Luty 2012 r. nr 2

e-Terroryzm.pl

INTERNETOWY BIULETYN
Centrum Studiów nad Terroryzmem
i kwartalnika e-Studia nad Bezpieczeństwem i Terroryzmem

Terroryzm Bezpieczeństwo Ochrona
Wyzwania Zagrożenia Dylematy
Doniesienia Sprawozdania Analizy

W numerze:

Szanowni Czytelnicy!

Oddajemy Państwu kolejny, drugi numer biuletynu Centrum Studiów nad Terroryzmem oraz kwartalnika e-Studia nad Bezpieczeństwem i Terroryzmem. Przy jego powstaniu uwzględniliśmy część krytycznych uwag skierowanych pod naszym adresem przez Czytelników. Bieżący numer ma większą objętość i jak sądzimy następne jego wydania będą zawierać coraz więcej informacji, analiz, naszych przemyśleń przydatnych wszystkim zainteresowanym problematyką bezpieczeństwa i terroryzmu.

W aktualnym numerze biuletynu jego redaktorzy zajęli się problematyką cyberterroryzmu, ekoterroryzmu, podstawowymi międzynarodowymi dokumentami regulującymi zwalczanie terroryzmu oraz podpisaniem umowy ACTA. Opisaliśmy podstawowe metody cyberataku oraz zasadnicze sposoby zabezpieczania się przed zagrożeniami w sieci komputerowej.

Przedstawiamy kilka propozycji pozycji książkowych, wartych naszym zdaniem przeczytania. Jeden z autorów pokusił się o krótki opis koncepcji oficera Sztabu Generalnego carskiej armii płk. Jewgienija Messnera, dotyczącej tzw. miatieżewojny, będącej interesująca teorią działań asymetrycznych i nieregularnych.

Za zespół
Kazimierz Kraj

Artykuły Czytelników z prośbą o publikację prosimy przesyłać pod adres e-mailowy:
redakcja@e-terroryzm.pl
Redakcja zastrzega sobie prawo do korekty oraz publikacji tylko wybranych materiałów.
Zapraszamy do dyskusji na Forum internetowym Biuletynu – http://e-terroryzm.pl/forum

Terroryzm to zjawisko złożone i skomplikowane. Stąd ważne są działania na wielu płaszczyznach, a kompleksowy system zwalczania terroryzmu musi je obejmować.

Zwalczanie terroryzmu może być prowadzone trzema metodami. Będzie to zdanie się głównie na własne narodowe siły oraz systemy bezpieczeństwa lub węższy lub szerszy udział w systemie bezpieczeństwa zbiorowego. W drugim przypadku, współpraca międzynarodowa sprowadzi się tylko do wymiany informacji z innymi państwami na mniejszą lub większą skalę, udzielania sobie gwarancji solidarności i pomocy w razie zagrożenia i transferu doświadczeń praktycznych. Trzecia droga to tzw. integracja systemów bezpieczeństwa. Polega ona na ujednolicaniu wszystkich istotnych dla bezpieczeństwa służb państw członków organizacji międzynarodowych, jak Unia Europejska czy Wspólnota Niepodległych Państw. Ogólnie, w tej koncepcji celem jest osiągnięcie jednolitych w strukturach i procedurach służb bezpieczeństwa, interoperacyjnych i skoordynowanych do działania na terenie wielu państw. Praktycznym przykładem mogłoby być np. utworzenie "Policji Europejskiej" na wzór amerykańskiej FBI, która posiadałaby jednakowe uprawnienia, struktury i procedury we wszystkich członkowskich państwach. Wzrost skuteczności działania takich służb łatwo sobie wyobrazić. Z drugiej strony nie trudno też o różne kontrowersje wokół tego rodzaju pomysłów, jak i trudności w realnej ocenie szans utworzenia służb i związane z tym komplikacje.

Działania podejmowane w celu zwalczania terroryzmu, zakładające zarówno integrację systemów bezpieczeństwa, jak i prowadzenie tylko luźnej współpracy lub zdawanie się wyłącznie na własne siły, mogą być prowadzone na pięciu płaszczyznach: politycznej, prawnej, wywiadowczej, policyjnej oraz militarnej.

Na **płaszczyźnie politycznej** zwalczanie terroryzmu odbywać się może za pomocą umów dwustronnych, albo umów wielostronnych. Umowy takie mogą być dokumentami ramowymi, wyznaczającymi dopiero drogę i sposób uchwalania konkretnych praw w dalszym zakresie, deklaracjami wyrażającymi wspólne stanowisko, czy też dalej idącymi dokumentami. Zakres porozumień może obejmować inne formy współpracy niż międzynarodowe umowy, sprowadzając się do wszelakiej kooperacji pomiędzy zainteresowanymi krajami. To także międzynarodowe negocjacje i wypracowywanie porozumienia w palących kwestiach. Działania polityczne będą tworzyć podstawę do działań prawnych, właśnie dzięki ratyfikacji umów międzynarodowych i potrzebie tworzenia własnego prawa w zakresie zgodnym z przyjętymi dokumentami.

Działania na **płaszczyźnie prawnej** w zwalczaniu terroryzmu to przede wszystkim regulacje prawne. Demokratyczne państwo nie może działać poza prawem, stąd potrzebne są jak najskuteczniejsze i odpowiednie do zagrożeń systemy prawne. Od strony praktycznej, to uprawnienia służb potrzebne w ich pracy. Przykładem jest zwiększanie zakresu legalnego stosowania podsłuchów i innych środków nadzoru, rewizji, łatwiejszy dostęp do danych i zapisów telekomunikacyjnych oraz uproszczona wymiana posiadanych wiadomości pomiędzy odpowiednimi służbami. Specjalne regulacje dotyczące aresztowania i zatrzymywania podejrzanych o terroryzm osób, dające służbom więcej uprawnień niż dotychczasowe rozwiązania. Od strony prewencji i karania może być to penalizacja groźnych zachowań i czynów w prawie karnym, obejmująca nie tylko karanie za dokonanie aktu terrorystycznego, ale również i za przygotowania do niego czy nawoływanie, albo udzielanie pomocy w jego realizacji.

Płaszczyzna wywiadowcza jest oceniana jako jedna najefektywniejszych form zwalczania terroryzmu. Polega głównie na uprzedzaniu terrorystów, aby można było wykryć kulminację ich działalności, w postaci zamachu, zanim do niego dojdzie. Żeby skutecznie prowadzić działania wywiadowcze, niezbędne są służbom odpowiednie uprawnienia - stąd istota wcześniejszych działań prawnych i politycznych. Zwiększyć efektywność wywiadowczą można tworząc jednostki i centra koordynujące starania wszystkich krajowych służb w zakresie zwalczania terroryzmu.

Dysponując odpowiednimi informacjami, dzięki wywiadowczemu rozpoznaniu, można przejść do **płaszczyzny policyjnej**. Sama policja prowadzić będzie dalsze rozpoznanie. Prócz tego, służby policyjne powinny podejmować działania, polegające na analizie otoczenia pod względem zagrożeń dla obiektów podatnych na możliwy atak oraz patrolowaniu i monitorowaniu miejsc szczególnie ważnych. Ponieważ terroryzm jest często powiązany z międzynarodową przestępczością, handlem narkotykami, przemytem broni czy praniem brudnych pieniędzy, policja zwalczając groźną przestępczość przyczynia się pośrednio do zmniejszenia siły organizacji terrorystycznych. Nie można zapominać o roli policji w czasie zamachu. To właśnie wyspecjalizowane policyjne jednostki kontrterrorystyczne, staną oko w oko z jego sprawcami. Zostaną użyte także, gdy w wyniku uzyskania informacji wywiadowczych uda się ustalić miejsce pobytu terrorystów, co będzie wymagało ich pochwycenia. Pomocna okazać się może współpraca z policjami innych państw oraz zrzeszającymi je organizacjami, w tym Europolem lub Interpolem.

Płaszczyzna militarna w tym ujęciu to ostatnia z nich. Działania militarne w zwalczaniu terroryzmu przybrać mogą w zasadzie dwie formy. Pierwsza, to typowe wojskowe uderzenie uprzedzające, na kraj, który uważany jest za źródło terroryzmu. Przykładem międzynarodowe operacje w Afganistanie i Iraku. Drugą formą działań, jest użycie narodowych sił zbrojnych wtedy, gdy atak terrorystyczny lub cała ich seria przybiera zbyt duże rozmiary, aby można było sytuację opanować wyłącznie siłami policyjnymi. Warto dodać, że nowoczesne siły zbrojne prócz wojsk konwencjonalnych, to także siły specjalne wyposażone w zaawansowaną technologię i uzależnione od danych wywiadowczych.

Można zauważyć, ze wszystkie wymienione płaszczyzny uzupełniają się wzajemnie, tworząc swego rodzaju kompleksowy system zwalczania terroryzmu, obejmujący podstawowe formy działalności państwa i jego służb.

Tobiasz Małysa

Pięć płaszczyzn zwalczania terroryzmu

I. Działania polityczne
II. Działania prawne
III. Działania wywiadowcze
IV. Działania policyjne
V. Działania militarne

Źródło:

K. Liedel, Zwalczanie terroryzmu międzynarodowego w polskiej polityce bezpieczeństwa, Warszawa, 2010.

Globalna Strategia Zwalczania Terroryzmu przyjęta przez ONZ wymienia środki, jakimi można przeciwdziałać przyczynom powstawania terroryzmu i ekstremizmu, oraz jak zapobiegać i zwalczać terroryzm.

By możliwe było zwalczanie terroryzmu potrzebne są dokumenty regulujące wszystkie kwestie prawne związane z konkretnymi działaniami służącymi eliminacji tego zjawiska. Ze względu na jego globalny zasięg ważnym czynnikiem jest także współpraca organizacji międzynarodowych.

Organizacje takie jak: **Organizacja Narodów Zjednocznych**, **NATO i Unia Europejska** opracowały dokumenty (konwencje, dyrektywy, protokoły), które służą nie tylko zwalczaniu, ale przede wszystkim przeciwdziałaniu terroryzmowi.

ONZ

ONZ jako organizacja międzynarodowa mobilizuje swoich członków do czynnego angażowania się w zapobieganie i zwalczanie terroryzmu. W tym celu dnia 8 września 2006 r. Zgromadzenie Ogólne ONZ przyjęło **Globalną Strategię Zwalczania Terroryzmu** – *UN Global Counter-Terrorism Strategy*.

Dokument ten wymienia środki, jakimi można przeciwdziałać przyczynom powstawania terroryzmu i ekstremizmu. Jak zapobiegać i zwalczać terroryzm, a także w jaki sposób chronić prawa człowieka i zapewnić rządy prawa w czasie prowadzenia walki z terroryzmem.

Na forum ONZ trwają obecnie prace nad przyjęciem **Kompleksowej Konwencji** w sprawie **Zwalczania Terroryzmu** - *Comprehensive Convention on International Terrorism* (CCIT). Jednak istnieje kilka kwestii spornych, które opóźniają jej przyjęcie. Chodzi m.in. o jednolitą definicję terroryzmu uznaną przez wszystkich członków, określenie różnic między walką narodowo-wyzwoleńczą, a działaniami terrorystycznymi. **Rada Bezpieczeństwa Organizacji Narodów Zjednoczonych** uchwaliła także kilka rezolucji dotyczących przeciwdziałania i zwalczania terroryzmu:

– **Rezolucja 1267** (1999 r.) – dotyczy ona sankcji wobec Al-Kaidy i Talibów. Państwa będące członkami ONZ zostały zobligowane do zamrożenia kont bankowych, co do których istnieje podejrzenie, że są wykorzystywane do finansowania działalności Al-Kaidy. Mają również zapobiegać przekraczaniu granic przez osoby wspierające i mające jakikolwiek związek z tą organizacją poprzez materialne, techniczne, szkoleniowe wsparcie.

– **Rezolucja 1368** (2001 r.) – Organizacja Narodów Zjednoczonych w tej rezolucji potępiła ataki terrorystyczne z 11 września 2001 r. i uznała je za zagrażające pokojowi oraz bezpieczeństwu na świecie. Wszystkie państwa członkowskie zostały wezwane do ratyfikacji konwencji antyterrorystycznych uchwalonych przez tą organizację.

– **Rezolucja 1373** (2001 r.) – obliguje członków ONZ do pociągania do odpowiedzialności karnej osoby lub organizacje, które finansują terroryzm, oraz do nie udzielaniu *pomocy podmiotom lub osobom zaangażowanym w działalność terrorystyczną*, a także przekazywanie innym państwom informacji dotyczących działalności terrorystycznej.

– **Rezolucja 1540** (2004 r.) oraz **1673** (2006 r.) – *które dotyczą zapobieganiu proliferacji broni masowego rażenia (CBRN – broń chemiczna, biologiczna, radiologiczna i nuklearna)*.

NATO

Podczas szczytu Sojuszu w Pradze w 2002 r. została przyjęta **Militarna Koncepcja Obrony przed Terroryzmem** – *The Military Concept for Defence against Terrorism* oraz **Plan Działań Partnerstwa na Rzecz Walki z Terroryzmem** – *The Partnership Action Plan against Terrorism* (PAPT).

Dokument ten powstał w celu koordynacji działań podjętych w walce z terroryzmem i zacieśnienia współpracy między państwami członkowskimi, poprzez budowę wzajemnego zaufania, a także wymianę informacji. Wskazuje również na potrzebę udzielania wzajemnej pomocy w wypadku przeprowadzenia ataku terrorystycznego na terytorium, któregokolwiek z członków NATO.

Aby wymiana informacji wywiadowczych między sojusznikami odbywała się skutecznie i była na odpowiednim poziomie podczas szczytu w Stambule w 2004 r. została powołana do życia **Jednostka Wywiadu ds. Zagrożenia Terrorystycznego** – *The Terrorist Threat Intelligence Unit* (TTIU). Został przyjęty **Program Prac na Rzecz Obrony przed Terroryzmem** – *The Defence Against Terrorism Programme of Work* (DAT), w którym to mowa jest o wspomaganiu przez państwa członkowskie badań naukowych i prac w celu udoskonalania technologii wspomagających zwalczanie terroryzmu (np. system AWACS).

UE

Dnia 3 grudnia 2003 r. Unia Europejska przyjęła **Europejską Strategię Bezpieczeństwa** – *The European Security Strategy*, w której to terroryzm poza konfliktami regionalnymi, upadkiem państwa oraz przestępczością zorganizowaną został zaliczony do największych zagrożeń dla bezpieczeństwa UE.

Po zamachach w Madrycie w 2004 r. i w Londynie w 2005 r. Rada Europejska przyjęła **Strategię w sprawie zwalczania terroryzmu** – *The EU Counter-Terrorism Strategy*, w której UE zobowiązana jest do zwalczania terroryzmu na całym świecie, aby obywatele Unii żyli w poczuciu bezpieczeństwa, wszystkie działania do tego zmierzające maja odbywać się z poszanowaniem praw człowieka. W tym samym roku została przyjęta **Strategia w Sprawie Zwalczania Radykalizacji Postaw i Rekrutacji do Organizacji Terrorystycznych** – *The European Union Strategy for Combating Radicalisation and Recruitment to Terrorism*. UE prowadzi również dialog z państwami z poza Unii, propagując dokumenty dotyczące zwalczania terroryzmu. Podejmuje także działania w obrębie inicjatyw regionalnych np. ASEM – *The Asia-Europe Meeting*.

Wszystkie wymienione organizacje mimo różnic programowych mają jeden nadrzędny cel – nie dopuścić by terroryzm stał się plagą XXI wieku.

Artykuł jest wstępem do szerszego cyklu omawiającego poszczególne dokumenty, a kolejne opracowania będą ukazywały się w następnych numerach biuletynu.

Anna Rejman

Źródła:

- T. Aleksandrowicz, Terroryzm międzynarodowy, Wyd. Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008
- http://www.unic.un.org.pl/terroryzm/strategia.php
- http://europa.eu

Terroryzm chemiczny można podzielić na dwa podtypy: pierwszy z wykorzystaniem bojowych środków trujących, drugi za pomocą związków chemicznych podwójnego działania.

Halabdża - *Chemiczny Ali*, *Aum Shinrikyõ – Najwyższa Prawda*. Łączy ich sarin, bezbarwny i bezwonny, lecz silnie toksyczny gaz. Został użyty (wraz z tabunem, iperytem i gazem VX) 16 marca 1988 r. w kurdyjskim mieście Halabdża, na północy Iraku. Rozkaz wydał *Chemiczny Ali* – Ali Hassan al – Madżid, kuzyn Saddama Husajna. Swoje bestialstwo (śmierć poniosło 5 tys. osób) przypłacił życiem, został powieszony w 2010 r.

Drugim znanym, współczesnym, atakiem z użyciem sarinu było miasto Matsumoto – w Japonii. 8 zabitych i ponad 200 zatrutych – to efekt rozlania ok. 30 litrów sarinu w 1994 r. Najsłynniejszym aktem terroryzmu chemicznego był zamach przeprowadzony 20 marca 1995 r. w tokijskim metrze. Zginęło 12 osób, a ponad 5 tysięcy było poszkodowanych. Obydwa ataki zostały przeprowadzone przez członków sekty *Najwyższa Prawda* Shõkõ Asahary. Jeden z ostatnich aktów tej historii miał miejsce 31 grudnia 2011 r., gdy członek sekty (odpowiedzialny za atak w metrze), oddał się w ręce policji. Był to 46-letni Makoto Hirata.

Przedstawione przypadki (Irak i Japonia) pokazują nam, że możliwy jest atak za pomocą tego typu broni. Terroryzm chemiczny można podzielić na dwa podtypy: pierwszy z wykorzystaniem bojowych środków trujących, drugi za pomocą związków chemicznych podwójnego działania. BŚT to m.in. środki paralityczno-drgawkowe (tabun, sarin, soman, VX) oraz środki parzące (iperyt czy luizyt zwany rosą śmierci). Różnego rodzaju ugrupowania terrorystyczne, bojówki lub ruchy partyzancko-wyzwoleńcze mogą wejść w posiadanie tych środków głównie poprzez kradzież lub kupno amunicji, bądź samych związków chemicznych od państw posiadających je w swoim arsenale. Jest to o tyle niebezpieczne, że ugrupowania mogą pozyskać BŚT najwyższej jakości, często w amunicji przystosowanej do ich przenoszenia i użycia. Produkcja własnymi siłami jest mało prawdopodobna ze względu na skomplikowany proces technologiczny. Wyjątkiem była sekta *Najwyższa Prawda*, a i tak sarin przez nich wyprodukowany był bardzo niskiej jakości (przyjmuje się, że miał od 5 do 30% „doskonałości" sarinu bojowego).

Znacznie poważniejszym zagrożeniem są związki chemiczne podwójnego przeznaczenia – np. chlor, fosgen, fluor, cyjanowodór; które są powszechnie używane w przemyśle. Co za tym idzie – łatwo dostępne. Najszybszym i najłatwiejszym sposobem ataku byłoby wysadzenie np. transportu takich środków czy urządzeń technologicznych je wykorzystujących lub magazynów. Eksplozja rozprasza substancje powodując skażenie powietrza, terenu i ludzi[1]. Taki atak, poza znacznie większymi możliwościami porażania organizmów żywych (w porównaniu z konwencjonalnymi atakami np. VBIED), może być bardziej dotkliwy dla gospodarki i finansów zaatakowanego regionu (państwa). Usuwanie skażenia jest kosztowne jak i czasochłonne.

Ważne zatem jest, by państwa posiadające broń chemiczną dbały o właściwe i skuteczne zabezpieczenie ich składowania, a wszyscy ze szczególną uwagą podchodzili do zabezpieczenia przemysłowych środków chemicznych.

[1] Por. katastrofa w Indiach, w mieście Bhopal w 1984 r.

Zob. więcej:

– http://manhaz.cyf.gov.pl/manhaz/WAT/Dokumentacja/CHEMIA.pdf

– http://rop.sejm.gov.pl/1_0ld/opracowania/pdf/material29.pdf

– http://www.malopolskie.pl/Pliki/2009/wystapenieADRmaj2009.pdf

– http://www.bbc.co.uk/birmingham/content/articles/2006/06/22/

Rodzaje alarmów, treść komunikatów ostrzegawczych, sygnały alarmowe:

– http://www.zanet.pl/telefony/alarm.html

Zachowanie podczas alarmu chemicznego – wg wytycznych MSW:

– http://www.msw.gov.pl/portal/pl/109/242/

Sygnał alarmu o skażeniach środkami chemicznymi lub biologicznymi nadawany jest: za pomocą syren (przez 3 minuty przerywany dźwięk - 10 sekund głos syreny, 25 sekund przerwy, 10 sekund syrena, 15 sekund przerwy), za pośrednictwem radia, telewizji i radiowęzłów lub pojazdów wyposażonych w megafony.

Jeżeli jedziesz samochodem:

– wyłącz dmuchawy i zamknij okna, włącz zamknięty obieg powietrza, słuchaj radia (najlepiej lokalnego) i stosuj się do poleceń służb ratowniczych,
– podjedź do pierwszego zamieszkanego budynku i postępuj według wskazówek dla osób przebywają cych poza budynkiem.

Jeżeli jesteś w budynku:

– pozostań w budynku,
– wpuść do niego zagrożonych przechodniów,
– poinformuj innych mieszkańców o zagrożeniu,
– zamknij drzwi i okna,
– wyłącz klimatyzację i wentylatory, pozalepiaj wywietrzniki, pozamykaj wywietrzniki w ramach okiennych,
– znajdź pomieszczenia bez okien,
– unikaj przebywania w piwnicach i innych nisko położonych częściach budynku,
– unikaj niepotrzebnego zużycia tlenu,
– włącz radio lub telewizor (najlepiej stację lokalną).

Jeżeli jesteś poza budynkiem:

– znajdź najbliższy zamieszkany budynek,
– w miarę możliwości poruszaj się prostopadle do kierunku wiatru, chroń drogi oddechowe (np. oddychaj przez chusteczkę do nosa),
– umyj dokładnie twarz, włosy i ręce, oczyść oczy i uszy,
– w przypadku kontaktu z niebezpiecznymi substancjami, zostaw odzież wierzchnią i obuwie przed domem.

Jeżeli doszło do skażenia:

– nie dotykaj i nie wąchaj podejrzanych przedmiotów, nie sprzątaj proszku, nie ścieraj cieczy,
– aby zapobiec rozprzestrzenianiu się substancji, przykryj ją np. kocem,
– pozamykaj okna oraz drzwi i wyłącz klimatyzację, nie dopuść do przeciągów,
– opuść pomieszczenie i nie wpuszczaj do niego nych osób,
– umyj dokładnie ręce wodą i mydłem,
– zdejmij ubranie, które miało kontakt z podejrzaną substancją i włóż do plastikowego worka,
– umyj się pod prysznicem,
– po kontakcie z podejrzanymi substancjami nie jedz, nie pij i nie pal,
– wszystkie osoby, które miały kontakt z podejrzaną substancją albo znalazły się w odległości ok. 5 m od niej, powinny się zgłosić na policję.

Jeżeli doszło do skażenia pomieszczeń aerozolami:

– wyłącz wentylatory i klimatyzację w całej okolicy,
– zamknij okna i drzwi, opuść pomieszczenie,
– wyłącz klimatyzację w budynku,
– sporządź listę wszystkich obecnych osób i udostępnij ją policji.

Piotr Podlasek

Dzisiejsi terroryści działają z rozmachem, w każdym zakątku świata, używając wszelkich metod, aby osiągnąć swój cel. Swoimi działaniami chcą spowodować jak największe zniszczenia, spektakularne i medialne, aby siać panikę, tak wśród władz państwowych jak i społeczeństw. Dlatego środki masowego rażenia są atrakcyjne dla terrorystów. Ich użycie spowodowałoby ogromne zniszczenia. Zagrożenie ich użyciem stanowi silną kartę przetargową.

Jednym z niebezpieczniejszych środków masowego rażenia jest broń biologiczna, która w rękach terrorystów z racji swoich właściwości (zabójcze mikroorganizmy, wytwarzane przez nie toksyny), może służyć do wywoływania epidemii chorób zakaźnych wśród ludzi i zwierząt. Środkami wykorzystywanymi jako broń biologiczna są bakterie, chlamydie, grzyby, riketsje, toksyny i wirusy. Najgroźniejszymi i najbardziej powszechnymi patogenami, które można wykorzystać są laseczki wąglika, pałeczki dżumy, które występuje u gryzoni głównie w obu Amerykach, Afryce, Azji i płd.- wsch. Europie. Tularemia, podobnie jak dżuma, pałeczki salmonelli, wirusy gorączek krwotocznych: Denga, Ebola, Hanta, Junin, Sabia są równie groźne jak wymienione powyżej.

Zdaniem ekspertów zagrożenie użyciem broni biologicznej przez terrorystów w ostatnich latach znacznie wzrosło. Incydent, który miał miejsce w USA w 2001 r. rozsyłanie listów zawierających pałeczki wąglika, spowodował śmierć 5 osób oraz 17 zachorowań. Wywołał psychozę strachu wśród społeczeństwa USA obawiającego się takiej przesyłki. Ponadto zamknięto skażone obiekty oraz przeprowadzano ich dekontaminację, która trwała nawet 26 miesięcy i pochłonęła 130 mln dolarów. W ostatnim czasie w USA wystąpiło zagrożenie użycia środków biologicznych za pomocą przesyłania ich w listach. Przesyłki mają otrzymywać senatorzy. (http://biznes.onet.pl/ostrzezenie-przed-atakiem-biologicznym-na-kongres-,18512,5034954,1,news-detal).

Broń biologiczna może być wygodnym narzędziem ataków terrorystycznych z powodu łatwego jej ukrycia i przenoszenia – jest bezwonna, często bezbarwna, a obecne systemy wykrywania i monitorowania nie gwarantują sukcesu. Jest bronią stosunkowo tanią. W wymiarze do użytych środków finansowych wywołane skutki (użycie w dobrych warunkach atmosferycznych nad zaludnionym miastem 50 kg laseczek wąglika) spowodowałoby śmierć około 100 tys. ludzi. Atak bronią biologiczną na systemy infrastruktury krytycznej niesie za sobą szczególne niebezpieczeństwo dla ludności, może nastąpić pod postacią zatrucia ujęcia wody, skażenia produktów spożywczych w zakładach produkujących żywność, rozpylenia w miejscach częstych migracji np. stacjach metra, lotniskach. Broń biologiczna jest bardzo groźna z powodu okresu, po którym pojawią się objawy choroby, nieświadomość „nosicieli", którzy niezwłocznie powinni poddać się kwarantannie. Nieświadomość może doprowadzić do zarażenia (przy odpowiednich warunkach) większej ilości osób, wręcz epidemii.

Pomimo szeregu zalet broni biologicznej posiada ona wady. Stanowi duże zagrożenie dla zamachowca, wiele z jej rodzajów jest wrażliwych na warunki atmosferyczne i promienie słoneczne. Nie ma skutecznej metody wczesnego wykrywania środków biologicznych. Ważne jest jej rozpoznanie już po użyciu, żeby ograniczyć skażony teren, podjąć szybkie i właściwe środki ratownicze oraz kwarantannę. Same regulacje międzynarodowe dotyczące zakazu produkcji, składowania i użycia broni biologicznej mogą okazać się niewystarczające. Skuteczny system wczesnego wykrywania i ostrzegania powinien zawierać w sobie odpowiedni monitoring dużego obszaru geograficznego z informacjami dotyczącymi ilości zachorować i nawet niewielkich odchyleń od normy, pojawienia się nietypowych objawów chorobowych. Ważne jest przygotowanie przez odpowiednie instytucje planu reagowania w wypadku ataku bioterrorystów. Niezbędne szkolenia i ćwiczenia praktyczne właściwych służb, kooperacja między nimi oraz wymiana informacji i doświadczeń z instytucjami na całym świecie.

Tomasz Tylak

Ekoterroryzm – zielona strona terroryzmu

Terroryzm w dzisiejszych czasach ma wiele twarzy, może przejawiać się poprzez zamachy bombowe skierowane na strategiczne obiekty, przypadkową ludność cywilną lub konkretne osoby. Może przybierać nieco łagodniejszą postać, bez rozlewu krwi, wywierając jednak naciski na rządy, instytucje, czy przedsiębiorstwa.

Ekoterroryzm posługuje się szeroką gamą metod począwszy od prowadzenia akcji protestacyjnych, poprzez wykorzystywanie prawa i luk prawnych w celu blokowania różnego rodzaju inwestycji pod pretekstem szkodliwości dla środowiska naturalnego, sięga po radykalne metody przestępcze, używa siły, lub przemocy wobec przedsiębiorstw i osób fizycznych. Początków ekologii na świecie można się doszukiwać już w latach siedemdziesiątych, gdy Arne Naess zaczął propagować „pogłębianie naszej identyfikacji ze wszystkimi formami życia i z Gają, naszą piękną, starą planetą", co skutkowało powstaniem nowych ruchów ekologicznych.

Nie każdy ekolog i działacz na rzecz ochrony środowiska naturalnego i zwierząt jest ekoterrorystą, niestety te różnice często zacierają się. Gdzie kończy się szlachetny cel ratowania natury, a zaczyna ekoterroryzm? Trudno jednoznacznie stwierdzić, ekolodzy swoimi działaniami często łamią prawo: wylanie farby na futro właściciela, niszczenie wyposażenia rzeźni, obiektów myśliwskich, szpikowanie drzew gwoździami, które doprowadziło już do śmierci drwali, podpalenia składów i magazynów chemicznych, taranowanie statków wielorybniczych. Na pewno można to uznać za radykalne i niezgodne z prawem metody.

Liczne blokady inwestycji przeprowadzane przez ekologów mogą być groźne w skutkach – warto wspomnieć sprawę przebudowy wałów przeciwpowodziowych w Warszawie, inwestycja już od 9 lat jest skutecznie blokowana przez miłośników ptaków. Swoisty haracz ci sami obrońcy ptaków wymogli za odstąpienie od blokady budowy lotniska w Modlinie, gdzie od inwestora zażądali 7 mln zł na wykupienie 700 ha bagien i przeniesienia tam ptaków z Modlina. Głośna sprawa blokowania budowy parków wiatrowych w Polsce, jest najlepszym przykładem ekoterroryzmu, gdzie wysnuwane zarzuty przez organizacje ekologiczne o tym, że łopaty wiatraków będą stwarzać niebezpieczeństwo dla ptaków, zagrożenia dla zdrowia ludzi (poprzez rzekomo wytwarzane infradźwięki), szerzono tezy o nieopłacalności inwestycji. Opinie głoszone przez ekologów zostały obalone przez kompetentne organy i specjalistów. Szerzenie wśród społeczności lokalnej, gdzie te wiatraki mają funkcjonować fałszywej perspektywy zagrożenia zdrowia, jest skuteczną metodą wykorzystywania naiwności i braku odpowiedniej wiedzy.

Blokowanie inwestycji w Polsce przez „ekologów" jest coraz bardziej powszechne – rozbudowa szpitala dziecięcego w Krakowie – Prokocimiu – sprzeciw wycince lasu (konkretnie samosiejek), przebudowa i podwyższenie krakowskiego wieżowca zwanego szkieletorem - zagraża przyrodzie i pogorszy się panorama miasta.

Kilkunastu działaczom organizacji Greenpeace, domagającym się zmiany polityki energetycznej rządu, udało wejść na jedną z ponad 100 metrowych chłodni kominowych Elektrowni Bełchatów (obiekt infrastruktury krytycznej), przez kilka godzin malowali farbą na kominie napis "Stop CO2", elektrownia oceniła straty w wyniku akcji ekologów na co najmniej 100 tys. zł.

Ekoterroryzm w Stanach Zjednoczonych uznany jest przez FBI za jedno z największych zagrożeń wewnętrznych państwa, które jak widać i w Polsce zyskuje powoli na sile. Zapobiegać tego typu zjawiskom nie jest łatwo, ale aby to czynić należy nawiązać odpowiedni dialog między rządami, a organizacjami ekologicznymi, a skrajne ugrupowania ekologiczne wpisać na listę organizacji terrorystycznych. Według mojej opinii należy zaostrzyć przepisy prawa karnego, uwzględniając zagrożenia niesione przez ekoterroryzm. Niezbędne jest zapewnienie młodemu pokoleniu rzetelnej edukacji w zakresie ekologii.

Tomasz Tylak

Cyberterroryzm w zarysie

Istnieje wiele definicji cyberterroryzmu, każdy kraj w zasadzie wypracował swoją definicję tego zjawiska. Według ABW „cyberterroryzmem określamy wykorzystywanie zdobyczy technologii informacyjnej w celu wyrządzenia szkody. Wysoki poziom rozwoju technologicznego przyczynia się do poprawy zarządzania wieloma sferami życia politycznego, społecznego i gospodarczego, ale jednocześnie uzależnia państwo od sprawności i bezpieczeństwa infrastruktury krytycznej. Atak na jeden z elementów systemu może zakłócić funkcjonowanie pozostałych („efekt domina"), ponieważ są one ściśle ze sobą powiązane.

Najpoważniejszym źródłem zagrożeń dla sieci teleinformatycznych – obok niedoskonałości rozwiązań technicznych – są celowe działania. Mogą przyjmować formę:

- zakłócenia działania systemów;
- nieupoważnionej danych;
- łamania zabezpieczeń, co pozwala na przejęcie kontroli nad poszczególnymi elementami infrastruktury (np. na wypadek wojny).

Po tę ostatnią metodę mogą sięgać służby specjalne nieprzyjaźnie nastawionych państw oraz organizacje terrorystyczne. Z kolei grupy przestępczości zorganizowanej mogą być zainteresowane wykradaniem danych lub dokonywaniem nieupoważnionych zmian np.: systemach i sieciach instytucji finansowych."[1]

W USA działań hakerskich nie traktuje się jako cyberterroryzmu, chyba, że dokonywane są one przez organizacje terrorystyczne. Próby uzyskania nieuprawnionego dostępu do sieci wojskowych czy rządowych, które mają na celu kradzież danych (tajnych informacji) klasyfikować powinniśmy raczej jako szpiegostwo niźli sam akt cyberterroryzmu. Taka sama sytuacja dotyczy włamań do systemów bankowych, których celem jest opróżnienie kont. Tę działalność powinno klasyfikować się jako klasyczną działalność kryminalną, a nie jak w pierwszym zdaniu definicji cyberterroryzmu umieszczonej na stronie ABW do cyberterroryzmu. Jednak dane zdobyte w czasie włamań cybernetycznych pierwotnie nie zaliczanych do cyberterroryzmu mogą posłużyć do prowadzenia tzw. I-War czyli wojny cybernetycznej (jest to nowy rodzaj konfliktu), a pieniądze zdobyte przez cyberkradzieże mogą z łatwością posłużyć do finansowania ataków terrorystycznych i działalności propagandowej terrorystów.

Metody używane przez cyberterrorystów mogą być różne w zależności od celu jaki chcą osiągnąć soft-terroryści. Jednak wśród najczęściej stosowanych metod pojawiają się takie jak tworzenie sieci botnet (tzw. sieci zombie), których celem jest wykonywanie ataków np. DDoS na z góry ustalone serwery. W ten sposób możliwa jest blokada dostępu do usług tego serwera, a dzieje się tak przez wygenerowanie przez sieć zombie bardzo dużej ilości połączeń z serwerem, których nie jest on w stanie obsłużyć. W ostatnich czasach mieliśmy do czynienia z tym typem podczas ataków grupy Anonymus na rządowe serwery. Jest to często stosowana metoda, gdyż w sieci jest dużo różnego oprogramowania umożliwiającego ich tworzenie i wykonywanie ataków DDoS. Każdy komputer bez zainstalowanej należytej ochrony antywirusowej jest łatwym celem dla ludzi chcących stworzyć takie sieci.

Inną często spotykaną metodą jest łamanie haseł dla konta administratora serwera i przejmowanie nad nim kontroli. Jest to o tyle niebezpieczne, że w przypadku infrastruktury krytycznej i potencjalnego przejęcia kontroli nad nią przez osoby niepowołane lub wręcz wrogo nastawione do państwa może się to zakończyć całkowitą dezorganizacją działań np.. pomocowych w sytuacjach kryzysowych.

Jednak bylibyśmy w błędzie licząc, że cyberterroryści uciekają się tylko do działań technicznych aby osiągnąć swój cel. W obecnych czasach w obrębie ich zainteresowania są działania „socjotechniczne" a wszystko przez to, że łatwiej „złamać" człowieka niż hasło. W wielu przypadkach jest to mniej kosztowne, tak pod względem niezbędnego czasu jak i ryzyka.

Bernadetta Terlecka

[1] Definicja podana na stronie http://www.abw.gov.pl/

Metody wykorzystywane w cyberataku

Koniec XX i początek XXI wieku przyniósł ogromne zmiany w postępie cywilizacyjnym. Nowe technologie, zmiany polityczne, społeczne i kulturowe sprawiły, że życie stało się o wiele łatwiejsze. Przemiany przyniosły ze sobą także wiele zagrożeń dla bezpieczeństwa i funkcjonowania państwa w tym zjawisko cyberterroryzmu. Cyberterroryzm „to politycznie motywowany atak na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na państwie lub instytucji daleko idących politycznych i społecznych celów w szerszym rozumieniu tego słowa, a także groźba dokonania takiego ataku; jest to również użycie Internetu do komunikowania się, propagandy i dezinformacji przez organizacje terrorystyczne."[1] Ataki przeprowadzane są za pomocą wielu różnych metod. Poniżej zamieszczone zostały najczęściej stosowane metody, zarówno przez cyberterrorystów, przestępców i hakerów:[2]

Wirus – *To samo reprodukujący się kod, uszkadzający dane lub programy, zmieniający działanie sprzętu.* Po uruchomieniu programu następuje aktywacja kodu, który dołącza do innych programów i zaraża coraz to większe obszary w komputerze. Wirusy możemy podzieli na kilka odmian: bootsektora, makrowirusy, plikowe, złożone, polimorficzne, ukryte, dzikie itd.

Robak – *To program, którego zadaniem jest rozprzestrzenianie się w sieci komputerowej.* Może zachowywać się jak wirus, włamuje się do komputerów w podobny sposób jak hakerzy. Atakuje słabe punkty w poczcie elektronicznej, stronach WWW, programach obsługujących czaty, IRC, ICQ.

Bakteria (królik) – *To program, który wprost nie powoduje uszkodzenia pliku, jego zadaniem jest rozmnażanie.* Dzieli się na dwie kopie i uruchamia w środowisku zasobów danych. Tworzy też dwa nowe pliki, które są kopią programu wyjściowego. Te programy będą powtarzać tą czynność, aż do momentu zajęcia ogromnej ilości pamięci procesora, przestrzeni dyskowej i innych zasobów.

Bomba logiczna – *To rodzaj wirusa komputerowego, który przez długi czas może być nieaktywny do momentu wystąpienia określonego zdarzenia. Uaktywnienie prowadzi do zniszczenia lub zdeformowania sprzętu i oprogramowania*. Aktywację może wywołać obecność odpowiednich plików, określona data lub użytkownik uruchamiając aplikację.

Koń trojański – To program wykonujący niepożądane działania np. usuwanie plików, ponowne formatowanie dysku lub przesyłanie danych do swego twórcy, bez zgody użytkownika programu i jego wiedzy. Można go umieścić w prawie każdym programie. Jest rozpowszechniany za pomocą poczty elektronicznej lub Internetu. Stanowi doskonałe narzędzie w działalności terrorystycznej można penetrować zasoby informacyjne obiektu, który ma stać się celem ataku nie budząc podejrzeń.

Chipping – To umieszczanie w komputerach chipów, zawierających programy umożliwiające dostęp do systemu lub wad konstrukcyjnych powodujących uszkodzenia komputera.

Tylne drzwi – To nieautoryzowane w dokumentacji możliwości stworzone przez programistów w celu naprawienia w późniejszym czasie błędów w napisanych przez siebie aplikacjach. Czasami tylko po to by odczytać zawartość dysku użytkownika bez jego wiedzy i zgody. Może dochodzić wówczas do zdalnego kasowania plików zmiany ich nazwy, kopiowania danych i wprowadzania wirusów.

Spoofing – Jest to podszywanie się pod jednego z użytkowników systemu, który ma własny adres IP. *Stosuje się także programy podszywające się pod legalny serwer lub proces systemowy.* Atak tego typu ma na celu obejście zabezpieczeń zastosowanych przez administratora sieci wewnętrznej.

Hijacking – *Polega na przechwyceniu transmisji odbywającej się między dwoma systemami. Umożliwia dostęp do szczególnie chronionych programów lub informacji.*

Sniffing – *To śledzenie ruchu w sieci, stosowany jest specjalny program wychwytujący w sieci wiadomości i kopiujący wybrane (m. in. dane osobowe, hasła dostępu i wiele innych cennych informacji) na dysk.*

DOS (Denial of Service) – *To odmowa usługi, blokowanie pojedynczej usługi sieciowej bądź blokowanie pracy całego serwera przez przeciążenie go za pomocą niezliczonej ilości zapytań.*

E-mail bombing – To wysyłanie dużej ilości e-maili w celu zablokowania działania poczty elektroniczne.

Radio frequency – To ataki z wykorzystaniem częstotliwości radiowej, używane są *urządzenia emitujące promieniowanie elektromagnetyczne należące do widma radiowego*, które powodują zniszczenie urządzeń elektronicznych i zbiorów informatycznych.

Anna Rejman

[1] K. Liedel, Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego, Toruń 2006, s. 36.

[2] Opracowanie własne na podstawie: Liedel K., Piasecka P, Cyberterroryzm, [w:] Liedel K., Piasecka P (red), Jak przetrwać w dobie zagrożeń terrorystycznych, Warszawa 2007, s. 42-43; A. Bógdał-Brzezińska, M. F. Gawrycki, Atak cyberterrorystyczny, [w:] A. Bógdał-Brzezińska, M. F. Gawrycki (red), Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie, Warszawa 2003, s. 145-152.

Metody zwiększania cyberbezpieczeństwa

W raporcie o stanie bezpieczeństwa cyberprzestrzeni RP w 2010 roku, przygotowanym przez Rządowy Zespół Reagowania na Incydenty Komputerowe (raport za rok 2011 ma ukazać się niebawem), autorzy w rozdziale "Minimalne zalecenia dla administratorów systemów jednostek administracji państwowej" wymieniają szereg istotnych wskazówek, które mogą przyczynić się do zwiększenia bezpieczeństwa komputerów oraz całych sieci. Spróbujmy na podstawie informacji tam zawartych dokonać podsumowania i rozwinięcia najważniejszych zaleceń, przydatnych nie tylko administratorom, ale również i użytkownikom:

1. Podstawą bezpiecznego systemu jest posiadanie systemu legalnego i jego ciągłe aktualizowanie. Rezygnacja z automatycznych aktualizacji może narazić go na różnego rodzaju luki, prowadzące nie tylko do niestabilności czy spadku wydajności, ale także umożliwić cyberatak.
2. Instalację oprogramowania antywirusowego (najlepiej wyposażonego w zaporę sieciową) powinno przeprowadzić się jak najszybciej po instalacji surowego systemu, jeszcze przed instalacją innych programów oraz przed właściwym użytkowaniem komputera. Warto posiadać oprogramowanie antyspamowe.
3. Przy instalacji oprogramowania pobranego z Internetu należy zachować wysoką ostrożność, skanując pobrane pliki i upewniając się co do ich wiarygodności. Oprogramowaniem antywirusowym powinno skanować się wszystkie pobrane pliki, co do których bezpieczeństwa nie możemy mieć 100% pewności. Instalacja oprogramowania powinna być możliwa tylko przez administratora sieci.
4. Aktualizacja musi dotyczyć nie tylko samego systemu operacyjnego oraz oprogramowania antywirusowego. Praktycznie każdy zainstalowany program powinien być aktualizowany, jeśli istnieje taka możliwość, również sterowniki sprzętowe. Aktualizacje pobierać należy ze strony producenta.
5. Konta użytkowników mających korzystać z systemu należy odpowiednio przemyśleć pod względem ich organizacji i przydzielonych im uprawnieniom. Powinna obowiązywać zasada tzw. dostępu minimalnego, gdzie użytkownik domyślnie nie posiada żadnych praw dostępu, a otrzymuje je wyłącznie do potrzebnych mu zasobów (a nie odwrotnie). Konta nieużywane (np. gość) powinny być zablokowane. Nie należy pracować ponadto z uprawnieniami administratora, gdy wykonuje się tylko czynności biurowe.
6. Dysk twardy dobrze podzielić jest na partycję systemową (C) oraz partycję roboczą (D). Wszelkie dokumenty oraz inne pliki nad którymi się pracuje najlepiej przechowywać na partycji D, którą dodatkowo można zaszyfrować. Należy regularnie wykonywać kopie zapasowe dysku twardego, najlepiej na zewnętrzny nośnik.
7. Należy dobrze zabezpieczyć sieć WiFi lub zrezygnować z niej na rzecz połączenie komputerów kablem. Dobry poziom zabezpieczeń sieci bezprzewodowej daje szyfrowanie WPA2. Absolutnie nie należy korzystać z sieci nieszyfrowanych, także w miejscach poza pracą – informacje przesyłane w takich sieciach bardzo łatwo można przechwycić.
8. Usługi nieużywane w systemie, jak np. udostępnianie drukarki powinny być wyłączone.
9. Użytkownicy nie powinni mieć możliwości wnoszenia i wynoszenia nośników danych, gdyż grozi to nie tylko przypadkowym lub celowym wyciekiem poufnych danych, ale także, nieświadomym zakażeniem systemu komputerowego np. wirusem poprzez pamięć USB.
10. Użytkownicy komputerów powinni być przeszkoleni w zakresie zagrożeń informatycznych i metod ochrony przed nimi. Powinni być zaznajomieni z wewnętrzną polityką bezpieczeństwa komputerowego. Muszą znać zasady tworzenia i używania bezpiecznych haseł. Należy zdać sobie sprawę, że nie istnieje całkowicie bezpieczny system, a włamanie się do niego lub jego uszkodzenie jest tylko kwestią użytego czasu oraz środków.

Pamiętajmy, że są to minimalne zalecenia. Nie ustrzegą one nas przed bardzo poważnymi atakami, lecz powinny zabezpieczyć komputery przed atakami najprostszymi, najłatwiejszymi do przeprowadzenia.

Tobiasz Małysa

Zobacz więcej:

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2010 roku. Minimalne zalecenia dla administratorów systemów jednostek administracji państwowej. s. 54-56
– http://cert.gov.pl/portal/cer/57/422/Raport_o_stanie_bezpieczenstwa_cyberprzestrzeni_RP_w_2010_roku.html

Nie taka ACTA straszna jak ją malują

Przez kilkanaście dni na ulice polskich miast wychodziło wielu młodych (ciałem albo duchem) ludzi. Protesty internautów to jednak nie tylko zgromadzenia na ulicach, to również grupy hakerskie (w tym np. Anonymus), które pod pretekstem walki z ACTA dokonywały ataków na strony rządowe (próby cyberterroryzmu, mającego na celu wymusić zmianę decyzji rządu). Ataki te to zazwyczaj bardzo łatwe do wykonania napady DDoS (aby je wykonać wystarczy ściągnąć program z sieci botnet). Miały na celu wyłączenie dostępności takich stron jak: sejm.gov.pl, zaiks.org.pl, premier.gov.pl, cert.gov.pl.

Przeciw czemu protestowało społeczeństwo? Wszyscy protestowali przeciw podpisaniu przez Polskę Umowy Anti-Counterfeiting Trade Agreement czyli lepiej znana, jako ACTA. Jednak czy wszyscy protestujący wiedzieli, czym jest ACTA i o co w niej chodzi? Niestety nie! Tylko nieliczni zadali sobie trud przeczytania całej treści umowy, większość natomiast oparła się na wszechobecnych w sieci sloganach o ograniczeniu wolności słowa czy też zakazie pobierania plików z Internetu. Ustawa o Ochronie Praw Autorskich w Polsce już dawno zabraniała takich praktyk traktując je, jako kradzież treści objętych prawami autorskimi. Kolejnym mitem, który mieliśmy wielokrotnie okazję słyszeć było to, że w myśl umowy providerzy internetowi będą mieli obowiązek sprawdzać, co robimy, a raczej, co ściągamy i wysyłamy oraz kontrolować nasze prywatne wiadomości. Celem miało być szukanie przesłanek mogących świadczyć o tym, że łamiemy prawa autorskie. W umowie czytamy, że nikt nie ma prawa odebrać nam naszych praw do wolności słowa, sprawiedliwego procesu oraz prywatności, a za fałszywe oskarżenia należy nam się odszkodowanie. Co więc tak kontrowersyjnego jest w ACTA, że aż tyle osób domagało się, aby Polska nie podpisywała jej?

Telewizje rozpowszechniały informację jakoby w umowie ACTA w artykułach 8 i 11 były zapisy łamiące nasze prawa, choćby do domniemania niewinności. Faktycznie Artykuł 12 ustęp 2 wydaje się być kontrowersyjny, bo mówi:

„Każda strona przyznaje swoim organom sądowym prawo do zastosowania środków tymczasowych bez wysłuchania drugiej Strony, w stosownych przypadkach, w szczególności, gdy jakakolwiek zwłoka może spowodować dla posiadacza praw szkodę nie do naprawienia lub gdy istnieje możliwe do wykazania niebezpieczeństwo, że dowody zostaną zniszczone. W przypadku postępowania prowadzonego bez wysłuchania drugiej strony, każda Strona przyznaje swoim organom sądowym prawo do podejmowania natychmiastowego działania w odpowiedzi na wniosek o zastosowanie środków tymczasowych i do podejmowania decyzji bez zbędnej zwłoki."

To nie jest tak, że każdy może nas oskarżyć i zażądać zastosowania środków tymczasowych (są one zarezerwowane tylko dla wyjątkowych sytuacji). W myśl umowy może to zrobić właściciel praw, aby zażądać zastosowania środków tymczasowych muszą istnieć ku temu naprawdę mocne i udokumentowane powody, o czym mówi ustęp 4 omawianego artykułu:

„Każda Strona przyznaje prawo swoim organom do wymagania od wnioskodawcy żądającego zastosowania środków tymczasowych, aby dostarczył wszelkie możliwe do pozyskania dowody, aby organy te mogły przekonać się w wystarczającym stopniu, że prawo wnioskodawcy zostało naruszone lub, że istnieje groźba takiego naruszenia, a także prawo do nakazania wniesienia kaucji lub przedstawienia innego równoważnego zabezpieczenia wystarczającego dla ochrony osoby, przeciwko której skierowany jest wniosek, i zapobieżenia nadużyciu. Taka kaucja lub równoważne zabezpieczenie nie mogą nadmiernie zniechęcać do korzystania z procedur dotyczących takich środków tymczasowych."

Co jeśli pomimo tych zabezpieczeń zostaniemy posądzeni o coś, czego nie zrobiliśmy? Tak jak w wielu innych sprawach tak i w myśl tej umowy mamy prawo do żądania odszkodowania. Gwarantuje nam to kolejny (5) ustęp tegoż artykułu, który brzmi następująco:

„W przypadku uchylenia lub wygaśnięcia środków tymczasowych na skutek działania lub zaniechania wnioskodawcy, lub w przypadku późniejszego ustalenia, że naruszenie prawa własności intelektualnej nie miało miejsca, organy sądowe mają prawo nakazać wnioskodawcy, na wniosek osoby, przeciwko której skierowany był wniosek, aby zapłacił tej osobie odpowiednią rekompensatę z tytułu wszelkich szkód spowodowanych przez te środki."

Dodatkowo wszystkie procedury i uznanie za zasadne lub nie wniosku rozpatrywane jest na podstawie prawa lokalnego, czyli naszego polskiego. Kolejną rzeczą, o której nie usłyszeliśmy w telewizji ani nie przeczytaliśmy w Internecie jest artykuł 3 ustęp 2, który mówi, że nasze władze nie muszą podjąć się rozpatrzenia wniosku, jeśli na terenie naszego kraju dane prawo własności nie obowiązuje. Artykuł 3 ustęp 2

„Niniejsza Umowa nie tworzy obowiązku stosowania przez Stronę środków w przypadku, gdy dane prawo własności intelektualnej nie jest chronione na podstawie przepisów ustawowych i wykonawczych danej Strony."

Ciekawym i bardzo istotnym jest również artykuł 27 ustęp 2, który mówi, że podczas tych działań nikt nie może ograniczyć nam takich praw jak: prawo do wolności słowa, sprawiedliwego procesu oraz prywatności:

„Poza postanowieniami ust. 1, procedury dochodzenia i egzekwowania każdej Strony mają zastosowanie do naruszenia prawa autorskiego lub praw pokrewnych za pomocą sieci cyfrowych, które może obejmować bezprawne wykorzystywanie środków powszechnego rozpowszechniania w celu dokonania naruszenia. Procedury są stosowane w sposób, który pozwala uniknąć tworzenia barier dla zgodnej z prawem działalności, w tym handlu elektronicznego, oraz, zgodnie z prawem Strony, przy zachowaniu podstawowych zasad, takich jak wolność słowa, prawo do sprawiedliwego procesu i prywatności."[1]

Nawet artykuł 27 ustęp 4 nie wprowadza nic nowego do naszego „cybernetycznego życia". Ustęp ten mówi o możliwości wydania przez providera internetowego na podstawie nakazu sądowego danych osobowych posiadacza adresu IP, z którego nastąpiło naruszenie praw intelektualnych, właścicielowi tych praw. Jednak jak wiedzą pracownicy Polskich providerów internetowych takie sytuacje zdarzają się nader często i wcale nie rzadziej miały miejsce nim o ACTA ktokolwiek usłyszał.

„Strona może, zgodnie ze swoimi przepisami ustawodawczymi i wykonawczymi, przewidzieć możliwość wydania przez swoje właściwe organy dostawcy usług internetowych nakazu niezwłocznego ujawnienia posiadaczowi praw informacji wystarczających do zidentyfikowania abonenta, co, do którego istnieje podejrzenie, że jego konto zostało użyte do naruszenia, jeśli ten posiadacz praw zgłosił w sposób wystarczający pod względem prawnym żądanie dotyczące naruszenia praw związanych ze znakami towarowymi, praw autorskich lub pokrewnych i informacje te mają służyć do celów ochrony lub dochodzenia i egzekwowania tych praw. Procedury są stosowane w sposób, który pozwala uniknąć tworzenia barier dla zgodnej z prawem działalności, w tym handlu elektronicznego, oraz, zgodnie z prawem Strony, przy zachowaniu podstawowych zasad, takich jak wolność słowa, prawo do sprawiedliwego procesu i prywatności."

Po co więc podpisywać Umowę ACTA?

Jednym z najważniejszych powodów, jaki możemy przeczytać w Uzasadnieniu jest „zacieśnienie międzynarodowej współpracy zmierzającej do skuteczniejszego egzekwowania praw własności intelektualnej na poziomie międzynarodowym, a także uzupełnienie dotychczasowych regulacji międzynarodowych w tym zakresie”.[2]

Wyżej wymienione uzasadnienie jest logiczne i moim zdaniem wystarczające, aby ja podpisać. Musimy przecież pamiętać, że będąc krajem członkowskim Unii Europejskiej oprócz przywilejów mamy również obowiązki, a są nimi między innymi ujednolicenie przepisów, które obowiązują wszystkie państwa członkowskie UE.

Zważając na to wszystko należy się zastanowić czy aby przypadkiem nie byliśmy narzędziem w czyichś rękach. Musze przyznać, że sama dałam się początkowo zmanipulować informacją w telewizji i Internecie na temat ACTA. A artykuł ten zamiast wydźwięku bądź, co bądź pozytywnego miał mieć negatywny. Jak pokazuje praktyka musimy wczytać się dokładnie w to, o czym mamy pisać czy przegłosowywać, a nie jak niektórzy europosłowie opowiadać się za lub przeciw czemuś nie, mając bladego pojęcia, za czym czy przeciw czemu się opowiadają.

Jak widać nawet w teoretycznie rzetelnych i wiarygodnych źródłach możemy spotkać się z błędami lub manipulacjami. Jednym z niewielu pozytywów, jakie wynikły z całej tej sytuacji jest fakt, że potrafimy nadal się zjednoczyć w walce o jakiś cel. Niestety ten pozytyw przyćmiewa wada, jaką ujawniliśmy, czyli to, że bardzo łatwo nas zmanipulować.

Aby zbyt często nie powtarzało się takie manipulowanie nami czytajmy sami, zamiast wierzyć na słowo zwłaszcza, gdy jest ono poparte tylko wyrwanymi z kontekstu fragmentami, a nie całymi ustępami lub nawet artykułami. Pamiętajmy, aby krytycznie podchodzić do wiadomości, które w swych źródłach czy pseudo cytatach odsyłają nas do treści, o których nie wspominają żadne wymienione przez nich źródła.

Bernadetta Terlecka

[1] Na przykład, bez uszczerbku dla przepisów prawa Strony, przyjęcie lub utrzymanie systemu przewidującego ograniczenie odpowiedzialności dostawcy usług internetowych lub środków zaradczych przeciwko nim, przy jednoczesnym zachowaniu uzasadnionych interesów posiadacza praw.

[2] Umowa ACTA str. 9 punkt 1. (adres online: http://img.interia.pl/wiadomosci/nimg/0/4/Zobacz_tresc_ACTA_rzadu_5615354.pdf)

Warto przeczytać:

Analiza ACTA wg instytutu INPRIS
– http://www.inpris.pl/infografika-prawo/acta-news-szymel/t/acta/

Analiza ACTA wg portalu webhosting.pl
– http://webhosting.pl/ACTA.nie.taki.diabel.straszny

Treść umowy ACTA
– http://img.interia.pl/wiadomosci/nimg/0/4/Zobacz_tresc_ACTA_rzadu_5615354.pdf

Мятежевойна Jewgienija Messnera

Definicja wojny asymetrycznej przed wydarzeniami z 2001 r. r. znana była nielicznemu gronu specjalistów. Pojęcie asymetria pojawiło się współcześnie w 1995 r. w publikacji pt. „Połączona walka sił zbrojnych USA". Asymetria była definiowana jako starcie pomiędzy sobą różnego rodzaju sił zbrojnych np. sił powietrznych z siłami morskimi.

Np. dla niemieckich specjalistów wojna asymetryczna jest tzw. małą wojną lub konfliktem o obniżonej intensywności, w którym państwa lub społeczeństwa wystawione są na zagrożenia ze strony aktorów państwowych lub niepaństwowych: grup terrorystycznych, bojowników o wolność, hakerów komputerowych, stosujących najczęściej niekonwencjonalne środki ataku.

Silniejsza strona poddana jest niekonwencjonalnym atakom słabszego przeciwnika. W wojnie asymetrycznej ni ma rozróżnienia pomiędzy kombatantami i ludnością cywilną. Podczas wojny asymetrycznej znajdują zastosowanie wszystkie możliwe środki walki, a swoją brutalnością wobec ludności cywilnej przypomina wojnę totalną. Istotnym przejawem wojny asymetrycznej jest liczebny wzrost niepaństwowych aktorów w polityce międzynarodowej. Zaliczamy do nich oprócz ruchów wyzwoleńczych, ruchów oporu, zorganizowaną przestępczość, prywatne siły zbrojne, prywatne organizacje wywiadu i bezpieczeństwa, globalne koncerny, organizacje pozarządowe. Nastąpiło sprywatyzowanie (odpaństwowienie) wojny.

Wojna przeniosła się ze sfery, gdzie rozważa się rachunek strat i zysków, do sfery trudno dostrzegalnych powodów ideologiczno – emocjonalnych. Stała się sposobem na życie, celem samym w sobie. Wojna asymetryczna to zacieranie granicy pomiędzy wojną a pokojem, bezpieczeństwem wewnętrznym i zewnętrznym, sferą prywatną i społeczną.

Badaczem zajmującym się nowymi obliczami wojny, który stworzył koncepcję ogólnoświatowej *мятежевойны* był pułkownik Sztabu Generalnego carskiej armii, Jewgienij Messner. Już ponad pięćdziesiąt lat temu uprzedzał przed nastaniem ery nieklasycznych wojen, ogólnoświatowego buntu, rebelii (*мятеж*) i nie znającego granic terroru.

Pułkownik J. Messner urodził się w 1891 r, zmarł w 1974 r. w Buenos Aires w Argentynie. Był człowiekiem niezwykłej erudycji, wspaniałego intelektu. Władał językami: angielskim, niemieckim, francuskim, hiszpańskim i serbskim. Unikalność pułkownika J.E. Messnera jako praktyka i teoretyka wojen związana jest z faktem, że jego twórczość obejmuje ponad pół wieku. Wieku pełnego wojen, wybuchów społecznych, przeładowanego techniczno – wojennymi rewolucjami. Messner napisał dziesiątki prac naukowych, kilka tysięcy artykułów i wzmianek opublikowanych w emigracyjnych wydawnictwach rosyjskich i pismach zagranicznych.

W swoich pracach naukowych i publicystycznych Jewgienij Messner sformułował i nagłośnił ideę nowej formy walki zbrojnej - *борьбы мятежом*. W swojej pracy z 1972 r. pt. *Terror* przewidująco ocenił zagrożenia jakie niesie terroryzm. Stwierdził, że terroryzm zmienił swój zasięg, charakter i istotę. Akty terrorystyczne stały się najważniejszymi operacjami *Всемирной Мятежевойны*. Pokazał cechy współczesnego terroryzmu, takie jak: brak granic, wielką ilość aktów terrorystycznych, doskonałą organizację, swojego rodzaju inteligencję (wynikającą ze składu uczestników), nie zwyczajną rewolucyjność, lecz różnorodność celów terroryzmu, możliwość wyzwolenia współczucia sprawiedliwości społecznej i jego umiędzynarodowienie. W opinii Messnera należy z tym zagrożeniem prowadzić walkę i bronić się wojskowymi sposobami. Messner podkreślał, że terroryzm jest jednym z elementów nieklasycznej, zalewającej cały świat wojny, która nosi nazwę *Мятеж*. W jego opinii wojny splotły się z buntami, rebeliami, rebelie z wojnami i tak powstała nowa forma konfliktów zbrojnych, którą nazwał *Мятежевойна*.

Fenomen ten należy rozpatrywać z różnych punktów widzenia. Walka w stylu *Мятежевойны* (partyzanci, dywersanci, terroryści) przyjmie ogromne rozmiary. Będąc bystrym obserwatorem otaczającej go rzeczywistości Messner doszedł do wniosku, że walki nieregularne mieszają się i splatają z uderzeniami z podziemia (terroryzm) tajnych lub terrorystycznych

organizacji, grup sabotażowych, rozmaitych indywidualnych jednostek (ludzi). Wszystkie te zdarzenia trudno klasyfikować, wskazywać ich źródła. Niezależnie czy jest to zemsta na okupancie czy wyzwolenie kraju lub przewrót polityczny. Mieszaninę, splątanie ideologii, bezideowego zła, pryncypialnego protestu, awantury bez zasad nazwał - *мятежом*.

Według Messnera *мятежевойна* nie kieruje się określonymi normami czy szablonami postępowania. Taktyka wojny – rebelii jest elastyczna, unikaj tego co silne, bij w słabe punkty. Oczekują cię u bram, wejdź oknem. Partyzanci powinni zmieniać miejsce swoich działań jak woda lub wiatr.

Fazy *мятежевойны* to: demoralizacja, nieporządek, terror, postępujący werbunek do sprawy rewolucji, przebudowa dusz (stworzenie nowego człowieka), konstruowanie systemu człowieka maszyny. Celem strategicznym tej wojny jest burzenie, dewastowanie struktury państwa. Zburzone państwo nie może być odbudowane, tak jak martwy nie może być przywrócony życiu powtarzał za Sun Tzu.

Zasadniczymi czynnikami, które przyczyniły się do powstania *мятежевойны* wg Messnera byli fabianie, pacyfiści, Nowa Lewica w USA, masoneria, radykalny humanizm, tzw. pożyteczni idioci, Organizacja Narodów Zjednoczonych oraz komunizm. Pozostałymi elementami wpływającymi na rozwój *мятежевойны* to *watykański III świat*, demokratyzacja, destabilizacja, dechrystianizacja, ruch państw niezaangażowanych, będący ogromną rezerwą *czerwonej* strony *мятежевойны*. Pozostałe czynniki tej ogólnoświatowej wojny to m in. bunt młodzieży z 1968 r., ruch Czarnych Panter w USA, kolonializm, antykolonializm i syjonizm.

Prowadzenie wojny jest sztuką. Obecnie powstaje nowa sztuka – prowadzenie *мятежевойны* stwierdził J. Messner.

Podstawowymi celami tego typu wojny jest zniszczenie morale wrogiego narodu, rozbicie jego aktywnej części takiej jak wojsko, partyzantka, walczących ruchów narodowych, zniszczenie lub przechwycenie obiektów mających wartość psychologiczną, zniszczenie lub zajęcie obiektów mających wartość materialną, stworzenie wrażenia zewnętrznego porządku dzięki zdobyciu nowych sojuszników dla spowodowania upadku ducha sojuszników wroga.

Strategia *мятежевойны* polega na wzięciu do psychologicznej niewoli wrogiego narodu. Celem jest strącenie go z jego ideowych pozycji, wniesienie trwogi i zamieszania. Utwierdzenie w zwycięstwie naszych idei i przyciągniecie go do nich. *Мятежевойна* to odstępstwo od dogmatów klasycznej sztuki wojennej. To herezja. *Мятежевойна* to wojna heretycka, trwająca dopóki wojna nie oddzieli się od *мятежа*.

Aby pojąć czym jest *мятежевойна* należy odstąpić od utrwalonej przez wieki tradycji pojęcia wojny. Zakończyć myślenie, że wojna jest wtedy kiedy walczą, a pokój kiedy nie walczą.

Jądrem systemu przeciwko *мятежевойне* i główną siłą uderzeniową musi stać się niewielka, lecz jakościowo silna, doborowa, profesjonalna armia.

Aby móc zwyciężyć w *мятежевойне,* kierować nią w interesie cywilizowanych państw, należy posługiwać się określonymi dla tej wojny prawidłami, które nie zostały systemowo opracowane. To nie zgłębiona forma wojny i jej prawa są nieznane. Poprzez badanie partyzanckich i przeciw partyzanckich wojen, doświadczeniu w walce z wojenno – politycznym bandytyzmem i terroryzmem można stworzyć dostatecznie jasną i precyzyjną naukę, jak pokonać *мятежевойну* na poziomach: politycznym, strategicznym i taktycznym.

Pułkownik Jewgienij Messner nie mógł przewidzieć takich form *мятежевойны* jak np. cyberterroryzm, lecz w mojej ocenie stał się prekursorem w badaniu zjawiska asymetryczności oraz nieklasycznych, nowatorskich form prowadzenia działań wojennych.

Kazimierz Kraj

Bibliografia

Хочешь мира, победи мятежевойну!, Творческое наследие Е.Э. Месснера, Москва 2005

Е.Э. Месснер, Всемирная мятежевойна, Москва 2004

„Z Afganistanu.pl”

„Książka długo oczekiwana. Pozwoli zobaczyć inny obraz – inny niż to, co pokazują media w kraju – trudu, wysiłku i poświęcenia polskich żołnierzy. Tylko oni wiedzą, ile ich to naprawdę kosztowało. Maja swój udział w historii Polski, co autor plastycznie pokazał w książce.”

Waldemar Skrzypczak, generał broni rezerwy (opinia z okładki książki „Z Afganistanu.pl”)

Kilka dni temu trafiłam do empiku w poszukiwaniu książki, która stałaby się lekiem na długą i nudną podróż naszą koleją. W ten sposób trafiła w moje ręce książka Marcina Ogdowskiego pt. „Z Afganistanu.pl”. Jako, że miałam wcześniej przyjemność czytywać blog autora zafganistanu.pl postanowiłam przyjrzeć się jej dokładnie. Od razu rzuciła mi się w oczy opinia generała broni rezerwy Waldemara Skrzypczaka, która utwierdziła mnie w przekonaniu, że bez tej pozycji moja biblioteczka będzie niekompletna.

Książkę tą powinien przeczytać każdy, kto choć troszkę interesuje się losem naszych żołnierzy w Afganistanie jak również zagorzali przeciwnicy takich misji. Ten przedziwny alfabet ukazuje nam cywilom i żołnierzom prawdziwy obraz wojny, choć nie jest ona taka, jaką znamy z książek historycznych traktujących o II wojnie światowej.

W książce znajdziemy obraz wojny widziany oczyma korespondenta wojennego. Podczas podróży po kolejnych literach alfabetu poznajemy opinie misjonarzy i ich rodzin. Dowiadujemy się również o problemach zawodowych i osobistych trapiących misjonarzy, tak w czasie misji, jak i po powrocie z niej. Autor w książce podkreśla wagę problemu, który dla naszego wojska jest tematem tabu, czyli PTSD (zespół stresu pourazowego).

Książka jest bogato ilustrowana kolorowymi zdjęciami wykonanymi podczas pobytów Autora w Afganistanie, a i jakość papieru (kredowy) wręcz zaskakuje w publikacji.

Bernadetta Terlecka

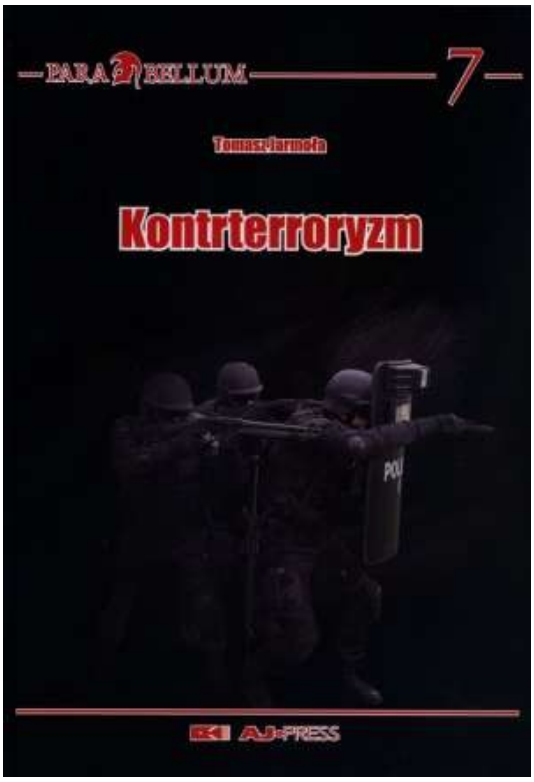
M. Ogdowski, Z Afganistanu.pl, Alfabet polskiej misji. Wydawca: War Report, 2011 r.

(…) To miało być i jest opracowanie dla kogoś, kto nie siedzi dobrze w temacie i o sprawach związanych z AT wie z telewizji lub gazet codziennych, a chciałby dowiedzieć się czegoś więcej - jak choćby prawnicy, na codzień stykający się nieco w pracy z tematem a nie mający o tym zielonego pojęcia. Sam jestem policjantem i prawnikiem z wykształcenia i wiem jak niewielka w tych środowiskach (nie licząc AT i ich przełożonych) jest wiedza o tematyce zawartej w książce. Nie uważam się za autorytet w tej dziedzinie,ale od wielu lat interesuję się tą tematyką, sporo praktyki (szkolenia w policji, wojsku czy warsztaty Specops i zawody Paramedyk) oraz kontakty z wieloma funkcjonariuszami służb uzbrojonych sprawiły, że postanowiłem napisać coś, co dotrze do szerszego grona i rozwieje pewne dziwne stwierdzenia zwłaszcza prasowe o działaniach AT (…)

Zawarta na jednym z forów dyskusyjnych (http://specops.com.pl/forum/topics95/kontrterroryzm-tomasz-jarmola-vt7213.htm) wypowiedź Autora doskonale oddaje charakter tej pracy. Jest to kompilacja wiedzy o istocie kontrterroryzmu, o jednostkach AT (KT), ich wyposażeniu, uzbrojeniu, wyszkoleniu i taktyce. Opracowanie przydatne dla laików, pozwalające częściowo usystematyzować ogrom definicji, pojęć i wiedzy z tego tematu. Choć w książce jest trochę błędów (errata dostępna na stronie wydawnictwa) – to jednak wynikają one w większości bądź to z pomyłek edytorskich, bądź z nieaktualnych źródeł. Jednak te ostatnie po części są usprawiedliwione – dynamika zmian w organizacji i strukturach jednostek AT (KT) powoduje dezaktualizację danych.

Reasumując – książka warta uwagi, swoiste wprowadzenie w ten szeroki i trudny temat, jakim jest kontrterroryzm. Z zastrzeżeniem – zarówno zawartym w słowie od Autora jak i przedmowie dr hab. K. Kubiaka – jest to synteza, kompilacja, wprowadzenie. Jeśli tego oczekujemy od tej pozycji – to dokładnie to otrzymaliśmy. Czytając książkę miejmy w pamięci jej rok wydania -2009 - nieco dezaktualizujący zawarte w niej wiadomości. Lecz jako wprowadzenie do problematyki jest to pozycja wielce przydatna.

Piotr Podlasek



T. Jarmoła, Kontrterroryzm
Wydawnictwo: Aj Press, 2011 r.
ss. 232

„Dziesięć kawałków o wojnie. Rosjanin w Czeczenii”

„Dziesięć kawałków...” to wspomnienia żołnierza rosyjskiego z wojen w Czeczenii. Arkadrij jako żołnierz poborowy w wieku 18 lat trafia do wojska. Trwa pierwsza wojna czeczeńska. Chłopak najpierw przerażony perspektywą udziału w działaniach zbrojnych po krótkim czasie zaczyna wręcz marzyć o przerzuceniu na front i walce z „Czeczakami”. Wszystko bowiem jest lepsze od tego, czego doświadcza w swym oddziale.

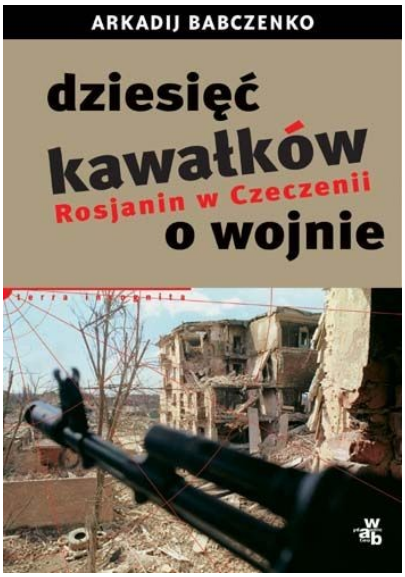
Książka Babczenki to prawdziwy szok dla osób, które nigdy nie interesowały się tematyką związaną z wojnami rosyjsko-czeczeńskimi, które nigdy nie słyszały o diedowszczyźnie, które nie wiedzą, co działo się w tej małej górskiej republice. „Dziesięć kawałków...” to książka, która wstrząsa każdym swym rozdziałem, która pozostawia czytelnika w szoku i niesmaku, w zadumie i odrętwieniu. Każdy jej wers na długo pozostaje w pamięci czytelnika.

Książka to opowieść przede wszystkim o wojsku rosyjskim, o okrucieństwie żołnierzy wobec poborowych, o braku moralności, humanitaryzmu, prawa, o samowolce. Można by rzec, że tam gdzie kończą się reguły, tam zaczyna się rosyjskie wojsko. Babczenko pisze o bestialstwie starszych stażem żołnierzy, którzy alkoholem, narkotykami i biciem poborowych urozmaicali sobie czas i odreagowywali stres. Jak pisze: „Bili mnie wszyscy, zaczynając od szeregowca i kończąc na zastępcy dowódcy pułku (...). Nie bił mnie jeszcze tylko generał. Zapewne dlatego, że w naszym pułku nie ma generałów. (...) Nie możemy odetchnąć pełną piersią – pięści rezerwistów tak urządziły nasze klatki piersiowe, że stały się jednym wielkim siniakiem i oddychamy po trochu, z trudem płytko wciągając powietrze. (...) W armii tylko przez pierwsze pół roku jest ciężko, a potem już po prostu nie boli”.

Pomimo takich doświadczeń, Babczenko zgłasza się jako ochotnik do wyjazdu na drugą wojnę czeczeńską. Pisze, że wojna to najsilniejszy narkotyk. Podaje, że wrócił na nią „może dlatego, że tam została moja przeszłość, całe moje życie – z tamtej wojny wróciło tylko ciało, ale nie dusza”. I dodaje: „kocham cię wojno (...) za to, że masz w sobie moją młodość (...) za to, czego mnie nauczyłaś: że najpaskudniejsze życie jest tysiąc razy lepsze od śmierci. (...) jesteś moją pierwszą kobietą, moją pierwszą miłością. (...) nikogo nie pokochałem tak jak ciebie. (...) dla mnie na zawsze będzie wojna”.

Pozycja dla czytelników o mocnych nerwach.

Ewa Wolska



A.Babczenko, „Dziesięć kawałków o wojnie. Rosjanin w Czeczenii". Warszawa 2009 r., ss. 322

Język farsi (perski)

Od bieżącego numeru na łamach naszego biuletynu będą się ukazywać krótkie lekcje języka farsi (perskiego). Język ten jest używany przez wiele milionów ludzi zamieszkujących Iran, Afganistan i Irak.

Nie będą to zwykłe lekcje, jakich wiele jest w Internecie. Celem lekcji będzie pokazanie czytelnikom najważniejszych zwrotów w tym języku. Zwroty będą dotyczyły różnych dziedzin życia, od podstawowych jak: powitania, podziękowania i pożegnania, po zwroty bezpośrednio związane z tematyką biuletynu. W kolejnych częściach w miarę możliwości przedstawione będą zwroty przydatne w sytuacjach które mogą przytrafić się np. służbom porządkowym i bezpieczeństwa podczas kontaktu z obcokrajowcem w Polsce, z którym możliwa jest komunikacja tylko w tym języku.

Zaznajomienie czytelnika ze zwrotami to nie jedyny cel kursu. Innym równie ważnym jest przedstawienie kultury ludzi żyjących w tych krajach.

Istotną rzeczą podczas nauki języka farsi jest zwracanie uwagi na sposób zapisu liter, które w zależności od swego położenia w wyrazie (początek, koniec lub wewnątrz wyrazu) są pisane w różny sposób. Pisownię szerzej omówię w jednym z kolejnych numerów biuletynu.

Jeśli chodzi o wymowę będę używać transkrypcji angielskiej (nie jest mi znana dokładna transkrypcja polska).

Kultura

W krajach Islamskich musimy pamiętać, że nie witamy się poprzez podanie ręki, a polski gest pocałowania kobiety w rękę jest zabroniony. Witamy się (przekazujemy znak pokoju) poprzez położenie ręki prawej na sercu i skinienie głowy. Należy również pamiętać, że nic nie dajemy, bierzemy lewą ręką, a już w ogóle nie używamy jej do jedzenia.

Wyrażenia:

Witaj *(a jak w wyrazie „far" czyli dłuższe a)/*	Salām / salam
Do widzenia (*kh czytamy jak w szkockim „loch", a jak w powyższym przykładzie/)*	khodā hāfez
Tak/ Nie	bale / na
Przepraszam (*kh czytamy jak w szkockim „loch"/)*	bebakhshid
Bardzo mi przykro (przepraszam) (*kh czytamy jak w szkockim „loch")*	ma'zerat mikham
Proszę	lotfan
Spokój! / Cisza!	doroste!
Rozumiesz? / Zrozumiałeś mnie?	motavajjeh mishin?
Zrozumiałem / Zrozumiałam	bale mifahmam
Nie zrozumiałem / Nie zrozumiałam	na namifahmam
Jak się nazywasz?	esmetun chi ye?
Nazywam się…	esmam… e
Skąd pochodzisz	[shomā] kojami hastin?
Mieszkam w Europie	man ahl e urupā am
Mówisz po angielsku?	[shomā] ingilisi baladin?
Tak, mówię	bale, baladam
Nie, Nie mówię	na, balad nistam
Tak, ale słabo	[man] ye kami balad am
Nie mam nic do oclenia	[man] chiz e khāssi nadāram ke ettelā' bedam
Czy mogę zadzwonić do ambasady / konsulatu	mishe be sefārat/ konsulgari am telefon konam

Bernadetta Terlecka

Kalendarium

15.01.12. W Syrii dokonano zamachu terrorystycznego na pociąg transportujący paliwo, wykolejenie nastąpiło z powodu podłożenia i zdetonowania na torach ładunku wybuchowego. W tym samym dniu uzbrojona grupa terrorystyczna dokonała zamachu na transformator elektryczny co skutkowało zerwaniem kolejowej trakcji elektrycznej między stacjami na północy Syrii.

16.01.12. W Jemenie bojownicy Al-Kaidy przejęli całkowitą kontrolę nad miastem Rada leżącym około 150 km od stolicy kraju. W walce zginęło dwóch funkcjonariuszy sił rządowych.

19.01.12. Zamach terrorysty-samobójcy na lotnisku w Kandaharze, zginęło co najmniej sześć osób. Terrorysta dokonał zamachu przy wejściu na lotnisko. Celem był prawdopodobnie opancerzony samochód sił zagranicznych. Do zamachu przyznali się talibowie.

24.01.12. Dwa samochody – pułapki eksplodowały w Bagdadzie, zginęło co najmniej dziesięć osób. Detonacja materiałów wybuchowych nastąpiła w dzielnicy zamieszkanej głównie przez szyitów.

24.01.12. Francuska policja zlikwidowała islamistyczną organizację o nazwie Forsane Alizza, która za pomocą Internetu rekrutowała swoich bojowników.

27.01.12. Około 30 osób zginęło, a 60 zostało rannych podczas uroczystości pogrzebowych w Bagdadzie wskutek wybuchu samochodu- pułapki.

30.01.12. Zbrojne ugrupowanie terrorystyczne wysadziło w powietrze syryjski gazociąg łączący centrum kraju z wybrzeżem. Był to już kolejny taki incydent w czasie powstania przeciwko syryjskiemu prezydentowi Baszarowi Al – Assadowi.

31.01.12. W trakcie walki na terytoriach plemiennych w północno-zachodniej części Pakistanu, zginęło siedmiu pakistańskich żołnierzy i 25 talibskich bojowników.

5.02.12. Zamach bombowy na gazociąg łączący Egipt, Izrael i Jordanię na północnym wybrzeżu półwyspu Synaj wstrzymał przesyłanie gazu. Sprawcy nie są znani, lecz podejrzewa się o to zamieszkujących ten region –Beduinów.

8.02.12. W Iraku stracono kolejne 14 osobach, które skazano na śmierć za terroryzm i działalność przestępczą. W ubiegłym roku dokonano 68 takich egzekucji, w bieżącym już 65.

09.02.12. Atak amerykańskiego samolotu bezzałogowego na północnym zachodzie Pakistanu, spowodował śmierć 3 islamskich bojowników, oraz niebezpiecznego terrorysty – szefa operacji Al-Kaidy w Pakistanie B. Mansoora.

14.02.12. Wybuch bomby w mieście Kaduna na północy Nigerii spowodował śmierć nigeryjskiego policjanta.

16.02.12. Nigeryjczyk U.F. Abdulmutallab (25l.) został skazany na dożywotnie więzienie w Detroit, za próbę wysadzenia w powietrze samolotu lecącego do Detroit w dniu 25 grudnia 2009 roku.

17.02.12. W zamachu samobójczym przed meczetem w Pakistanie zginęło ponad 30 osób. Zamachowiec-samobójca zdetonował ładunek wybuchowy poruszając się na motocyklu po ruchliwym targowisku w Parachinar.

19.02.12. W stolicy Iraku - Bagdadzie zginęło ponad 20 osób po zamachu samobójczym przed akademią policyjną. Zamachowiec-samobójca zdetonował ładunek wybuchowy umieszczony w swoim samochodzie.

Tomasz Tylak
(na podstawie serwisów informacyjnych)

Adresy stron internetowych:
- Biuletyn: www.e-terroryzm.pl
- Centrum Studiów nad Terroryzmem: www.terroryzm.rzeszow.pl
- Wyższa Szkoła Informatyki i Zarządzania w Rzeszowie: www.wsiz.rzeszow.pl

Wyższa Szkoła Informatyki i Zarządzania
w Rzeszowie, ul. Sucharskiego 2, 32-225 Rzeszów

Kontaktowe adresy e-mail:
– Redakcja Biuletynu: redakcja@e-terroryzm.pl

Zespół redakcyjny tworzą pracownicy Katedry Bezpieczeństwa Wewnętrznego i Centrum Studiów nad Terroryzmem Wyższej Szkoły Informatyki i Zarządzania w Rzeszowie oraz skupieni wokół tych jednostek znawcy i entuzjaści problematyki.