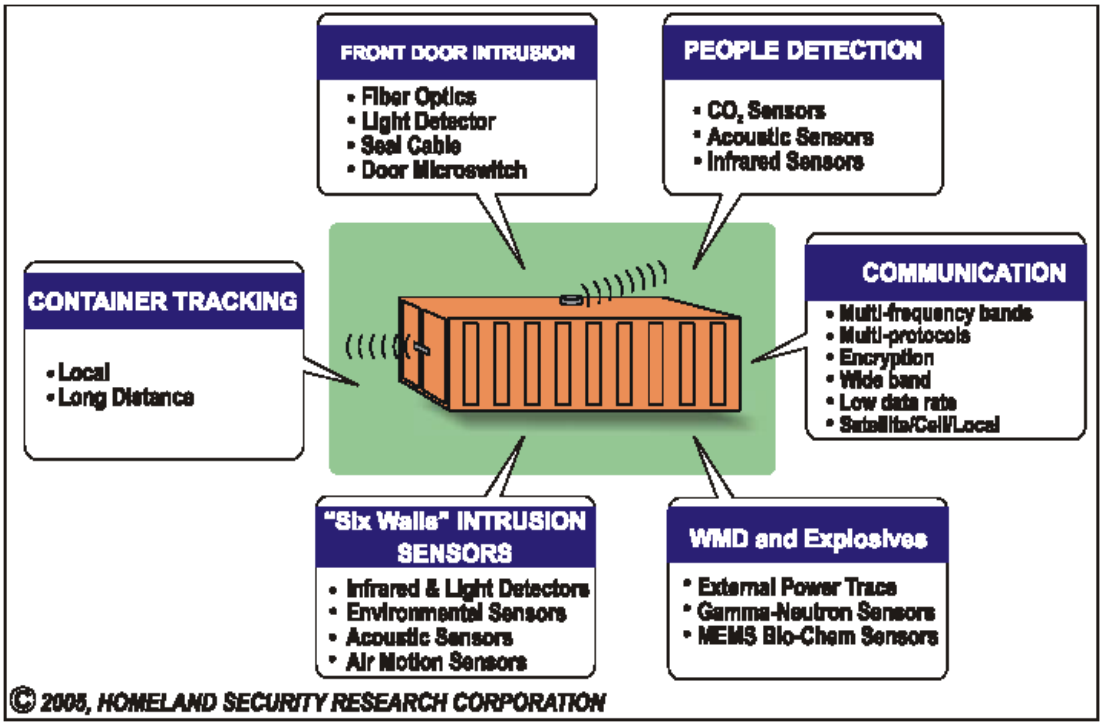
Pomimo imponujących możliwości technicznych w zakresie śledzenia kontenerów oraz wykrywania zagrożeń i monitorowania zachodzących zmian środowiskowych nadal trwają prace nad opracowaniem światowego standardu (zakres kontroli, standardy wymiany danych, częstotliwości). Próbę wytyczenia pewnego wzorca podejmuje poniższy projekt (rys. 3).

2.4. Monitorowanie i śledzenie ładunków

Brak możliwości śledzenia przesyłek w czasie rzeczywistym w dużym stopniu utrudnia sprawne zarządzanie łańcuchem dostaw, co nabiera szczególnego znaczenia w przypadku przewożenia produktów wrażliwych, towarów niebezpiecznych oraz przesyłek wartościowych. Informacja o ostatniej lokalizacji, jaką zapewnia RFID jest niewystarczająca. Monitorowanie ładunku w ruchu bywa zatem często ograniczone do jego rejestracji w punktach kontrolnych (np. czytniki stacjonarne w portach morskich, ba-

[11] [online]. [dostęp: 03.02.2009 r.]. Dostępny w Internecie: http://www.rfidjournal.com/article/view/1884/1/1.

zach) rozmieszczonych wzdłuż trasy w celu dokonania odczytu (identyfikacji), w ustalonych interwałach czasowych[12]. Brakuje natomiast informacji na temat przesyłki w czasie przemieszczania pomiędzy tymi punktami.



Rys. 3. Inteligentny kontener nowej generacji

Źródło: [online]. [dostęp: 22.09.2010 r.]. Dostępny w Internecie: http://hsrc.biz/researchreports.html.

Dlatego, aby uzyskać zdolność do śledzenia ładunków w czasie rzeczywistym należy połączyć technologię RFID z GPS/GSM, a także wprowadzić do eksploatacji tzw. inteligentne kontenery. Wdrożenie RFID w transporcie powinno polegać głównie na wykorzystaniu aktywnych tagów, które w przeciwieństwie do tagów pasywnych[13] posiadają własne zasilanie (bateria) oraz charakteryzują się dużą odległością odczytu (ok.100 m). Dzięki stosowaniu tagów aktywnych (np. na pierwszym i ostatnim pojeździe w kolumnie[14]) możliwy jest ich odczyt bez konieczności zatrzymywania kolumn pojazdów (konwojów) nawet przy prędkościach ok. 100 km/h. Kiedy etykieta radiowa

[12] Jednym z największych na świecie użytkowników technologii RFID jest armia amerykańska, która wykorzystuje ją podczas operacji prowadzonych między innymi w Iraku czy też w Afganistanie. Monitorowanie przesyłek według standardów obowiązujących w NATO (STANAG 2184) polega na przekazywaniu do centralnej bazy danych (Central Consignment Tracking Base) meldunków z informacjami o miejscu i czasie wysłania przesyłki, przejazdu przez punkty pośrednie oraz jej dostarczenia. Ponadto składane są meldunki o odchyleniach od planu przewozu i o zdarzeniach losowych. Punkty meldunkowe powinny być tak rozmieszczone aby czas między kolejnymi meldunkami nie przekraczał: dla transportu powietrznego – 1 godz., dla transportu drogą lądową – 6 godz., dla transportu drogą morską – 24 godzin.

[13] Tagi pasywne nie posiadają zasilania, a energię czerpią z czytnika i działają na zasadzie ,,fali odbitej'' – odczyt może odbywać się tylko na odległość do kilku metrów.

[14] Zasada ta obowiązuje w armii amerykańskiej.

znajdzie się w zasięgu pola emitowanego przez czytnik następuje automatyczny odczyt. Dane znajdujące się w pamięci procesora umieszczonego w tagu przesyłane są do czytnika, skąd trafiają do komputera, a następnie poprzez Internet do serwera centralnego. Częstotliwości fal radiowych wykorzystywanych w logistyce mieszczą się zazwyczaj w paśmie UHF (aktywne tagi RFID – zgodność z normą ISO 18000-7). Etykiety aktywne używane są powszechnie do znakowania: pojazdów, kontenerów transportowych, palet lotniczych.

Przytaczana wcześniej jako przykład armia amerykańska posiada na wyposażeniu specjalne mobilne punkty kontrolne, które wykorzystywane są w sytuacji braku dostępu do istniejącej infrastruktury logistycznej (misje, operacje). Pozwalają one na wydłużenie łańcucha dostaw, umożliwiając tym samym monitorowanie przepływu zaopatrzenia na teatrze działań, w szczególności tam, gdzie nie ma stałych czytników RFID oraz dostępu do Internetu (z dala od baz, portów i lotnisk). Przykładem takiego urządzenia jest oferowany przez firmę Savi Technology zestaw o nazwie PDK (Portable Deployment Kit) – składający się z walizki, w której znajdują się: laptop, modem GPS oraz Iridium[15], ręczny czytnik RFID i drukarka etykiet. Ponadto zestawy wyposażone są we własne zasilanie (panel słoneczny). Odczyt tagów jest uzupełniony o podanie koordynatów (pozycjonowanie za pomocą GPS), a następnie poprzez łącza satelitarne (Iridium) informacja ta wysyłana jest do jednego z czterech serwerów ITV na świecie (Azja, Europa, USA, Pacyfik). Dzięki dostępowi do internetu (ITV[16] Web portal), dowódcy mogą śledzić położenie wysyłanego zaopatrzenia oraz podejmować optymalne decyzje. Warto także w tym miejscu zauważyć, że Departament Obrony USA (U.S. Department of Defense – DoD) stworzył do obsługi własnego łańcucha dostaw największą działającą dzisiaj na świecie sieć monitorowania przesyłek będących w ruchu (w oparciu o aktywne tagi RFID). Obejmuje ona swoim zasięgiem około 40 państw położonych na różnych kontynentach, a kluczowe dla systemu elementy (stałe czytniki, mobilne punkty kontrolne) znajdują się w ponad 4000 miejsc na świecie (porty morskie, lotniska, składy polowe, terminale przeładunkowe), co umożliwia monitorowanie ponad 35 tys. przesyłek dziennie[17]. Informacje mogą być wzbogacone poprzez element wizualizacji (mapy cyfrowe), co pozwala sprawniej zarządzać przesyłkami. Wysyłając zapytanie (podając numer ID przyporządkowany konkretnemu znacznikowi, np. Tag # 5539210) możemy uzyskać informację o jego aktualnym położeniu oraz odtworzyć trasę przejazdu. Ponadto w razie odchylenia od trasy możemy ustalić, kiedy i gdzie doszło do zmiany[18]. Oprócz samego numeru, bardziej zaawansowane aktywne etykiety RFID[19] mogą dostarczać szczegółowych informacji, dotyczące np. zawartości kontenera. Dzięki temu możliwe jest sprawne podejmowanie decyzji w czasie rzeczywistym (lub zbliżonym), a także sprawne kierowanie ruchem w sposób bezkolizyjny (możliwość skiero-

[15] Operator telefonii satelitarnej (Iridium Satellite LLC), którego system łączności satelitarnej (66 satelitów komunikacyjnych, a po wypadku z dn. 10.02.2009r. już tylko 65) obejmuje swoim zasięgiem praktycznie cały glob włączając obszar oceanów oraz Arktykę.

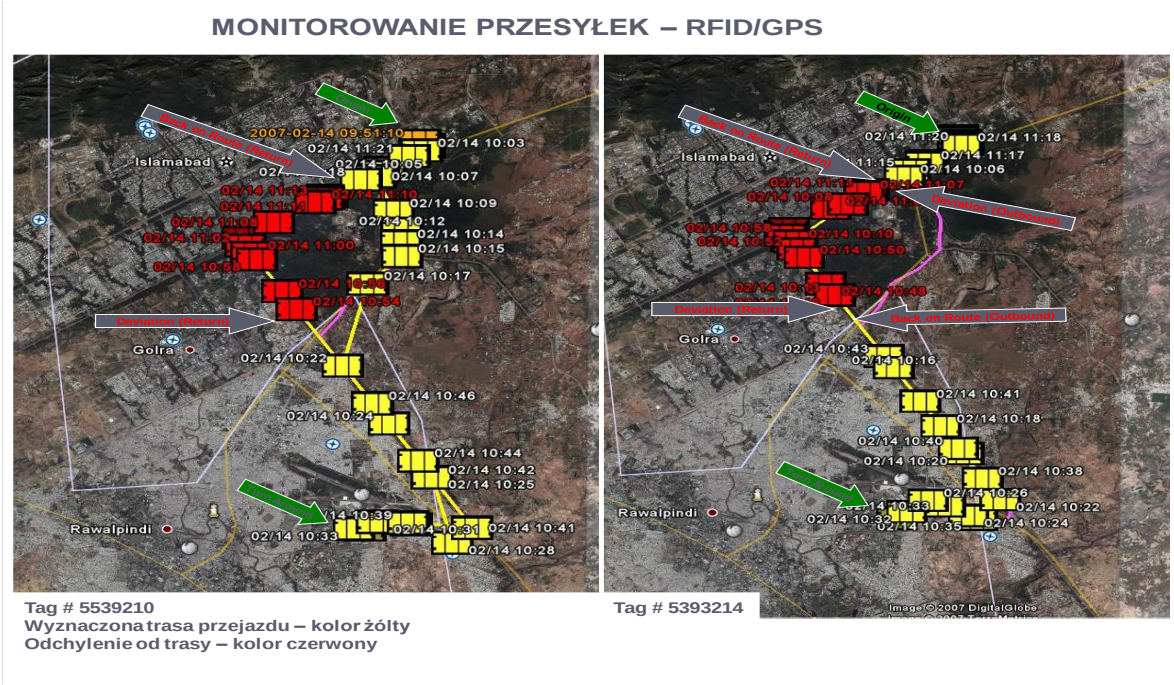
[16] In Transit – Visibility (możliwość śledzenia położenia pojazdu, kontenera będącego w ruchu).

[17] [online]. [dostęp: 02.02.2009]. Dostępny w Internecie: http://www.savi.com/capabilities/ solutions/in-transit-visibility.html.

[18] Patrz w: W. Biernikowicz, *Wykorzystanie technologii RFID do monitorowania ładunków w łańcuchu dostaw*, [w:] „Logistyka", nr 2/2009, wersja elektroniczna CD Nr 2.

[19] Dysponujące większą pojemnością, np. 128 kB – Tag 654 firmy Savi (co odpowiada objętości ok. 80 stron tekstu).

wania na inną drogę – celem np. objazdu przeszkody), wykluczający zjawisko kongestii transportowej. Przykładem takiego rozwiązania jest stosowany przez wojska koalicji w Afganistanie system śledzenia pojazdów/ładunków w ruchu RF-ITV (Radio Frequency - In Transit Visibility), co przedstawia poniższy rysunek nr 4. Do innych korzyści oferowanych przez radiową identyfikację zaliczyć można wykorzystywane w transporcie lotniczym oraz wojsku urządzenia pozwalające na identyfikację poszczególnych pojazdów, samolotów, co w przypadku działań wojennych pozwala na uniknięcie omyłkowego zestrzelenia np. przez własne środki ogniowe[20]. Kolejnym innowacyjnym zastosowaniem może być użycie aktywnych tagów RFID do oznakowania trasy przejazdu. Ukryte w newralgicznych punktach (np. skrzyżowania) tagi mogłyby służyć jako niewidoczne drogowskazy dla dowódców kolumn używających ręcznych czytników wysyłających ,,zapytanie''.



Rys. 4. Graficzne odwzorowanie trasy przejazdu na mapie cyfrowej

Źródło: [online]. [dostęp: 02.02.2012]. Dostępny w Internecie: www.savi.com

Przedstawione wcześniej niewątpliwie duże korzyści oferowane przez RFID nie powinny jednak pozostawić bez odpowiedzi następującej kwestii – bezpieczeństwa przesyłanych danych oraz możliwości zakłócenia przesyłanego sygnału przez inne urządzenia. Specjaliści (głównie wojskowi), zastanawiają się czy możliwe jest wykorzystanie znanej i stosowanej standardowo częstotliwości do detonacji tą drogą np. umieszczonego w kontenerze ładunku wybuchowego, którego wybuch nastąpiłby w momencie odczytu przez skaner np. w porcie morskim.

[20] Współczesna technologia RFID wywodzi się od opracowanego w 1939 roku w Wielkiej Brytanii i wykorzystanego po raz pierwszy podczas II wojny światowej systemu identyfikacji radiowej na bazie transponderów radiowych dużej mocy, który przy złych warunkach pogodowych służył do identyfikacji samolotów bojowych (tzw. IFF – Identyfication Friend Or Foe).

Problemem braku światowych standardów w zakresie używanych częstotliwości doprowadził do powstania opisującego to zjawisko terminu „wojna częstotliwości'', który ukazuje, jak wiele jeszcze pozostało w tym względzie do zrobienia. Istnieją bowiem rozbieżności, co do stosowanych standardów zarówno w USA, jak i w Europie oraz w Azji, co powinno zostać jak najszybciej uregulowane.

Kolejnym problemem jest również stosunkowo duży koszt, który powoduje, iż nie jest to technologia stosowana masowo. Niemniej jednak wraz z kolejnymi wdrożeniami koszty są coraz mniejsze, co można zauważyć na przykładzie malejących cen tagów, które kształtują się obecnie na poziomie od 20 do 5 centów za sztukę[21]). Duży wpływ na rozwój tej technologii, wywierają inicjatywy legislacyjne i wymagania branżowe, np. dyrektywa UE nr 178/2002[22], która od 1 stycznia 2005 roku nakłada w UE obowiązek znakowania i śledzenia (tzw. tracebility) towarów spożywczych, półproduktów i ich składników oraz pasz, co wymaga stosowania etykiety logistycznej i kodów kreskowych lub EPC (Electronic Product Code) i technologii RFID w celu rejestracji numerów jednostek wysyłkowych.

PODSUMOWANIE

Przedstawiona w artykule problematyka ukazuje olbrzymią złożoność problemu zapewnienia bezpieczeństwa w łańcuchach dostaw oraz wysiłki podejmowane w związku z realizacją tego celu.

Zaprezentowane rozwiązania pozwalają zrozumieć ogromną determinację poszczególnych rządów oraz instytucji i podmiotów działających na rynku związaną z ich wdrażaniem, zwłaszcza w kontekście wyszczególnionych realnych zagrożeń. Wskazane zostały również wymierne korzyści wynikające ze stosowania wymienionych procedur i zabezpieczeń, a w szczególności: skrócenie czasu transportu, uproszczenie procedur celnych, możliwość lokalizacji ładunku, odtworzenia trasy przemieszczenia oraz wpływania na zachodzące w czasie przewozu zmiany i nieprawidłowości.

Oprócz typowych praktycznych zastosowań zwrócono uwagą na innowacyjność poszczególnych rozwiązań, wskazując potencjalne obszary zastosowań oraz dalsze kierunki prac nad możliwościami rozwoju tych stosunkowo nowoczesnych technologii.

LITERATURA:

1. Biernikowicz W., Smal T., *Nowe standardy bezpieczeństwa na rynku przewozów kontenerowych*, [w:] *Edukacja dla bezpieczeństwa*, WSB 2008, s. 493.
2. Biernikowicz W., *Wykorzystanie technologii RFID do monitorowania ładunków w łańcuchu dostaw*, [w:] „Logistyka", nr 2/2009, wersja elektroniczna CD Nr 2.
3. [online]. [dostęp: 04.02.2009r.]. Dostępny w Internecie: http://www.logasiamag.com/article-52-schenkerrfidgpscontainersecuritysolution-LogisticsAsia.html.

[21] S. Beth, D. Burth, W. Copacino, C. Gopal, H.L. Lee, R.Porter Lynch, S. Morris, *Budowanie relacji w ramach łańcucha dostaw*, Harvard Business Review, Zarządzanie łańcuchem dostaw, Helion 2007.

[22] Rozporządzenie WE nr 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 roku ustanawiające ogólne zasady i wymagania prawa żywnościowego, powołujące Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiające procedury w zakresie bezpieczeństwa żywności.

4. [online]. [dostęp: 02.08.2010r.]. Dostępny w Internecie: http://www.rapiscansystems .com/datasheets/ Rapiscan_GaRDSPortal_Screen.Pdf.
5. [online]. [dostęp: 02.08.2010r.]. Dostępny w Internecie: http://www.rapiscansystems. com /datasheets/Rapiscan_Eagle M45Series_Screen.Pdf.
6. [online]. [dostęp: 18.08.2012r.]. Dostępny w Internecie: http://www.cbp.gov/xp/ CustomsToday/2003/December/smart_box_sidebar.xml.
7. Giermanski J., *Tapping the Potential of smart containers*, [in:] „Supply Chain Management Review", January/February 2008, s. 38.
8. [online]. [dostęp: 02.02.2019r.]. Dostępny w Internecie: http://www.rfidjournal.com /article/view/1884/1/1.
9. [online]. [dostęp: 22.09.2010r.]. Dostępny w Internecie: http://hsrc.biz/researchrep orts.html.
10. Rozporządzenie WE nr 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 roku ustanawiające ogólne zasady i wymagania prawa żywnościowego, powołujące Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiające procedury w zakresie bezpieczeństwa żywności.
11. [online]. [dostęp: 27.09.2010r.]. Dostępny w Internecie: http://www.savi.com/ capabilities/solutions/in-transit-visibility.html.
12. *STANAG 2184* – Zasady i procedury śledzenia zasobów.
13. Beth S., Burth D., Copacino W., Gopal C., Lee H.L., Porter Lynch R., Morris S., *Budowanie relacji w ramach łańcucha dostaw*, [w:] „Harvard Business Review", Zarządzanie łańcuchem dostaw, Helion 2007.

NEW TECHNOLOGIES OF THREATS DETECTION AND ELIMINATION IN SUPPLY CHAINS

Summary

The purpose of this article is to describe the main threats to contemporary supply chains security and the new technologies of their detection and elimination. In particular, the article explores the technical capabilities and use of possible solutions as well as the benefits connected with their implementation.

Keywords: *transport, security, supply chain, container, cargo tracking, container scanning, terrorism*