ZESZYTY NAUKOWE AKADEMII MARYNARKI WOJENNEJ
ROK XLIX NR 2 (173) 2008

**Joanna Jedel**
**Akademia Marynarki Wojennej**

# CYBERPRZESTRZEŃ NOWĄ PŁASZCZYZNĄ ZAGROŻEŃ TERRORYSTYCZNYCH DLA MORSKICH CENTRÓW LOGISTYCZNYCH

## STRESZCZENIE

Celem niniejszego artykułu jest prezentacja i analiza potencjalnych zagrożeń, jakie niesie za sobą cyberatak na porty morskie wraz z otaczającą infrastrukturą komunikacyjną. Kierunkiem ekspansji przestrzennej portów morskich stają się morskie centra logistyczne wraz z systemem zarządzania transportem międzynarodowym, które mogą stanowić potencjalny cel cyberataku terrorystycznego.

Słowa kluczowe:
cyberprzestrzeń, cyberterroryzm, cyberatak, morskie centra logistyczne.

## WSTĘP

Terroryzm jest największym globalnym zagrożeniem XXI wieku, a obecnie ataki terrorystyczne stanowią potwierdzenie istnienia tego faktu. Kiedy 11 września naruszono poczucie bezpieczeństwa jednego z największych mocarstw świata — Stanów Zjednoczonych, a wraz z nimi ich sojuszników — problem terroryzmu nabrał międzynarodowego i globalnego rozgłosu, stając się dla współczesnego świata zagrożeniem o wymiarze ekonomicznym, finansowym oraz społecznym.

## NOWY OBSZAR DZIAŁALNOŚCI LUDZKIEJ

Dzisiaj nowoczesne techniki komunikacji, technologie informatyczne oraz media elektroniczne odgrywają zasadniczą rolę w tworzeniu nowej globalnej płaszczyzny funkcjonowania świata. Równoległą płaszczyzną, na której funkcjonuje

nasza cywilizacja, jest Internet. Każda forma działalności w Internecie ma globalny zasięg, zwany w środowisku internautów cyberprzestrzenią[1].

Cyberprzestrzeń w ogólnym znaczeniu tego słowa to: „Przestrzeń komunikacyjna tworzona przez system powiązań internetowych. Jest przestrzenią otwartego komunikowania się za pośrednictwem połączonych komputerów i powiązań informatycznych pracujących na całym świecie”[2]. Definicja ta uwzględnia wszystkie systemy komunikacji elektronicznej (w tym również klasyczne sieci telefoniczne). „Cyberprzestrzeń, definiowana jako integralny składnik realnego świata, w którym koegzystują ze sobą i zwalczają się wzajemnie najrozmaitsze ideologie i podkultury, jest nie tylko miejscem wymiany i rozpowszechniania informacji, lecz także polem walki, terenem, na którym podejmowane są skoordynowane akcje o zabarwieniu politycznym o mniej lub bardziej destrukcyjnym charakterze”[3]. Cyberprzestrzeń jest zatem podstawowym kanałem wymiany informacji. Internet jako jeden z efektów technologii informatycznych otworzył przed organizacjami rządowymi, pozarządowymi i prywatnymi instytucjami, a także przed osobami fizycznymi nowe możliwości globalnej współpracy. Dane przesyłane za pośrednictwem Internetu mają zasięg światowy. Funkcjonowanie w cyberprzestrzeni przynosi oszczędność czasu oraz szereg korzyści ekonomicznych i społecznych.

Transport i logistyka są także objęte siecią cyberprzestrzeni niezbędną w tym przypadku do zarządzania. Sektor ten to jeden z kluczowych sektorów polskiej gospodarki, z przychodami rzędu 100 mld zł, blisko 5-procentowym udziałem w PKB, zatrudniający 400 tysięcy pracowników. Wzrost gospodarczy i rosnąca w skali globalnej wymiana handlowa powodują dynamiczny rozwój rynku transportu. Nieustająca presja na redukcję kosztów i coraz powszechniejsza tendencja wśród przedsiębiorstw do koncentracji na działalności kluczowej sprawiają, że funkcje transportowe i logistyczne coraz częściej powierzane są wyspecjalizowanym firmom działającym w centrach logistycznych, co prowadzi do szybkiego wzrostu popytu na wszelkiego rodzaju usługi logistyczne i transportowe[4]. Międzynarodowa wymiana handlowa i usługi transportowe to również obiecująca oraz

[1] K. Wach, *Internet jako środek promocji oraz element konkurencyjności firm w dobie globalizacji*, http://www.zti.com.pl/instytut/pp/referaty/ref5_full.html z 25.01.2008.

[2] *Słownik internetowy*, http://www.i-slownik.pl/1,323,cyberprzestrzen.html z 02.12.2007.

[3] A. Adamski, *Cyberterroryzm*, Wydział Prawa i Administracji UMK w Toruniu, Katedra Prawa Karnego i Polityki Kryminalnej, http://unixlab.iis.pwsz.elblag.pl/~stojek/bezp.sys.komp/cyberterroryzm.pdf z 25.01.2008.

[4] Urząd Komitetu Integracji Europejskiej, raport *Rynek transportu i logistyki w Polsce*, http://www.ukie.gov.pl/www/serce.nsf/0/913169EE954C46C1C12572F10047AF72?Open z 02.02.2008.

błyskawicznie rozwijająca się płaszczyzna Internetu. Internet jest miejscem działalności gospodarczej, zarówno handlowej (sprzedaży i aukcji), jak i usługowej (logistyka, bankowość internetowa, ubezpieczenia), dlatego też zamachy terrorystyczne zaczęły obejmować nową formę, zastępując klasyczną, otwartą konfrontację militarną niekonwencjonalną formą walki w cyberprzestrzeni. Cyberataki są przez terrorystów skrupulatnie przygotowywane i potrafią w krótkim czasie wywołać całe spektrum szkód materialnych i strat finansowych prowadzących do destabilizacji zaatakowanego państwa. Organizacje terrorystyczne XXI wieku sięgają coraz częściej po niekonwencjonalne formy walki, jaką jest cyberatak. Ataki w cyberprzestrzeni nie są działaniami wymagającymi wysokich nakładów finansowych, natomiast wywołują ogromne straty ekonomiczne i są działaniami trudnymi do udowodnienia. Na uwagę zasługuje fakt, że nadal brakuje międzynarodowych, jednolitych regulacji prawnych umożliwiających ukaranie sprawców.

Internet to również baza zgromadzonych informacji dotycząca potencjalnych obiektów, na które ma zostać przeprowadzony atak. Stanowi podstawę do wyboru miejsca oraz celu ataku, ponadto pozwala dostosować plan działania, a w konsekwencji pomyślnie wykonać zadanie[5].

Miejsce na dokonanie ataku terrorystycznego w cyberprzestrzeni jest zawsze tak dobrane, aby osiągnąć strategiczny cel, jakim jest destabilizacja ekonomiczna sektora bądź regionu czy systemu zarządzania administracją państwową.

Jednym z sektorów, który może podlegać cyberatakowi, jest system zarządzania transportem międzynarodowym. Dzisiaj porty morskie odgrywają szczególną rolę w procesie integracji międzynarodowych systemów transportowych, natomiast centra logistyczne są jednostkami organizacyjnymi i systemem zaopatrywania rynku wewnętrznego kraju i obsługi partnerów międzynarodowych, a tym samym są newralgicznym i czułym otwartym systemem na cyberataki terrorystyczne. Koncepcja budowy morskich centrów logistycznych w Polsce dotyczy portu szczecińskiego i portu gdańskiego. Centra logistyczne, które mają funkcjonować na obszarze wybrzeża morskiego, są szczególnie narażone na cyberatak terrorystyczny, gdyż stanowią skomplikowaną organizację logistyczną, która w dużej części prowadzi swoją działalność drogą elektroniczną, opierając się na współczesnych technologiach informacyjno-komunikacyjnych, a dodatkowo skupia w sobie trzy rodzaje transportu — drogowy, morski, śródlądowy i powietrzny.

[5] A. M. Colarik, *Cyber Terrorism: Political and Economic Implications*, Published by IGI Global, 2006, s. 23.

## SEKTOR TRANSPORTU I LOGISTYKI WRAZ Z PORTAMI MORSKIMI W OBLICZU CYBERATAKU

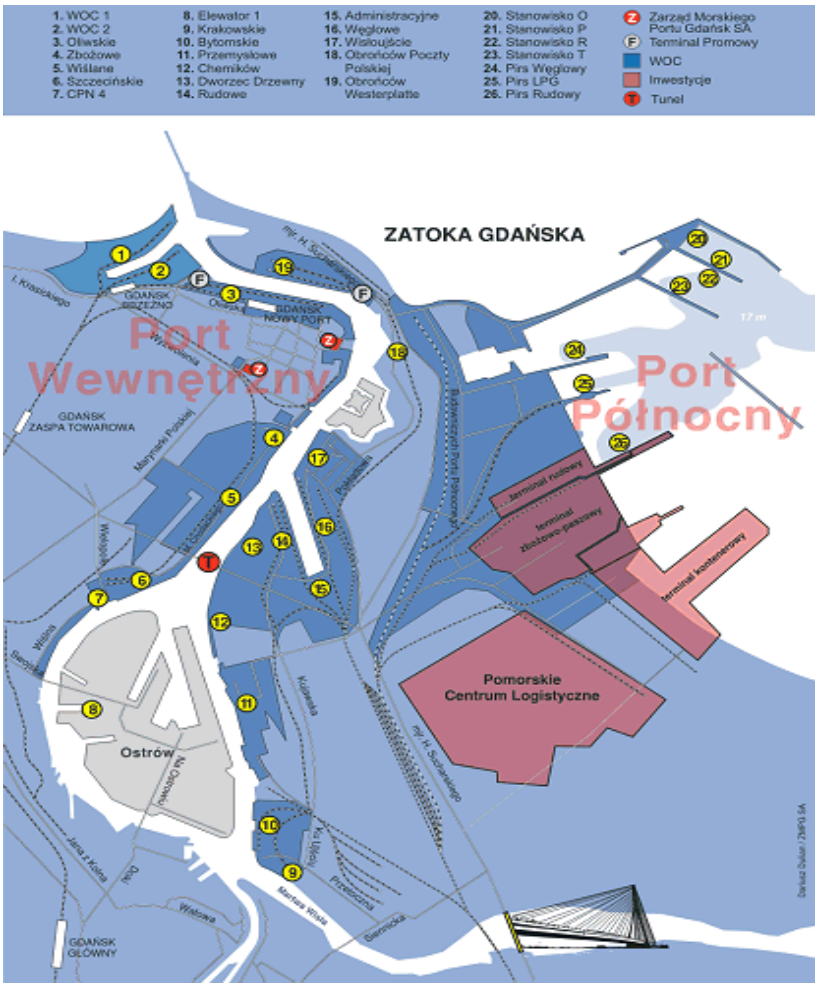
Porty morskie mogą stanowić potencjalny cel ataku terrorystycznego. Współczesny port morski odgrywa kluczową rolę w podziale procesu produkcyjnego gospodarki każdego morskiego państwa oraz w sferze dystrybucyjnej i usługowej. Usługi dokonywane w porcie morskim są kompatybilne względem siebie, tak by spełnić wszystkie postulaty logistyczne, czyli zintegrować takie czynności, jak: planowanie, sterowanie, realizacja oraz weryfikacja działań zgodnie z postulatem 6 R (ang. *right goods, right quanity, right pleace, right time and right quality*). Jak powszechnie wiadomo, „logistyka jest procesem koordynacji wszystkich czynności niematerialnych, które muszą zostać przeprowadzone dla wykonania usługi w sposób efektywny pod względem kosztów i zgodny z wynagrodzeniem klienta”[6]. Stąd związek między portem morskim a logistyką jest bardzo istotny. Obszar portu morskiego stanowi miejsce realizacji wymiany handlowej. Czynności te odnoszą się głównie do realizacji zlecenia, zarządzania potencjałem usługowym oraz dostawy usług poprzez kanał dystrybucyjny, czyli drogę od początkowego do ostatecznego klienta, konsumenta, użytkownika, określaną poprzez charakter stron oferujących dane usługi. I dlatego port morski odgrywa znacząca rolę w łańcuchu transportowym[7]. Przykładami portów morskich, które zawierają koncepcję powstania centrum logistycznego, są porty szczeciński, gdyński i gdański.

Koncepcja Pomorskiego Centrum Logistycznego w Gdańsku zakłada, że centrum to wraz z Morskim Terminalem Kontenerowym stanowić będzie kompleks obsługujący przepływ towarów w relacjach południkowych, obejmujący swym zasięgiem obszar Skandynawii i Europy Środkowej, zawierający: terminal multimodalny, kompleks magazynów i placów składowych, centrum biznesu, stacje obsługi pojazdów, zaplecze hotelowo-gastronomiczne[8]. Lokalizację Pomorskiego Centrum Logistycznego w gdańskim porcie przedstawia rysunek 1.

[6] H. CH. Pohl, *Zarządzanie logistyką*, Wyd. IliM, Poznań 1998, s. 12.

[7] S. Szwankowski, *Funkcjonowanie i rozwój portów morskich*, Wyd. Uniwersytetu Gdańskiego, Gdańsk 2002, s. 86.

[8] Strona internetowa Portu Gdańskiego: http://www.portgdansk.pl/index.php?id=transport_infr&lg=pl z 02.01.2008.

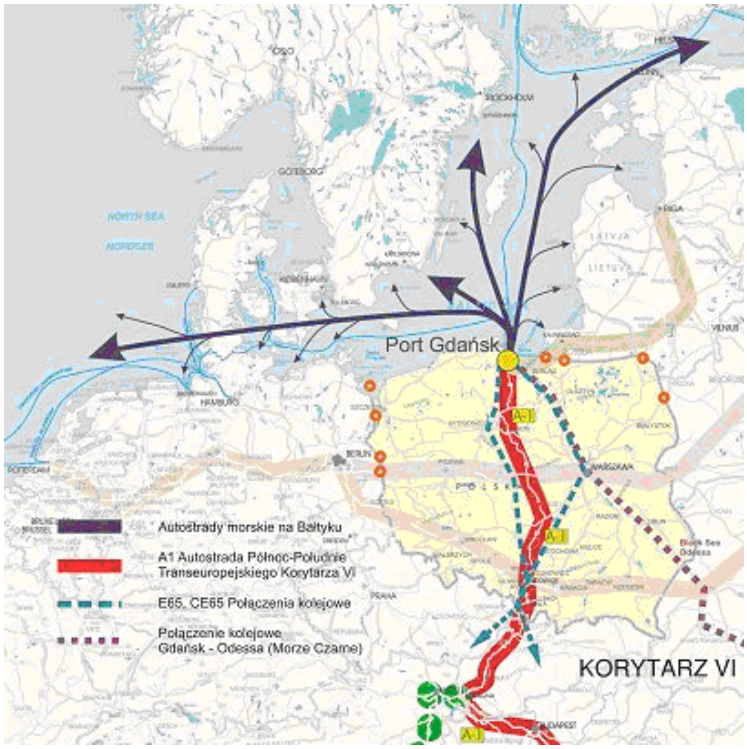



Rys. 1. Lokalizacja Pomorskiego Centrum Logistycznego w Porcie Północnym w Gdańsku

*Źródło: strona internetowa Portu Północnego w Gdańsku.*

„Ważnym kierunkiem ekspansji przestrzennej portów polskich są centra dystrybucyjno-logistyczne. Powstawanie centrów logistycznych w portach morskich jest wynikiem całego splotu czynników, wśród których za najważniejszy można uznać konieczność usprawnień w procesach magazynowania, przemieszczania i przetwarzania towarów. Mnogość funkcji realizowanych przez współczesny port morski, różnorodność gałęzi transportowych działających na jego terenie, jak również złożoność i niepowtarzalność poszczególnych procesów transportowych stanowią najlepsze miejsce do wdrażania systemów logistycznych, umożliwiających optymalizowanie całokształtu zjawisk zachodzących w porcie. Portowe centra logistyczne są z reguły

obszarami o dużej intensywności wykorzystania przestrzeni, czytelnych i prostych rozwiązaniach komunikacyjnych oraz wysokich standardach urbanistycznych. Ich powstanie w bardzo pozytywny sposób oddziałuje na najbliższe otoczenie portowe i miejskie, stymulując wzrost aktywności społeczno-gospodarczej w skali miasta i regionu, dynamizując wykorzystanie cennej przestrzeni portowej i wpływając na wzrost konkurencyjności portu. W polskich portach morskich przewiduje się utworzenie dwóch dużych centrów dystrybucyjno-logistycznych o zasięgu międzynarodowym”[9]. Jedno z nich ma być zlokalizowane na terenie gdańskiego Portu Północnego. „Port morski w Gdańsku będzie jednym z kluczowych ogniw Transeuropejskiego Korytarza Transportowego nr VI”[10]. Przebieg tej trasy w dużym stopniu pokrywa się z historycznym szlakiem bursztynowym.



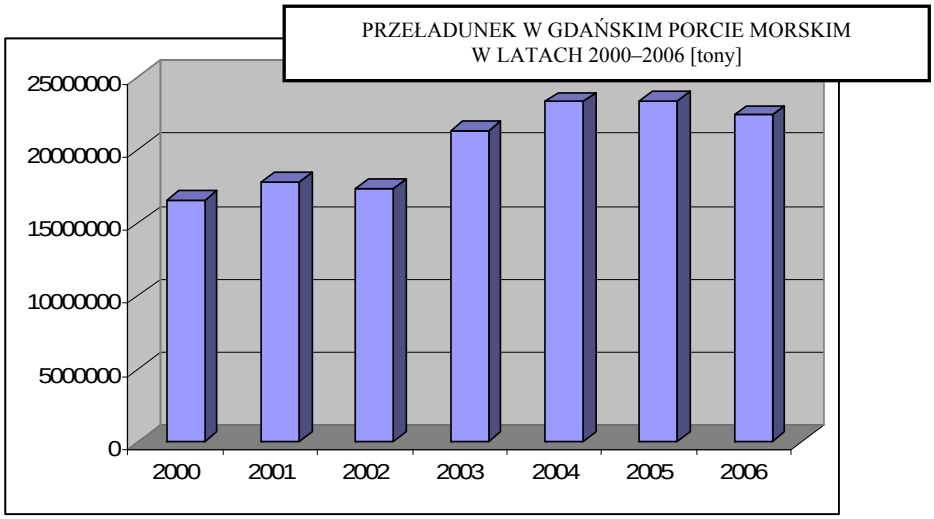

Rys. 2. Przebieg Transeuropejskiego Korytarza Transportowego nr VI

*Źródło: strona internetowa Portu Północnego w Gdańsku.*

[9] S. Szwankowski, *Polish seaports under the challenges of globalization*, [w:], *Maritime transport in a global economy*, University of Gdansk, Gdańsk 2001.

[10] Strona internetowa Portu Gdańskiego, http://www.portgdansk.pl/index.php?id=transport_infr&lg=pl z 02.01.2008.

„Atutem lokalizacji Portu Gdańsk jest centralne położenie na południowym wybrzeżu Morza Bałtyckiego w najszybciej rozwijającym się regionie Europy. Port jest kluczowym ogniwem Transeuropejskiego Korytarza Transportowego nr VI łączącego Skandynawię z Europą Południowo-Wschodnią”[11]. Port Północny odgrywa znaczącą rolę w systemie transportowym Europy, gdyż łączy na swoim obszarze wszystkie gałęzi transportu, tj. transport drogowy, morski, lotniczy i śródlądowy. Statystyka przeładunków w gdańskim porcie ukazana została na poniższych rysunkach.




Rys. 3. Przeładunek [tony] w gdańskim porcie morskim w latach 2000–2006

*Opracowanie własne.*

Rola portu morskiego w Gdańsku jako ogniwa transportu wyraża się ilością przeładowanej masy ładunkowej. Dane opublikowane przez GUS i załączone w tabeli 1. wskazują, iż wielkość przeładunku mierzona w tonach znacząco wzrastała z roku na rok.

Tabela 1. Przeładunek mierzony w tonach w gdańskim porcie morskim w latach 2000–2006

| LATA | 2000 | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 |
|---|---|---|---|---|---|---|---|
| RAZEM | 16543544 | 17812893 | 17371401 | 21292996 | 23314926 | 23341022 | 22407129 |

[11] Tamże.

Przyjmując rok 2000 za rok bazowy, a 2006 za rok końcowy, można obliczyć przyrost wielkości przeładunku w morskim porcie w Gdańsku. Wielkość ta została obliczona za pomocą relatywnego wskaźnika różnicy wielkości przeładunku[12] przedstawionego według poniższej formuły:

wielkość przeładunku z roku bazowego (2000) — 16543544 ton (= 100)

wielkość przeładunku z roku końcowego (2006) — 22407129 ton

i zapis matematyczny:

$$\mathbf{W_{RW}} = \frac{W_{PK} \times 100\%}{W_{PK}}$$

gdzie: $W_{RW}$ — relatywny wskaźnik różnicy wielkości przeładunku;

$W_{PB}$ — wielkość przeładunku z roku bazowego;

$W_{PK}$ — wielkość przeładunku z roku końcowego.

Podstawiając, otrzymujemy:

$$W_{RW} = \frac{22407129 \times 100}{16543544}$$

$$W_{RW} = 135{,}44.$$

Jako że

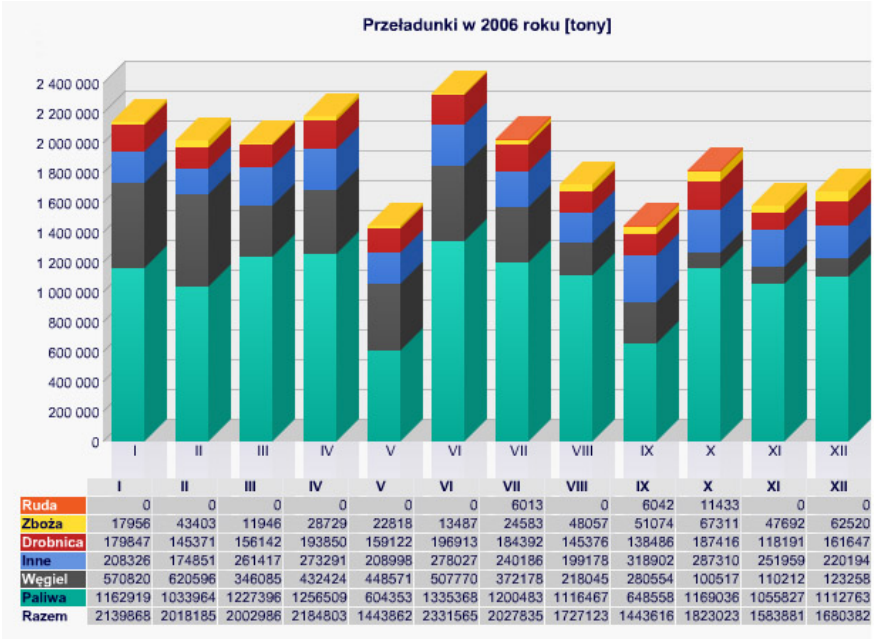
(2000 r.) 16543544 ton = 100%, to

(2006 r.) 22407129 ton = (135,44 – 100)% = 35,44%.

Z powyższego wynika, iż w 2006 roku nastąpił wzrost wielkości przeładunku o 35,44% w porównaniu z rokiem 2000.

W gdańskim porcie obsługiwane są wszystkie typy ładunków dostarczanych przez wymienne gałęzie transportowe. Rysunek 4. przedstawia, jaki udział miały poszczególne grupy ładunków (mierzone w tonach) w całościowym przeładunku w roku 2006.

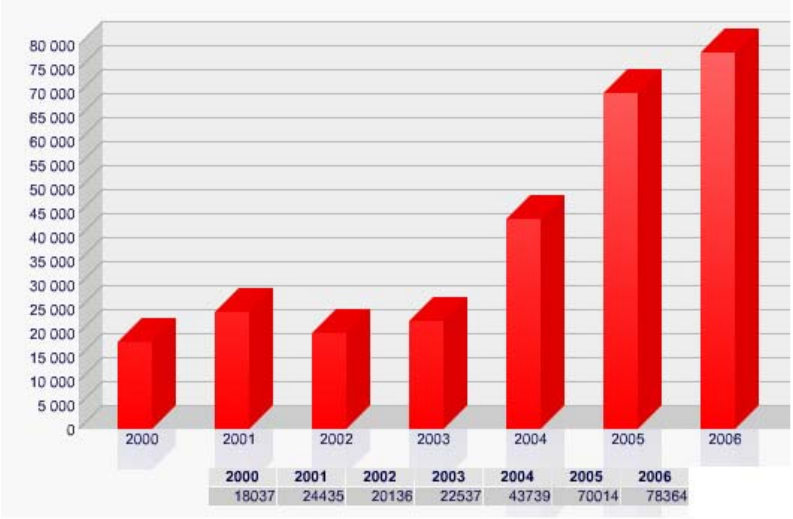
[12] Wskaźnik statystyczny skonstruowany na potrzeby niniejszej analizy przez autorkę.




| | I | II | III | IV | V | VI | VII | VIII | IX | X | XI | XII |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Ruda | 0 | 0 | 0 | 0 | 0 | 0 | 6013 | 0 | 6042 | 11433 | 0 | 0 |
| Zboża | 17956 | 43403 | 11946 | 28729 | 22818 | 13487 | 24583 | 48057 | 51074 | 67311 | 47692 | 62520 |
| Drobnica | 179847 | 145371 | 156142 | 193850 | 159122 | 196913 | 184392 | 145376 | 138486 | 187416 | 118191 | 161647 |
| Inne | 208326 | 174851 | 261417 | 273291 | 208998 | 278027 | 240186 | 199178 | 318902 | 287310 | 251959 | 220194 |
| Węgiel | 570820 | 620596 | 346085 | 432424 | 448571 | 507770 | 372178 | 218045 | 280554 | 100517 | 110212 | 123258 |
| Paliwa | 1162919 | 1033964 | 1227396 | 1256509 | 604353 | 1335368 | 1200483 | 1116467 | 648558 | 1169036 | 1055827 | 1112763 |
| Razem | 2139868 | 2018185 | 2002986 | 2184803 | 1443862 | 2331565 | 2027835 | 1727123 | 1443616 | 1823023 | 1583881 | 1680382 |

Rys. 4. Przeładunek [tony] w gdańskim porcie morskim w 2006 roku
*Źródło: http://www.portgdansk.pl/*

Z kolei rysunek 5. przedstawia udział przeładunków kontenerowych w całościowym przeładunku w latach 2000–2006.




| 2000 | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 |
|---|---|---|---|---|---|---|
| 18037 | 24435 | 20136 | 22537 | 43739 | 70014 | 78364 |

Rys. 5. Przeładunki kontenerów w gdańskim porcie morskim w latach 2000–2006
*Źródło: http://www.portalmorski.pl*

Głębokowodny terminal DCT Gdańsk SA przystosowany jest do obsługi największych jednostek wpływających na Morze Bałtyckie, stąd rosnąca tendencja w przeładunku kontenerowym[13]. Stosując zapis matematyczny, otrzymujemy:

$$W_{RW} = \frac{78364 \text{ x } 100}{18037}$$

$$W_{RW} = 434{,}46.$$

Jako że:

(2000 r.) 18037 ton = 100%, to

(2006 r.) 78364 ton = (434,46 – 100)% = 334,46%.

Z powyższego wynika, iż w 2006 roku nastąpił wzrost wielkości przeładunku kontenerów o 334,36% w porównaniu z rokiem 2000.

Jak wskazują dane, port w Gdańsku jest istotnym węzłem w łańcuchach transportowych i może stać się celem cyberataku terrorystycznego. Gdański Port Północny spełnia podstawowe funkcje portowe, do których należą[14]: funkcja transportowa, handlowa i przemysłowa. Dodatkowo, stosując kryterium przestrzenne, spełnia funkcje: miastotwórczą, regionotwórczą i regionalną. Wszystkie te argumenty pokazują, dlaczego gdański port morski został wybrany na lokalizację Pomorskiego Centrum Logistycznego. Centrum logistyczne zlokalizowane na jego terenie ma kluczowe znaczenie w dalszym rozwoju miasta i całego regionu pomorskiego.

Zastosowanie nowoczesnych technologii informatycznych w centrach logistycznych umożliwia podnoszenie jakości obsługi klienta poprzez zwiększanie wydajności wymiany towaru i usług[15]. Komunikacja w łańcuchu logistycznym jest istotnym elementem w poprawnym przebiegu procesu logistycznego oraz procesu transakcyjnego. Elektroniczna technologia komunikacyjna stwarza możliwości nieograniczonej wymiany danych oraz sprawnego zarządzania procesami logistycznymi, a tym samym może stać się celem cyberataku. Funkcje te łączy w sobie tzw. platforma logistyczna. Będąc integralną częścią centrum logistycznego, obsługuje, koordynuje i integruje wiele typów urządzeń.

[13] http://www.portgdansk.pl/o-porcie/grupy-ladunkowe z 02.02.2008.

[14] *Ekonomika portów morskich i polityka portowa*, red. L. Kuźma, Gdańsk 1993, s. 14–16.

[15] Z. Kordel, *Centra logistyczne jako efekt outsourcingu*, Oficyna Wyd. „Nasz Dom i Ogród", Wrocław 2001, s. 220.

Centra logistyczne bazujące na systemie RFID[16] mogą zapewnić natychmiastową, zdalną kontrolę stanów magazynowych, a dodatkowo wczytane informacje przesyłane są do systemu centralnego automatycznie, bez ingerencji człowieka. Cały proces przyjmowania i wydawania towaru można dowolnie zaprojektować i zautomatyzować, zakładając na przykład przy wjeździe do magazynu specjalne bramki z urządzeniami nadawczo-odbiorczymi.

Dzięki platformie logistycznej następuje przejrzysty i czytelny przepływ informacji oraz dokumentów we wszystkich etapach procesu zarządzania łańcuchem dostaw. Możliwe jest bieżące monitorowanie przepływu wszystkich wygenerowanych usług transportowych (na przykład usługa o nazwie „śledzenie przesyłki" za pomocą systemu zintegrowanego GPRS) i błyskawiczne reagowanie dostawcy usług logistycznych w razie wystąpienia jakiegokolwiek problemu. Komunikacja w łańcuchach logistycznych wymaga stosowania sformatowanych danych w postaci komunikatów między systemami informatycznymi[17]. Na potrzeby wymiany dokumentów elektronicznych powstał uniwersalny język — standard EDI, natomiast dominującym standardem międzynarodowym jest UN/EDIFACT (United Nations/Electronic Data Interchange For Administration, Commerce and Transport)[18]. Standardy dokumentów umożliwiają wymianę dokumentów bez konieczności kolejnego wprowadzania ich do bazy danych. Stwarza to możliwość przesyłania danych pomiędzy aplikacjami stosowanymi przez partnerów handlowych bez interwencji człowieka[19]. Do głównych korzyści komunikacji według standardu UN/EDIFACT można zaliczyć:

— zredukowanie kosztów obsługi papierowych dokumentów (zamówień, faktur) poprzez elektroniczną i automatyczną obsługę dokumentów wymienianych pomiędzy kontrahentami;

[16] RFID (ang. *Radio frequency identification*) — „system kontroli przepływu towarów w oparciu o zdalny, poprzez fale radiowe, odczyt i zapis danych z wykorzystaniem specjalnych układów elektronicznych przytwierdzonych do nadzorowanych przedmiotów. Niekiedy technologia RFID nazywana jest radiowym kodem kreskowym. I tak jak do rozpowszechnienia kodów kreskowych potrzebne były ogólnoświatowe działania unifikacyjne, tak też dla technologii RFID potrzebna jest tego rodzaju unifikacja", http://pl.wikipedia.org/wiki/RFID z 08.02.2008.

[17] L. Kiełtyka, *Multimedia w biznesie. Gospodarka elektroniczna. Multimedialne technologie informacyjne. Zarządzanie informacją. Nauczanie przez multimedia*, Wyd. Zakamycze, Kraków 2003, s. 63.

[18] UN/EDIFACT to zbiór międzynarodowych standardów oraz podręczniki i przewodniki dla elektronicznej wymiany sformatowanych danych, w szczególności danych dotyczących handlu towarami i usługami, między niezależnymi systemami informatycznymi. Standard UN/EDIFACT opracowany pod auspicjami ONZ uwzględnia dokumenty z takich dziedzin, jak handel i przemysł, administracja, transport, finanse, ubezpieczenia, cło, turystyka i inne.

[19] L. Kiełtyka, wyd. cyt., s. 67.

— minimalizację błędnych dokumentów i korekt (szybsza realizacja zamówień);
— przyspieszenie procesów logistycznych;
— możliwość wymiany danych z wieloma partnerami, w tym z sieciami handlowymi;
— bezpieczeństwo danych i niezawodność wymiany informacji,
— szybką reakcję na potrzeby rynku.

Przedstawione wyżej informacje wskazują, że komunikacja elektroniczna stanowi istotną i nierozerwalną część systemu i funkcjonowania centrum logistycznego i może być potencjalnym celem cyberataku.

Centra logistyczne są wyposażone w potężną sieć komputerową, której rozległość obejmuje rynek regionalny, krajowy i międzynarodowy. Dzięki infrastrukturze informatycznej zarządza się przepływem masy towarowej od nadawcy do finalnego odbiorcy. Różnorodność gałęzi transportu, takich jak transport morski, lądowy czy powietrzny, zarządzana za pomocą sieci komputerowej niesie w sobie konieczność zabezpieczenia tego systemu zarządzania przed potencjalnym atakiem terrorystycznym z cyberprzestrzeni.

„Systemy komputerowe narażone są na zagrożenia trzema formami cyberataków: propagandowo-dezinformacyjnymi (modyfikowanie stron www, ideologiczny spamming), sabotażem komputerowym (zamachy typu odmowa usługi, rozpowszechnianie wirusów i innych destrukcyjnych programów komputerowych) oraz zamachami na krytyczną infrastrukturę[20] połączonymi z ingerencją w jej funkcjonowanie”[21].

Doświadczenia oraz zdarzenia, które miały miejsce na przestrzeni ostatnich lat, a związane były z atakami terrorystycznymi w cyberprzestrzeni[22] (na zintegrowane systemy zarządzania ściśle powiązane z bazą informatyczną), koncentrowały się na następujących formach:

— ingerencja w dane systemowe;
— implementowanie programów destrukcyjnych (tzw. wirusów).

[20] „Infrastruktura krytyczna obejmuje w szczególności te zasoby rzeczowe, usługi, urządzenia informatyczne, sieci i aktywa infrastrukturalne, których zakłócenie lub zniszczenie miałoby znaczący wpływ na najważniejsze funkcje społeczne, w tym łańcuch dostaw, zdrowie, bezpieczeństwo, ochronę, pomyślność gospodarczą lub społeczną obywateli lub funkcjonowanie Wspólnoty lub należących do niej państw członkowskich”. Dz.U.UE.L.07.58.1, decyzja Rady Unii Europejskiej z 12 lutego 2007 r. ustanawiająca na lata 2007–2013 częścią ogólnego programu w sprawie bezpieczeństwa i ochrony wolności szczegółowy program „Zapobieganie, gotowość i zarządzanie skutkami terroryzmu i innymi rodzajami ryzyka dla bezpieczeństwa”. Zob. http://www.ms.gov.pl/ue_koop/decyzja_terroryzm.rtf z 03.02.3008 r.

[21] A. Adamski, *Cyberterroryzm…*, wyd. cyt.

[22] G. I. Rattray, *Strategic Warfare in Cyberspace*, Cambridge, MA, MIT Press, 2001, s. 18.

Ingerencja w dane systemowe centrum logistycznego może przybierać formę hackingu. „Uzyskanie nieuprawnionego dostępu do systemu komputerowego przy pomocy urządzeń telekomunikacyjnych jest klasyczną formą zamachu na bezpieczeństwo elektroniczne przetwarzanych informacji. Skuteczne dokonanie takiego zamachu i przejęcie kontroli nad zaatakowanym systemem umożliwia popełnienie kolejnych przestępstw, które mogą być skierowane przeciwko różnorodnym dobrom prawnym (np. ochrona informacji, życiu i zdrowiu, mieniu, danym osobowym wiarygodności dokumentów, etc.). Od integralności i niezakłóconego działania przetworzenia informacji zależeć może życie i zdrowie człowieka jak i prawidłowe funkcjonowanie gospodarki (systemy logistyczne) oraz bezpieczeństwo państwa i jego obywateli (systemy dowodzenia i kontroli lotów)”[23]. Dokonywanie jakichkolwiek ingerencji w dane i programy komputerowe centrum logistycznego powoduje wzrost kosztów obsługi dokumentów (zamówień, faktur) poprzez dezorganizację elektroniczną i błąd automatycznej obsługi dokumentów wymienianych pomiędzy kontrahentami. Prowadzi to do niemożności realizacji zamówień, zatrzymania procesów logistycznych oraz braku reakcji na potrzeby płynące z rynku. Wywołana niepoprawność i niekompletność przetwarzanej informacji i funkcjonowania programów komputerowych prowadzi w konsekwencji do destabilizacji procesów częściowych (np. na wstępnym poziomie obsługi) oraz ogólnych (zachodzące na poziomie zaawansowanym). Naruszenie integralności elektronicznego zapisu informacji wiąże się z ogromnymi stratami finansowymi ponoszonymi w momencie przestoju centrum logistycznego i poszczególnych jednostek zaangażowanych we współdziałanie z centrum logistycznym. Włamanie do systemów komputerowych centrum logistycznego jest zjawiskiem szkodliwym społecznie, wywołującym dezorganizację wewnętrzną (poszczególnych elementów wchodzących w skład centrum logistycznego) i zewnętrzną (wprowadzenie totalnego zamieszania pomiędzy centrum logistycznym rozumianym jako organizacja a poszczególnymi elementami współpracującymi, np. gałęziami transportowymi czy nadawcą i finalnym odbiorcą).

Dużym problemem może okazać się implementacja programów destruktywnych, np. „DoS” (tzw. programów złośliwych), które stworzono, aby penetrować lub uszkodzić system operacyjny komputera lub inne programy bez zgody właściciela. Często określa się je jako wirusy, robaki czy konie trojańskie. Jest to wprowadzanie

[23] A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy*, Wydawnictwo Dom Organizatora. Toruń 2001, s. 19.

do systemu komputerowego ukrytych programów, które podczas jego pracy (bez wiedzy użytkownika) replikują się i dokonują zniszczenia danych oraz systematycznej modyfikacji, zablokowania i wyniszczenia systemów i sieci komputerowych. Wirus jest programem, który na skutek ciągłego powielania samego siebie wykorzystuje coraz większe zasoby systemu komputerowego, powodując jego destabilizację. Implementacja wirusów odbywa się wszystkimi możliwymi kanałami dostępu do systemu. Powszechne techniki ataków na infrastrukturę sieciową wykorzystują głównie niedoskonałości systemu, tzw. luki systemowe, przez które wprowadza się programy mające na celu wyniszczenie systemu. W ostatnich miesiącach popularny stał się atak na system komputerowy i usługę sieciową świadczoną przez dowolne przedsiębiorstwo zintegrowane z Internetem o nazwie Denial of Service (DoS)[24].

Niekonwencjonalny atak terrorystyczny na bazę teleinformatyczną[25] centrum logistycznego, a wraz z nim portu morskiego stanowi poważne zagrożenie dla systemu transportowego, usługowego oraz dla osób zatrudnionych w porcie morskim. W sieciach komputerowych centrum logistycznego i portu morskiego atak DoS może w początkowej fazie wywołać działania polegającym na wysyłaniu do sieci komputerowej nadmiarowej ilości danych będących np. w formie zapytań o usługi. Po przeprowadzeniu takiego niekonwencjonalnego ataku niemożliwe do zrealizowania stają się podstawowe funkcje, jakie spełnia system teleinformatyczny i sieć komputerowa w centrum logistycznym i porcie morskim. Następuje zablokowanie i wyniszczenie infrastruktury informatycznej, a w konsekwencji zniszczenie systemu informatycznego zarządzania centrum logistycznym. Całkowity paraliż centrum logistycznego to w obecnej dobie wielomilionowe straty. Chaos spowodowany niekonwencjonalnym atakiem terrorystycznym na infrastrukturę informatyczną odzwierciedlony jest w braku koordynacji podstawowych funkcji działalności centrum logistycznego. Dezorganizacja powstająca na etapie czynności, procesów logistycznych i zjawisk zachodzących od źródła pozyskania klientów-nadawców i odbiorców, przez etapy transportu, aż do dostarczenia i odbioru w etapie końcowym prowadzi do istotnego zachwiania równowagi w funkcjonowaniu centrum logistycznego. Czynności te wykonywane w kilku bądź kilkunastu etapach przypadają na pewien odcinek czasu oraz tworzą zamkniętą całość rozwojową i konsumpcyjną. Dlatego zdestabilizowanie pojedynczej czynności prowadzi do dezorganizacji

[24] Microsoft TechNet, http://www.microsoft.com/poland/technet/security/topics/serversecurity/avdind_2.mspx z 10.12.2007.

[25] A. Kamal, *The Law of Cyber-Space*, Published by the United Nations Institute for Training and Research, New York 2007.

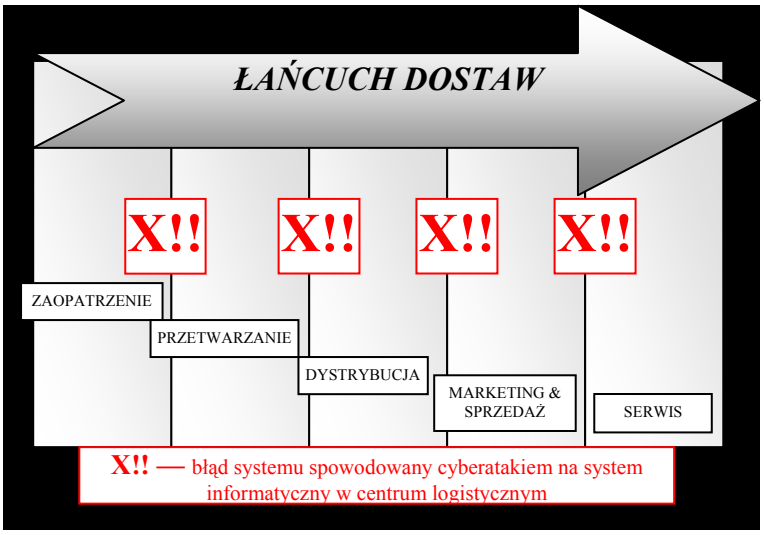
całego systemu funkcjonowania centrum logistycznego. Przepływ informacji jest dominującym czynnikiem, który wpływa na pomyślny przebieg każdego procesu logistycznego. Procesy te realizowane są według ściśle określonej procedury, a zachwianie pojedynczego podprocesu logistycznego znajduje swoje odzwierciedlenie w pomyślnej realizacji całego procesu logistycznego.

Pomyślna realizacja procesów transportowych, przeładunkowych i magazynowania przebiega dzięki odpowiedniej informacji zawartej w systemie i na etykietach dołączanych do towaru. Jeżeli we wstępnej fazie przeładunkowej wystąpi błąd, zakłócenie informacji elektronicznej, to sprawny i efektywny przepływ towarów będzie niemożliwy. Procesy logistyczne, do których zalicza się magazynowanie, przeładunek, pakowanie, znakowanie, przekazywanie i opracowywanie zamówień, są niczym innym jak zadaniami wprowadzanymi i zarządzanymi za pomocą systemu komputerowego. Wprowadzenie błędnych informacji do systemu centrum logistycznego może się przyczynić do dużej dezorganizacji w funkcjonowaniu oraz strat finansowych w centrum logistycznym. Oprócz zadań dotyczących realizacji, do działań logistycznych należą powiązane z nimi zadania planowania, sterowania i kontrolowania, czyli parametry brane pod uwagę przy podejmowaniu decyzji przez potencjalnych nadawców i odbiorców[26]. Wprowadzenie wirusa do systemu komputerowego zarządzającego procesami transportowymi może spowodować zawieszenie działalności centrum logistycznego.

Centrum logistyczne jako ogniwo w łańcuchu dostaw przyczynia się do redukcji czasu potrzebnego na każdy element procesu logistycznego. Na terenie centrum logistycznego realizowane są wszystkie usługi mieszczące się w łańcuchu dostaw. Do usług tych zalicza się: zaopatrzenie, przetwarzanie, dystrybucja, marketing i sprzedaż, a także serwis[27] (rys. 6.).

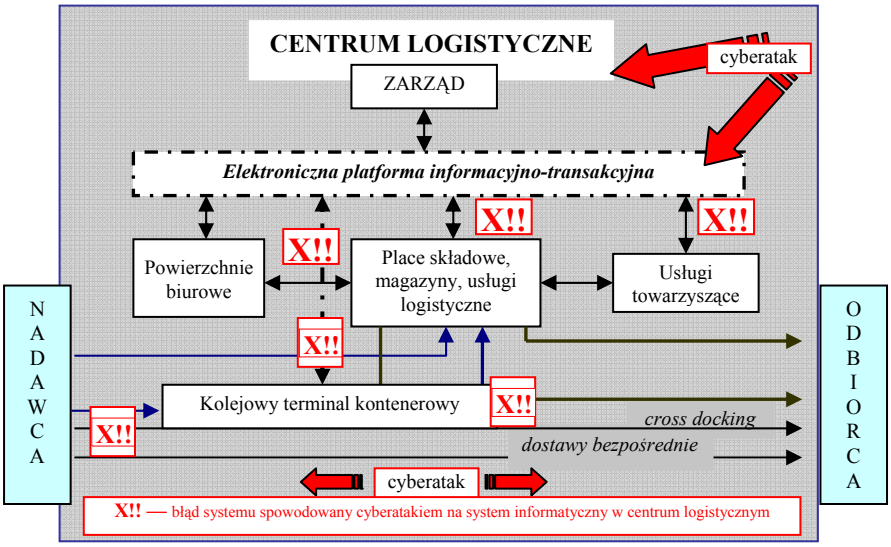
Atak terrorystyczny na centrum logistyczne niesie z sobą poważne straty finansowe, zarówno regionalne, jak i międzynarodowe. W jego konsekwencji PCL w Gdańsku może stać się niewiarygodnym i wątpliwym partnerem na arenie europejskiej w zakresie wymiany handlu zagranicznego i świadczonych usług logistycznych. Niebagatelny jest tu również aspekt społeczny, bowiem udany atak terrorystyczny może spowodować unieruchomienie PCL, a tym samym zwolnienia z pracy oraz niepokoje i niezadowolenie społeczne.

[26] H. CH. Phol, *Zarządzanie logistyką*, Wyd. IliM, Poznań 1998, s. 9.
[27] Tamże, s. 44.




Rys. 6. Procesy informatyczne związane z procesami logistycznymi

*Opracowanie własne*[28].




Rys. 7. Przykładowy schemat cyberataku terrorystycznego na centrum logistyczne

*Opracowanie własne*[29].

[28] Na podstawie rysunku zawartego w: M. Chaberek, *Mikro- i makroekonomiczne aspekty wsparcia logistycznego*, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2002, s. 43.

[29] Na podstawie rysunku zawartego w: *Uwarunkowania rozwoju systemu transportowego*, red. B. Liberadzki, L. Mindura, Wyd. Instytut Technologii Eksploatacji PiB, Warszawa 2006, s. 472.

Ewentualne zmiany i zachowania w procesach przemieszczania towarów na skutek ataków terrorystycznych byłyby najbardziej widoczne z punktu widzenia operatorów logistycznych. Wzrost wymagań klientów, by działać zgodnie z zasadą *just-in-time*, sprawił, że porty morskie w Europie zaczęto traktować jako centra dystrybucji. Porty te oferując „szeroki zakres usług logistycznych stały się istotnym ogniwem w łańcuchu dostaw surowców i towarów od producentów do finalnych odbiorców z punktu widzenia wymagań zleceniodawców”[30]. Przepływ towaru zakłócony implementacją złośliwego programu i zapisany błędnie w systemie dyskwalifikuje jednocześnie wszystkie związane z nim czynności, a więc[31]:

— dokonanie odpraw celnych;
— sortowanie towaru przed transportem;
— opłaty podatkowe i podobne opłaty;
— fizyczne przemieszczenie towaru.

Morskie centrum logistyczne swoją działalność rozszerza tak, aby dodatkowo na jego terytorium działali operatorzy logistyczni. „Zarządca centrum logistycznego jest jedynie dostawcą niezbędnej infrastruktury komunikacyjnej oraz usług podstawowych (utrzymanie, administracja, ochrona, udostępnianie infrastruktury transportowej). Usługi logistyczne są świadczone przez niezależne firmy logistyczne, osiedlone w centrum logistycznym koordynowane przez centrum logistyczne”[32].

Jak wcześniej ukazano, również projekt gdańskiego morskiego centrum logistycznego występuje jako organizacyjna koncepcja z główną bazą dla wyposażenia technicznego. Bazę stanowi odpowiednia infrastruktura telekomunikacyjna, umożliwiająca sprawny i szybki przepływ informacji, jak na przykład sieć internetowa, telefoniczna, faksowa, przy czym sieć internetowa powinna być kompatybilna z siecią satelitarną, by sprawnie monitować przepływ towaru za pomocą na przykład GPS (ang. *Global Positioning System — NAVigation Signal Timing And Ranging*). Nie należy zapominać, że dodatkowo w skład infrastruktury technicznej wchodzi profesjonalnie wykwalifikowany personel, który stanowi bazę intelektualną dla tej koncepcji centrum logistycznego. Dzięki szybkiej informacji dobrze funkcjonuje baza zarządzająca i koordynująca przepływ towarów. Tak działający operator logistyczny na terenie portu gdańskiego może oferować klientom pełen zakres usług logistycznych o zasięgu regionalnym, krajowym i międzynarodowym opierających się na maksymalnym wykorzystaniu przepływu informacji i tworzeniu określonych systemów

[30] Z. Kordel, *Centra logistyczne jako efekt outsourcingu*, wyd. cyt., s. 221.
[31] Tamże, s. 222.
[32] Tamże.

informacyjnych, które będą gwarantować skuteczną realizację zaprojektowanych łańcuchów dostaw[33]. Taka koncepcja pozwala na podjęcie natychmiastowych działań zaspokajających potrzebę zgłoszoną przez klienta, umożliwia elastyczność w działaniu, wybór optymalnego rozwiązania i szybkiego działania w czasie, pozwala na oferowanie konkurencyjnych cenowo i jakościowo usług logistycznych. Informacja będąc najcenniejszym z zasobów XXI wieku, w dobie rewelacyjnie rozwiniętej techniki i technologii, musi w krótkim czasie docierać do tych odbiorców, których dotyczy. Transport i logistyka stanowi około 5% udziału w PKB i zatrudnia 400 tysięcy pracowników, będąc ważnym elementem polskiej gospodarki. Morskie centra logistyczne stanowią istotną część funkcjonowania portu morskiego. Ze względu na swoją ważność ekonomiczną mogą stanowić obiekt ataku terrorystycznego, który zakłóci, a nawet zniszczy bazy i systemy informacyjne. Nieuchronnym tego skutkiem będzie wprowadzenie kompletnej dezorganizacji funkcjonowania portu morskiego i jego dystrybucji.

## ZAKOŃCZENIE

Reasumując, port morski wraz z funkcjonującym na jego terenie centrum logistycznym może stanowić potencjalny cel ataku terrorystycznego. Wybór portu morskiego wynika z perspektyw rozwoju polskiego handlu morskiego i tranzytu z siecią krajów oraz rozbudowy połączeń i współpracy z portami morskimi całego świata. Centra logistyczne w portach stanowią płaszczyznę obsługi handlu międzynarodowego. „Tworzenie centrów logistycznych odbywa się w ramach rozwoju portów morskich nowej generacji, które poprzez tworzenie logistycznych platform portowych stają się ośrodkami kompleksowej dystrybucji usług logistycznych oraz biegunami wzrostu gospodarczego w rozwoju regionów. Do takiej roli w przyszłości będą dążyć polskie porty: Gdańsk, Gdynia, Szczecin i Świnoujście”[34].

Gdański port stanowi istotny element programu strategicznego rozwoju gospodarczego regionu pomorskiego. Jako obszar integracji handlowej jest ważnym elementem w funkcjonowaniu gospodarczym kraju. Zakłócenie sprawnego przepływu informacji w gdańskim porcie morskim mogłoby skutkować wyeliminowaniem z procesu wymiany i dystrybucji towarów o zasięgu zarówno regionalnym, jak i międzynarodowym.

[33] Tamże.

[34] S. Szwankowski, B. Szwankowska, *Wielkoskalowe projekty inwestycyjne czynnikiem podnoszenia konkurencyjności polskich portów morskich*, www.portalmorski.pl/referaty/2003/21.pdf z 20.01.2008.

## WNIOSKI

1. Ewentualny atak terrorystyczny w cyberprzestrzeni na Pomorskie Centrum Logistyczne może stworzyć ogromne zagrożenie i straty w wymiarze ekonomicznym, finansowym i społecznym.
2. Udany cyberatak terrorystyczny na centrum logistyczne może spowodować odejście inwestorów, nadawców i odbiorców towarów z regionu i przeniesienie ich w inne miejsca, a tym samym straty finansowe.
3. Skuteczny cyberatak na port morski, który pełni funkcję centrum dystrybucji, spowoduje brak wiarygodności Polski jako partnera zabezpieczającego wymianę handlową na arenie międzynarodowej.

## BIBLIOGRAFIA

[1] Adamski A., *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy*, Wydawnictwo Dom Organizatora, Toruń 2001.

[2] Bógdoł-Brzezińska A., Gawrycki M., *Cyberterroryzm i problemy bezpieczeństwa informacyjne we współczesnym świecie*, Wydawnictwo ASPRA-JR, Warszawa 2003.

[3] Chaberek M., *Funkcje logistyki w stymulacji porządku systemów gospodarczych*, „Zeszyty Naukowe" UG, Gdańsk 2006.

[4] Chaberek M., *Integracyjne funkcje centrum logistycznego*, Spedycja i Transport, 2000.

[5] Chaberek M., *Makro- i mikroekonomiczne aspekty wsparcia logistycznego*, Wyd. Uniwersytetu Gdańskiego, Gdańsk 2002.

[6] Colarik A. M., *Cyber Terrorism: Political and Economic Implications*, Published by IGI Global 2006.

[7] Coyle J. J., Bardi E. J., Langley C. J. Jr., *Zarządzanie Logistyczne*, Wydawnictwo PWE, Warszawa 2002.

[8] *Ekonomika portów morskich i polityka portowa*, red. L. Kuźma, Gdańsk 1993.

[9] Kamal A., *The Law of Cyber-Space*, Published by the United Nations Institute for Training and Research, New York 2007.

[10] Kordel Z., *Centra logistyczne jako efekt outsourcingu,* Oficyna Wydawnicza „Nasz Dom i Ogród", Wrocław 2001.

[11] Krzyżanowski M., *Centra logistyczne w polskich portach morskich czynnikiem rozwoju transportu i handlu*, „Przegląd Komunikacyjny", 2000, nr 12.

[12] *Multimedia w biznesie. Gospodarka elektroniczna. Multimedialne technologie informacyjne. Zarządzanie informacją. Nauczanie przez multimedia*, red. L. Kiełtyka, Wyd. Zakamycze, Kraków 2003.

[13] Pohl H. CH., *Zarządzanie logistyką*, Wyd. IliM, Poznań 1998.

[14] Rattray G.I.R., *Strategic Warfare in Cyberspace*, Cambridge, MA, MIT Press, 2001.

[15] Szwankowski S., *Funkcjonowanie i rozwój portów morskich*, Wyd. Uniwersytetu Gdańskiego, Gdańsk 2002.

[16] Szwankowski S., *Polish seaports under the challenges of globalization*, [w:], *Maritime transport in a global economy*, University of Gdansk, Gdańsk 2001.

[17] *Uwarunkowania rozwoju systemu* transportowego, red. B. Liberadzki, L. Mindura, Wyd. Instytut Technologii Eksploatacji PiB, Warszawa 2006.

[18] Verton D., Black I., *Niewidzialna groźba cyberterroryzmu*, Wydawnictwo Helion, Gliwice 2004.

Źródła elektroniczne

[1] Adamski A., *Cyberterroryzm*, Wydział Prawa i Administracji UMK w Toruniu, Katedra Prawa Karnego i Polityki Kryminalnej, http://unixlab.iis.pwsz.elblag.pl/~stojek/bezp.sys.komp/cyberterroryzm.pdf z 25.01.2008

[2] http://www.microsoft.com/poland/technet/security/topics/serversecurity/avdind_2.mspx z 10.12.2007 (strona internetowa Microsoft TechNet)

[3] http://www.ms.gov.pl/ue_koop/decyzja_terroryzm.rtf z 03.02.3008 r.

[4] http://www.portalmorski.pl/ z 03.02.2008.

[5] http://www.portgdansk.pl/index.php?id=transport_infr&lg=pl z 02.02.2008.

[6] *Słownik internetowy*, http://www.i-slownik.pl/1,323,cyberprzestrzen.html z 02.12.2007.

[7] Szwankowski S., Szwankowska B., *Wielkoskalowe projekty inwestycyjne czynnikiem podnoszenia konkurencyjności polskich portów morskich*, ww.portalmorski.pl/referaty/2003/21.pdf z 20.01.2008.

[8] Urząd Komitetu Integracji Europejskiej, raport *Rynek transportu i logistyki w Polsce*, http://www.ukie.gov.pl/www/serce.nsf/0/913169EE954C46C1C12572F10047AF72?Open z 02.02.2008.

[9] Wach K., *Internet jako środek promocji oraz element konkurencyjności firm w dobie globalizacji*, http://www.zti.com.pl/instytut/pp/referaty/ref5_full.html z 25.01.2008.

## ABSTRACT

The aim of the paper is to present and analyse potential threats caused by cyberattack against sea ports and its communication infrastructure. Marine logistic centers along with the system for international transport management are becoming directions of spacial expansion of sea ports and they may constitute a potential target of terrorist cyberattack.

Recenzent prof. dr hab. Zdzisław Kordel