Czerwiec 2012 r. nr 6

e–Terroryzm.pl

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

WYZWANIA TERRORYZM ZAGROŻENIA BEZPIECZEŃSTWO DYLEMATY OCHRONA
DONIESIENIA SPRAWOZDANIA ANALIZY

W numerze:

e-Terroryzm.pl nr 6/2012 (6)

Internetowy Biuletyn
Centrum Studiów nad Terroryzmem

Publikacja jest bezpłatna, a zespół redakcyjny oraz Autorzy nie odnoszą z niej korzyści materialnych. Publikowane teksty stanowią własność Autorów, a prezentowane poglądy nie są oficjalnymi stanowiskami Centrum Studiów nad Terroryzmem oraz Wyższej Szkoły Informatyki i Zarządzania.

Artykuły poruszane w czasopiśmie służą celom edukacyjnym oraz badawczym. Redakcja nie ponosi odpowiedzialności za inne ich wykorzystanie.

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.

Adresy i kontakt:

- Poczta redakcji biuletynu: **redakcja@e-terroryzm.pl**
- Strona internetowa biuletynu: **www.e-terroryzm.pl**
- Centrum Studiów nad Terroryzmem: **www.terroryzm.rzeszow.pl**
- Wyższa Szkoła Informatyki i Zarządzania: **www.wsiz.rzeszow.pl**

Fotografia na okładce: U.S. Air Force photo, by Senior Airman Andria J. Allmond
Źródło: http://www.332aew.afcent.af.mil

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

Kalendarium

25.05.12. W przeprowadzonym zamachu samobójczym w północnej części Jemenu zginęło 12 osób. Zamachowiec poruszał się samochodem wyładowanym materiałami wybuchowymi. Wśród ofiar zamachu było 6 członków szyickiej grupy rebelianckiej.

31.05.12. Uprowadzony w styczniu w Nigerii obywatel Niemiec, został zabity przez swoich porywaczy. Porywacze, gdy dowiedzieli się o planowanym odbiciu go przez wojsko – zastrzelili Niemca. Grupa, która dokonała porwania i zabójstwa jest powiązana z Al-Kaidą.

04.06.12. W wyniku przeprowadzonego zamachu przy użyciu samochodu-pułapki na siedzibę organizacji religijnej w Bagdadzie zginęło co najmniej 22 osoby, a około 60 zostało rannych.

05.06.12. Czołowy strateg Al-Kaidy – Abu Jahja al-Libi, zginął w wyniku ataku amerykańskiego samolotu bezzałogowego w Pakistanie. Określany jako numer dwa Al-Kaidy odgrywał znaczną rolę w operacjach przeciwko USA i jego sojuszników. Podczas ataku zginęło 6 innych członków organizacji.

08.06.12. W wyniku wybuchu bomby w Peszawarze, w północno-zachodniej części Pakistanu, zginęło co najmniej 16 osób, a 30 zostało rannych. Ofiarami wybuchu byli głównie pasażerowie autobusu, pracownicy lokalnej administracji.

12.06.12. W środkowej części Afganistanu, w prowincji Wardak, doszło do wybuchu bomby podłożonej przez talibów. Śmierć poniosło 5 osób, a 2 zostały ranne. Przydrożna bomba wybuchła w chwili przejazdu pasażerskiego mikrobusu. Ponadto w wyniku innego zamachu przeprowadzonego również w środkowej części Afganistanu zginęło 7 osób, wśród których ofiarami były małe dzieci.

13.06.12. W przeprowadzonych atakach amerykańskiego samolotu bezzałogowego w południowo-wschodniej części Jemenu zginęło 30 członków Al-Kaidy, a kilkudziesięciu zostało rannych.

13.06.12. W stolicy Iraku – Bagdadzie podczas odbywających się szyickich uroczystości religijnych, doszło do ataków terrorystycznych z wykorzystaniem ładunków wybuchowych i broni palnej. Wskutek tych zamachów śmierć poniosły co najmniej 44 osoby.

16.06.12. W Bagdadzie, stolicy Iraku w wyniku wybuchu 2 samochodów-pułapek zginęło około 30 osób. Atak terrorystyczny był wymierzony w szyickich pielgrzymów udających się do grobu imama Musy al-Kadima. Do zamachu doszło pomimo zastosowania nadzwyczajnych środków ostrożności przez policję i wojsko, które dokonywały kontroli pojazdów i pieszych udających się do meczetu.

16.06.12. W wyniku wybuchu samochodu-pułapki na bazarze w mieście Landi Kotal (północno-zachodni Pakistan), zginęło ponad 25 osób, a co najmniej 30 zostało rannych. Celem ataku był przywódca plemienny wspierający rząd w walce z talibami. Ponadto w pobliskim okręgu Kohat zginęło co najmniej 7 osób.

17.06.12. W północnej części Nigerii – miastach Kaduna i Zaria doszło do 3 zamachów samobójczych na kościoły katolickie. Zginęło w nich około 20 osób, a 80 zostało rannych.

18.06.12. W mieście Aden w Jemenie w wyniku zamachu samobójczego zginął jemeński generał, który dowodził wojskiem prowadzącym walkę na południu kraju z Al-Kaidą. Po ostatnich sukcesach armii Jemenu, Al-Kaida zemściła się dokonując na nim planowanego zamachu.

Tomasz Tylak

Szanowni Czytelnicy!

Redakcja biuletynu oddaje do Państwa rąk przedwakacyjny numer naszego miesięcznika. Nie myślcie, że damy Wam spokój w lipcu i sierpniu. Nie damy. Otrzymacie kolejne, może nawet obszerniejsze publikacje. Jak zwykle zamieściliśmy statystykę ataków terrorystycznych, tym razem za kwiecień i maj oraz kalendarium. Przeczytacie artykuły na temat komunikacji z mediami w sytuacji kryzysowej i cyberterroryzmie przeciwko informatycznej infrastrukturze krytycznej. Zainteresowani otrzymają dawkę wiedzy na temat interwencji policyjnej. Kontynuowany jest cykl artykułów związany z zagadnieniami udziału Rosji w zwalczaniu terroryzmu w sferze międzynarodowej. Otrzymacie również garść informacji o terrorystach – samobójcach oraz historii ładunków IED. Ostatnie strony zostały poświęcone zaletom studiowania na kierunku bezpieczeństwo wewnętrzne w Wyższej Szkole Informatyki i Zarządzania w Rzeszowie. Potencjalni studenci oraz inni zainteresowani np. studiami podyplomowymi mogą zapoznać się z charakterystyką nauczycieli akademickich – pracowników Katedry Bezpieczeństwa Wewnętrznego.

Wspominając zmarłego generała Sławomira Petelickiego, zamieszczamy jego niepublikowane nigdzie zdjęcie, uzyskane dzięki uprzejmości Pana Andrzeja Wojtasa, redaktora naczelnego MMS Komandos.

Za zespół
Kazimierz Kraj

Ataki terrorystyczne na świecie – kwiecień 2012 r.

Lp.	Nazwa państwa	Liczba ataków	Zabici	Ranni	Porwani
1	Irak	141	117	352	0
2	Pakistan	87	105	165	13
3	Afganistan	75	115	318	22
4	Indie	62	22	26	13
5	Jemen	31	92	43	3
6	Kolumbia	21	20	29	1
7	Syria	17	39	145	0
8	Filipiny	16	23	62	1
9	Tajlandia	16	11	14	0
10	Turcja	16	10	15	0
11	Nigeria	14	116	85	0
12	Rosja	12	8	11	0
13	Meksyk	10	28	0	0
14	Somalia	9	32	10	0
15	Bahrajn	6	0	19	0
16	Nepal	5	4	11	0
17	Zjednoczone Królestwo	4	0	0	0
18	Egipt	3	6	23	0
19	Birma	3	4	2	3
20	Algieria	3	2	3	0
21	Bangladesz	3	0	3	0
22	Peru	2	3	2	7
23	Liban	2	1	20	0
24	Ukraina	2	0	30	0
25	Kenia	1	1	16	0
26	Wenezuela	1	0	0	1
27	Chile	1	0	0	0
27	Iran	1	0	0	0
29	Salwador	1	0	0	0
30	**Ogółem**	**565**	**759**	**1404**	**64**

Źródło: Centre of Exellence Defense Against Terrorism (COE – DAT), Monthly Terrorism Report 01 -30 April 2012

Ataki terrorystyczne na świecie – kwiecień 2012 r.

Lp.	Rodzaj ataku	Liczba	Zabici	Ranni	Porwani
1	Improwizowany ładunek wybuchowy (IED)	212	178	530	0
2	Atak zbrojny	129	195	130	0
3	Konflikt	88	136	136	0
4	Improwizowane ładunki wybuchowe montowane na pojazdach lądowych (VBIED)	32	162	0	0
5	Ogień pośredni	29	30	115	0
6	Atak samobójczy	25	130	177	0
7	Porwania	14	0	0	38
8	Egzekucja	11	32	150	0
9	Podpalenie	12	0	2	0
10	Napad	9	26	2	26
11	Fałszywy alarm	1	0	0	0
12	Cyberatak	1	0	0	0
13	**Ogółem**	565	759	1404	64

Źródło: Centre of Exellence Defense Against Terrorism (COE – DAT), Monthly Terrorism Report 01-30 April 2012

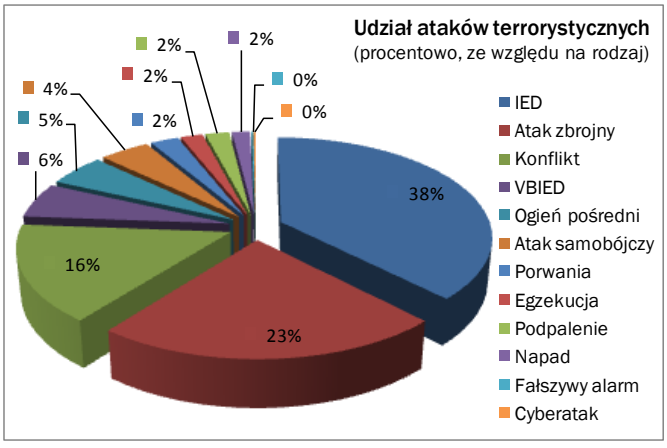


Diagram 1.
Opracowanie: T. Małysa, na podstawie danych COE - DAT

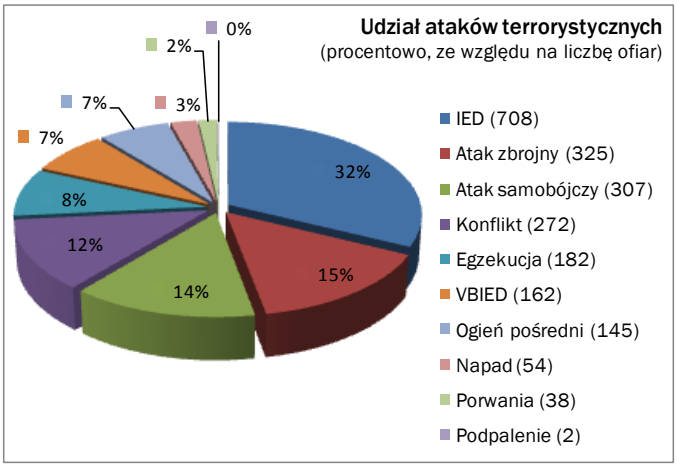


Diagram 2.
Opracowanie: T. Małysa, na podstawie danych COE - DAT

Centre of Exellence Defense Against Terrorism (COE – DAT – **www.coedat.nato.int**) *Opracował* ***Kazimierz Kraj***

Ataki terrorystyczne na świecie – maj 2012 r.

Lp.	Nazwa państwa	Liczba ataków	Zabici	Ranni	Porwani
1	Afganistan	92	166	124	20
2	Irak	86	97	261	0
3	Pakistan	83	139	318	4
4	Indie	42	23	27	2
5	Jemen	21	193	252	0
6	Syria	14	81	511	16
7	Somalia	14	27	23	0
8	Kolumbia	14	29	84	0
9	Turcja	14	10	21	16
10	Meksyk	10	63	9	0
11	Filipiny	10	12	31	0
12	Rosja	9	18	118	0
13	Tajlandia	9	10	12	0
14	Nigeria	7	40	31	5
15	Kenia	7	6	12	0
16	Nepal	6	1	0	0
17	Algieria	3	4	1	0
18	Birma	3	2	2	0
19	Włochy	3	1	10	0
20	Bangladesz	2	1	0	0
21	Argentyna	2	0	0	0
22	Zjednoczone Królestwo	2	0	0	0
23	Demokratyczna Republika Konga	1	27	60	0
24	Honduras	1	1	0	0
25	Liban	1	0	4	0
26	Bahrajn	1	0	4	0
27	Ukraina	1	0	3	0
27	USA	1	0	2	0
29	Benin	1	0	0	1
30	Iran	1	0	0	0
31	Tunezja	1	0	0	0
32	Ogółem	462	951	1920	64

Źródło: Centre of Exellence Defense Against Terrorism (COE – DAT), Monthly Terrorism Report 01 -31 May 2012

Ataki terrorystyczne na świecie – maj 2012 r.

Lp.	Rodzaj ataku	Liczba	Zabici	Ranni	Porwani
1	Improwizowany ładunek wybuchowy (IED)	170	196	468	0
2	Atak zbrojny	93	182	208	0
3	Konflikt	67	140	87	0
4	Ogień pośredni	36	60	159	0
5	Improwizowane ładunki wybuchowe montowane na pojazdach lądowych (VBIED)	26	32	138	0
6	Egzekucja	22	103	0	0
7	Atak samobójczy	21	228	854	0
8	Porwanie	12	0	0	64
9	Podpalenie	6	0	0	0
10	Napad	4	10	6	0
11	Fałszywy alarm	3	0	0	0
12	Cyberatak	2	0	0	0
13	**Ogółem**	**462**	**951**	**1920**	**64**

Źródło: Centre of Exellence Defense Against Terrorism (COE – DAT), Monthly Terrorism Report 01-31 May 2012

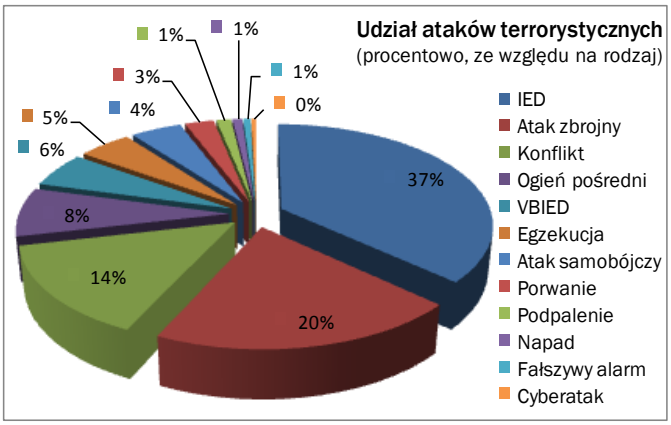


Diagram 1.
Opracowanie: T. Małysa, na podstawie danych COE - DAT

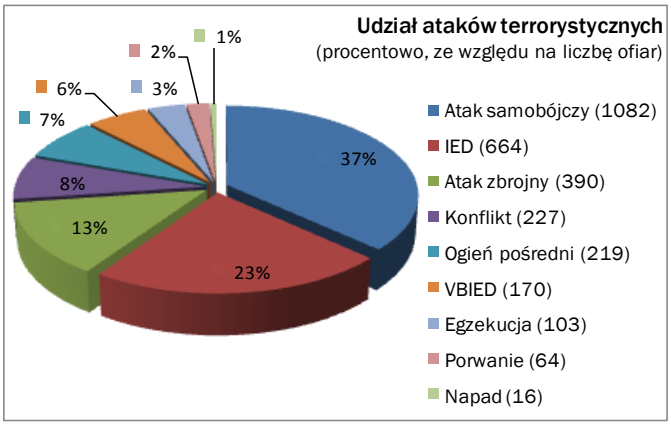


Diagram 2.
Opracowanie: T. Małysa, na podstawie danych COE - DAT

Centre of Exellence Defense Against Terrorism (COE – DAT – **www.coedat.nato.int**) *Opracował* ***Kazimierz Kraj***

Charakterystyka islamskiego terrorysty samobójcy

W artykule przedstawiam krótką charakterystykę terrorysty samobójcy wywodzącego się ze środowiska islamskiego. Jego wiek, status społeczny, czynniki kształtujące poglądy na słuszność postępowania, motywy działania.

Kim jest terrorysta samobójca? W odpowiedzi na to pytanie wielu ludzi powie, że pewnie to człowiek z problemami psychicznymi. Jednym słowem wariat, bo kto przy zdrowych zmysłach pozbawiałby się życia. W nielicznych przypadkach byłaby to może i słuszna odpowiedź, ale w większości to ludzie świadomi swoich czynów i mocno zdeterminowani w swym postępowaniu.

Terrorysta samobójca to człowiek młody w przedziale wiekowym od 16 do 28 lat, który pochodzi z klasy średniej. Niejednokrotnie posiada wyższe wykształcenie lub jest studentem. Dorasta w środowisku zamkniętym. Jego psychikę i poglądy kształtuje rodzina, szkoła koraniczna[1] i meczet, w którym krzewiony jest kult martyrologii[2]. Potencjalny terrorysta-samobójca niekiedy doznaje traumatycznego przeżycia widząc śmierć swoich bliskich, znajomych. Ciężkie obrażenia lub ich brutalne poniżanie. Powoduje to chęć zemsty, wzmaga nienawiść (np. do okupanta). Pojawia się marzenie: *zostać męczennikiem to jest coś*[3]. Kiedyś terrorystą samobójcą mógł zostać tylko mężczyzna, jednak już od kilku lat tendencja ulega zmianie.

Na zdjęciu: Samochód-pułapka uzbrojony w IED skutecznie zatrzymany przez siły ISAF w Kandaharze (Afganistan). Terrorysta samobójca usiłował wjechać nim w patrol żołnierzy. Po ostrzelaniu i unieruchomieniu pojazdu odnaleziono w nim trzy dużej siły urządzenia wybuchowe.
Fot. ISAF Headquarters Public Affairs Office from Kabul, Afghanistan.

Na zdjęciu: Pasy z materiałami wybuchowymi, przeznaczone do samobójczych zamachów, odnalezione przez Siły Obronne Izraela podczas operacji przeciwko radykalnej frakcji al-Fatah (Tanzim). Urządzenia przeznaczone były do ataków na terenie Izraela.
Fot. The Israel Defense Forces, http://www.flickr.com/photos/idfonline/

Terroryści samobójcy to nie tylko mężczyźni. Dużą grupę stanowią kobiety. Tworzone są specjalne oddziały kobiece w organizacjach terrorystycznych. Różni je pochodzenie, wykształcenie, ale łączą motywy skłaniające do oddania życia za Allacha. Są to:

- **przyzwolenie ze strony przywódców religijnych i wojskowych**: *Błogosławieństwo każdemu, kto wzniecił dżihad w imię Allacha*[4],
- **motyw narodowo-religijny:** walka z okupantem,
- **motyw społeczny:** nie tylko chęć zemsty za krzywdy, ale w dużej mierze presja i nacisk ze strony otoczenia w przypadku porzucenia przez męża, oskarżenia o zdradę czy posiadania dziecka przed ślubem. Czynniki te pozbawiają kobiety honoru, jedynym sposobem by go odzyskać jest śmierć w zamachu samobójczym,
- **motyw uczuciowy**: często ich mężowie należą do organizacji terrorystycznych,
- **motyw ekonomiczny**: organizacje terrorystyczne dobrze opłacają osoby wstępujące w ich szeregi, co pozwala na poprawę sytuacji ekonomicznej rodziny[5].

Kobiety, jak zostało przedstawione powyżej mają nieco inną motywację niż mężczyźni, by zostać męczenniczkami w imię Allacha. Wiele z nich to wdowy, które straciły bliskich w akcjach odwetowych ze strony władz po zamachach (konflikt izraelsko-palestyński). Fenomenem jest fakt, że zamachów dokonują także kobiety będące Europejkami, które przeszły na islam lub ich mężowie pochodzą z krajów islamskich.

Dużą rolę w kształtowaniu terrorysty samobójcy odgrywa organizacja terrorystyczna. Człowiek indoktrynowany od najmłodszych lat nie zawsze sam z siebie zostaje terrorystą samobójcą. Młodym człowiekiem, który szuka własnej drogi, zainteresowane są organizacje terrorystyczne. Po pozyskaniu ,,kandydata" na zamachowca członkowie organizacji poddają go odpowiedniemu procesowi szkolenia. Przyszli **szahidzi**[6] zostają wysyłani do specjalnych ośrodków szkoleniowych, gdzie zostają odpowiednio przeszkoleni. Przywódcy organizacji decydują o **miejscu** i **celu ataku** np. na: budynki w których mieszczą się siedziby władz państwowych, miejsca symboliczne, miejsca kultu, skupiska ludzi typu targowiska, hotele, oraz środki transportu. Podejmują decyzję o **czasie zamachu.** Wykorzystują różne metody by przekonać wybraną osobę o słuszności i celowości jej postępowania m. in.:

- **inicjują sytuacje**, od których nie ma odwrotu: nagrywanie kaset video z pożegnaniem i pisanie listów o podobnej treści,

Na zdjęciu: Fotografia dziecka z założonymi materiałami wybuchowymi. Zdjęcie odnaleziono w domu jednego z poszukiwanych terrorystów w mieście Hebron (Zachodni Brzeg Jordanu, Palestyna).
Fot. The Israel Defense Forces, http://www.flickr.com/photos/idfonline

- **utwierdzają** ją **w przekonaniu**, że śmierć w imię Allacha jest słuszna, przez co zamachowiec zyskuje poczucie zbawcy narodu, co ułatwia mu tylko dokonanie zamachu,
- **szantażują** kobiety, które zostały wykorzystane seksualnie przez członków organizacji, że ujawnią ten fakt, jeśli te nie zgodzą się zostać żywymi bombami,
- **przedstawiają korzyści**, jakie może osiągnąć zamachowiec, a także jego rodzina (palestyński terrorysta samobójca) i tak są to:
  - ***osobisty image*** (w społeczności, z której się wywodzi będzie postrzegany jako bohater, patriota, a przede wszystkim męczennik za wiarę),
  - ***osobiste korzyści*** (życie w raju w otoczeniu 72 hurys, ujrzenie Allacha),
  - ***korzyści dla rodziny*** (poprawienie statusu materialnego rodziny, a także obietnica, że 70 wybranych członków rodziny osiągnie życie wieczne)[7].

Wszystkie wymienione czynniki sprawiają, że młodzi ludzie oddają swoje życie w imię Allacha. Śmierć poniesiona w taki sposób jest traktowana jak śmierć poniesiona na polu bitwy.

Anna Rejman

Przypisy

1 W szkołach koranicznych znajdują się specjalne klasy, gdzie duchowni kształcą potencjalnych zamachowców korzystając z wybranych fragmentów Koranu lub innych pism o treści religijnej. W fragmentach tych idealizowana jest dobrowolna śmierć za Allacha i walka z niewiernymi.
2 Martyrologia «cierpienie i męczeństwo narodu lub wyznawców religii» http: //sjp.pwn.pl/slownik/2567116/martyrologia, 11-06-2012.
3 B. Hołyst, Terroryzm, Wyd. Lexis Nexis, Warszawa 2009, s. 831.
4 M. Adamczuk, Kobieca droga do... raju – próba analizy zjawiska terroryzmu samobójczego kobiet (zarys problemu), [w:] K. Liedel, P. Piasecka, T. R. Aleksandrowicz (red), Bezpieczeństwo w XXI wieku, Wyd. Difin, Warszawa 2011, s. 104.
5 Tamże. s.105. Szeregowy członek organizacji zarabia miesięcznie od 300 do 600 dolarów, a rodzina terrorysty samobójcy otrzymuje od 500 do 1500 dolarów.
6 Szahid (męczennik) to ten, który oddaje swoje życie w sprawie Bożej, za co ma obiecaną nagrodę wieczną, czyli życie w raju. http://www.niedziela.pl/artykul_w_niedzieli.php?doc=nd200541&nr=13, 11-06-2012.
7 B. Bolechów, Terroryzm, aktorzy, statyści, widownie, PWN Warszawa 2010, s. 175.

Zagrożenie IED w historii

Kontynuując problematykę IED pragnę wrócić do jej początków, czyli historii. Mówiąc o tak zwanych w gwarze wojskowej – *ajdikach* – pomijamy cały wątek ewolucji zagrożenia. Możemy stwierdzić, że historia IED rozpoczęła się od wilczych dołów. Następnie przyszły granaty i urządzenia wybuchowe, miny aż do współczesnych IED. Od zarania dziejów człowiek konstruował różnego rodzaju pułapki. Na początku były to zwykłe doły, w których wbite były dobrze zamaskowane, zaostrzone pale, w które wpadały mamuty. Z czasem ten sposób zaczęto nazywać wilczymi dołami. Z upływem lat przerodziło się w sposób walki z przeciwnikiem, który chciał zająć nasze terytorium. Powstawały wszelkiego rodzaju fortyfikacje od grodzisk przez grody, zamki do twierdz i cytadel, gdzie stosowano wszelkiego rodzaju przemyślne pułapki. Budowano umocnienia uniemożliwiające przeciwnikowi dostanie się do środka. Ważnym celem było spowodowanie jak największych strat po stronie przeciwnej. Początki państwa Polskiego wiążą się z walką za pomocą wilczych dołów, paści, przesieków itp. Nowoczesne metody walki za pomocą czarnego prochu oraz wilczych dołów zastosowali Krzyżacy pod Grunwaldem w 1410 r.

Fot. 1, Afganistan

Fot. 2, Afganistan

Pierwsze granaty, nie były niczym innym, tylko chałupniczo robionymi i produkowanymi na potrzeby obrońców ręcznymi bombami. Wynalazca i konstruktor testował takie urządzenie na oblegających. Jego skuteczność psychologiczną i praktyczną. Likwidował przeciwnika przez rażenie odłamkami lub samą falą uderzeniową, Te granaty można nazwać pierwszymi improwizowanymi urządzeniami wybuchowymi. Można je porównać do współczesnych IED, gdyż jak w przeszłości tak i współczesne są wytwarzane domowymi sposobami z amunicji artyleryjskiej (fot. 1), bomb lotniczych oraz konstruowane z pozornie bezpiecznych i powszechnie używanych przedmiotów (fot. 2).

Pierwszy historyczny zapis o użyciu żeliwnej bomby w Europie pochodzi z 1467 roku. Na większą skalę granaty rozpowszechniły się na przełomie wieków XVI i XVII. Ze względu na ich dużą masę, rekrutowano do ich miotania silnych żołnierzy, grupując ich w oddziały grenadierów[1]. XVI wiek przyniósł postęp technologiczny w postaci zamka kołowego[2] do broni strzeleckiej, umożliwił konstruowanie różnego rodzaju pułapek minerskich, w których zaczęto stosować mechanizmy zegarowe, pozwalające na konstruowanie bomb-pułapek[3]. Początek XX wieku, I wojna światowa dała szerokie pole do popisu dla konstruktorów min, pułapek i innych urządzeń mogących zabijać lub ranić


Fot. 3, Afganistan

żołnierzy przeciwnika. Zaczęto produkować na masową skalę wszelkiego rodzaju zapalniki tarciowe, chemiczne. W początkowym okresie wykorzystywano niemieckie **granaty ręczne**[4] *stielhandgranate i brytyjskie bomby Millsa*[5], których używano do minowania wszystkiego, co się dało: od puszek z jedzeniem po wszelkiego rodzaju sprzęt, broń, wyposażenie, drogi podejścia do okopów, okopy, miejsca zakwaterowania lub ukrycia. Wszelką dostępną technikę wojskową, którą przeciwnik mógłby wykorzystać. Obie wojujące strony bardzo często korzystały z takiej możliwości[6]. Przy czym żołnierze niemieccy wykazywali się dużą dozą pomysłowości w demoralizacji wojsk przeciwnika. Jednym z nich było zakładanie ładunków wielkiej mocy, wybuchających z dużym opóźnieniem[7].

II Wojna Światowa pokazała jak śmiertelne żniwo mogą zebrać wszelkiego rodzaju domowymi sposobami konstruowane ładunki wybuchowe.


Fot. 4, Afganistan


Fot. 5, Irak

Nie zbyt odległym dużym konfliktem, w którym zostały wykorzystane różnego rodzaju pułapki była wojna w Wietnamie. Partyzanckie oddziały Vietkongu stosowały przeróżnego rodzaju pułapki począwszy od stosowania min do dołów najeżonych palami bambusowymi.

Jan Czarny

Przypisy

1 http://pl.wikipedia.org/wiki/Granat_ręczny.

2 Zamek kołowy (zamek krzosowy) – zamek ręcznej broni palnej odprzodowej, w którym zapalenie prochu następuje od iskier powstałych przez pocieranie obracającego się karbowanego koła o piryt zamocowany w szczękach kurka. Przed odpaleniem należało nakręcić sprężynę koła za pomocą klucza. Naciśnięcie spustu broni zwalniało sprężynę i powodowało obrót koła. Iskry padające na panewkę wywoływały zapalenie się podsypanego tam prochu, a następnie poprzez zapał, odpalenie prochu w lufie. Źródło online: [http://www.naukowy.p/encyklopedia/Zamek_ko%C5%82owy], dostęp: 18.05.2012.

3 Skrzynia pułapka został użyta przez Polaków oblegających Psków. Wysłali skrzynię do dowódcy obrony miasta. Kiedy skrzynia została otwarta zabiła znajdujących się w pobliżu. I. Jones „Złośliwa śmierć. Historia pułapek wojennych od I w – do Wietnamu", Warszawa 2005, s. 14.

4 Pierwsze wersje granatów składały się ze skorupy z papieru, ceramiki lub niskiej jakości szkła, wypełnionej prochem i czasem dodatkowo siekańcami metalowymi lub substancjami mającymi zwiększyć ich działanie bojowe np. kwasem, substancjami zapalnymi, lub drażniącymi (np. wapno palone). Zapalnik miał postać lontu, który należało podpalić przed rzuceniem, co utrudniało ich użycie. Granaty takiej postaci pojawiły się w Chinach za czasów dynastii Tang.

5 http://www.naukowy.pl/encyklopedia/Granat_r%C4%99czny#-18-05-2012.

6 Szczególną uwagę można zwrócić na moment, kiedy Niemcy wycofywali się na linie Hindenburga lub jak Anglicy z Gallipoli. I. Jones, „Złośliwa śmierć…", op. cit., s. 25-50.

7 Tamże, Ratusz w wiosce Baupame marzec 1917, lub Athies 1917.

Fot. autor i archiwum autora z misji PKW Afganistan oraz PKW Irak

Stopnie zagrożenia terrorystycznego w Federacji Rosyjskiej

Nieco ponad tydzień temu, 14 czerwca prezydent Federacji Rosyjskiej Władimir Putin podpisał dekret określający stopnie zagrożenia terrorystycznego. Ich przyjęcie powoduje podejmowanie dodatkowych przedsięwzięć mających na celu zapewnienie bezpieczeństwa ludzi, społeczeństwa oraz państwa. Możliwość określania stopni zagrożenia terrorystycznego została zadekretowana w podczas nowelizacji ustawy *O przeciwdziałaniu terroryzmowi*[1] w dniu 3 maja 2011 r. Artykuł 5 przywoływanej ustawy daje prezydentowi FR prawo wprowadzania stopni zagrożenia terrorystycznego, nieograniczających praw i swobód obywateli, w celu wdrożenia dodatkowych przedsięwzięć podnoszących poziom bezpieczeństwa ludzi, społeczeństwa oraz państwa[2].

Omawiany dekret określa porządek wprowadzania i ogłaszania dla podmiotów biorących udział w przeciwdziałaniu zagrożeniu terrorystycznemu konkretnych stopni zagrożenia (niebezpieczeństwa) terrorystycznego.

Zgodnie z dekretem stopnie *niebieski* (podwyższony) oraz *żółty* (wysoki) na okres do 15 dób ogłasza, zmienia i odwołuje przewodniczący komisji antyterrorystycznej właściwego podmiotu Federacji Rosyjskiej w porozumienie z kierownikiem terytorialnego organu Federalnej Służby Bezpieczeństwa. O fakcie tym niezwłocznie zostaje poinformowany przewodniczący Narodowego Komitetu Antyterrorystycznego – Dyrektor FSB. Oczywiście konkretny stopień zagrożenia ustala się na podstawie informacji na temat sytuacji w podmiocie federacji, czy części tego podmiotu (rejonie, mieście, konkretnym obiekcie itp.).

Niebieski stopień zagrożenia terrorystycznego powoduje, że można podejmować m in. przedsięwzięcia takie jak: pozaplanowe przeciwdziałanie w celu sprawdzenia możliwości dokonania ataku terrorystycznego, dodatkowe instruktaże prowadzone dla oddziałów policji i innych służb mundurowych, personelu potencjalnych celów zamachów terrorystycznych, wzmocnienie patroli, w tym z udziałem psów w miejscach masowego przebywania ludzi. Innymi działaniami podejmowanymi podczas stanu *niebieskiego* są: wzmocnienie kontroli w portach lotniczych, obiektach metra, dworcach kolejowych itp. Uprawnione służby dokonują przeglądu infrastruktury krytycznej i miejsc, gdzie potencjalnie można podłożyć ładunki wybuchowe. Przeprowadza się również rozpoznanie przy pomocy środków technicznych miejsc masowego przebywania obywateli, mające na celu wykrycie założonych ładunków wybuchowych. Ponadto ludność powinna być na bieżąco informowana na temat postępowania w warunkach zagrożenia terrorystycznego.

Przy stopniu *żółtym* wprowadza się podwyższony stopień gotowości jednostek służby zdrowia, dokonuje sprawdzenia gotowości personelu i jednostek organizacyjnych potencjalnych obiektów zamachów terrorystycznych, instytucji związanych z zarządzaniem kryzysowym i przeprowadza ich szkolenie w działaniach mających na celu zapobiegnięcie aktowi terrorystycznemu oraz ratowanie ludzi. Ponadto właściwe służby prowadzą wzmożony nadzór nad poruszaniem się obywateli FR, poruszaniem się przedstawicieli władz, reżimem meldunkowym, stałym lub czasowym pobytem, wjazdem i wyjazdem osób z terytorium Rosji, tranzytem przez terytorium FR.

Najwyższy stopień zagrożenia terrorystycznego *czerwony,* powoduje, że w stan gotowości stawiane są siły i środki niezbędne dla przeprowadzenia operacji kontrterrorystycznej, służby medyczne działają w reżimie sytuacji nadzwyczajnej, ulega wzmocnieniu ochrona potencjalnych obiektów zamachów terrorystycznych, przygotowuje się miejsca czasowego pobytu ludności w związku z wprowadzeniem na danym terytorium (obiekcie) reżimu operacji kontr-terrorystycznej, zabezpiecza wyżywienie i ubranie. Podejmowane są również natychmiast niezbędne przedsięwzięcia dla ratowania ludzi, ochrony majątku pozostającego bez właściciela, zapewnia nieprzerwaną pracę służb ratowniczych. Do stanu gotowości doprowadzane są środki transportowe dla celów ewakuacji ludzi, jednostki służ-

by zdrowia w celu przyjęcia osób poszkodowanych podczas aktu terrorystycznego. Następuje również wzmocnienie kontroli nad poruszaniem się środków transportu przez granice administracyjne podmiotu FR, na którym został ustanowiony stopień *czerwony* zagrożenia terrorystycznego. Kontrola środków transportu ma na celu wykrycie broni i materiałów wybuchowych.

Podsumowując możemy stwierdzić, że wprowadzenie w Rosji stopniowania zagrożenia terrorystycznego ma celu polepszenie ochrony ludności, społeczeństwa i państwa oraz obiektywne informowanie obywateli o zagrożeniu i uzyskanie ich pomocy dla celów przeciwdziałania zagrożeniom terrorystycznym.

KraK

Przypisy

1 Ustawa była uchwalona w marcu 2006 r.
2 Również ustawa O bezpieczeństwie z 28 grudnia 2010 r. wskazuje, że priorytetem w zapewnieniu bezpieczeństwa są przedsięwzięcia uprzedzające, systemowość i kompleksowość podejścia.

Nie żyje generał Sławomir Petelicki

Fot. Marek Strzałkowski. Arch. MMS Komandos

„Siła bez honoru jest pusta, jałowa. Niszczy. Nie umie budować. A honor... Bez honoru nie da się, po prostu..."

(Sławomir Petelicki w rozmowie z Michałem Komarem – GROM. Siła i Honor)

Dnia 16 czerwca 2012 roku zmarł twórca i dowódca jednostki wojskowej GROM, generał brygady Sławomir Petelicki. Miał 65 lat. Generał Sławomir Petelicki zostanie pochowany 26 czerwca b.r. w Alei Zasłużonych na cmentarzu na warszawskich Powązkach W uroczystości pogrzebowej wezmą udział poza rodziną i bliskimi – politycy, osoby związane z jednostką GROM i przedstawiciele Sił Zbrojnych RP. Gen. Sławomir Petelicki pełnił służbę na placówkach dyplomatycznych m.in. w Chinach, Szwecji, USA i Wietnamie. Był twórcą i dowódcą jednostki antyterrorystycznej GROM. W swojej karierze był m. in. szefem Wydziału Ochrony Placówek MSZ, oficerem wywiadu PRL. Uczestniczył w wielu zagranicznych operacjach wojskowych.

Wszystkie jego umiejętności i zdolności zdobyte podczas służby wojskowej nie jest łatwo wymienić. Jako żołnierz do zadań specjalnych posiadał szereg specjalistycznych uprawnień m.in. płetwonurka, snajpera, skoczka spadochronowego wojsk powietrznodesantowych i kierowcy pojazdów wojskowych. Posiadał honorowe członkostwo Sił Specjalnych Stanów Zjednoczonych. Został odznaczony m.in. Krzyżem Komandorskim Orderu Odrodzenia Polski i Krzyżem Zasługi za Dzielność. Po odejściu z armii zajął się biznesem, pracował m. in. w firmie doradczej Ernest & Young.

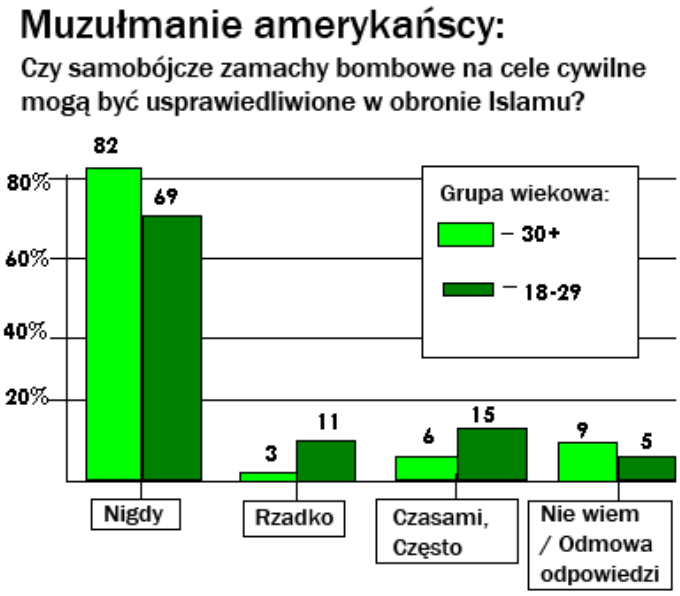
Islamofobia

Największa migracja muzułmanów do Wielkiej Brytanii rozpoczęła się wraz z końcem jej imperium kolonialnego, jako odpowiedź na zapotrzebowanie wyspiarzy na siłę roboczą. Anglia oferowała emigrantom lepsze warunki bytowe. Muzułmanie osiedlając się tu na stałe rozpoczęli budowanie meczetów (13 w 1963 r., 338 w 1985 r.), szkół i organizacji religijnych[1]. Mimo powiększania się muzułmańskiej mniejszości narodowej, nie była ona objęta ochroną praw gwarantowanych przez ustawę z 1976 r. regulującą stosunki rasowe w Wielkiej Brytanii (w 1983 ustawa objęła żydów i sikhów, muzułmanów jednak nie)[2].

Islamofobia

Termin ten powstał pod koniec lat 80, kiedy zaczęła narastać dyskryminacja religijna muzułmanów. Islamofobia to „nieuzasadniona wrogość w stosunku do islamu, która przekłada się na niesprawiedliwą dyskryminację osób i społeczności muzułmańskiej przez wyłączenie tychże poza życie polityczne i społeczne”[3]. Raport Komisji ds. Brytyjskich Muzułmanów i Islamofobii z 1997 r. poruszał problem braku rozróżnienia w prawie brytyjskim dyskryminacji religijnej, która utrudniała praktyki religijne w miejscu pracy i powodowała niedostateczną ochronę ofiar przemocy, ponieważ prawo przewiduje wysoką karę za atak na tle rasowym, nie zaś religijnym[4]. Raport już wtedy ukazywał problem wizerunku islamu w mediach, który ukształtował stereotypowe postrzeganie muzułmanów.

O wydarzeniach na świecie dowiadujemy się głównie i najczęściej z mediów, którym dramatyczne lub kontrowersyjne tematy dają największą oglądalność. Jednak obrazy medialne kształtują ludzkie postrzeganie bohaterów wiadomości w określony sposób. Jeśli widz „karmiony” jest relacjami z systematycznie przeprowadzanych zamachów w Iraku, bądź też ogląda wiejące grozą komentarze dotyczące przebiegu wyborów w Turcji w 2007 r., czy słucha o sposobie traktowania



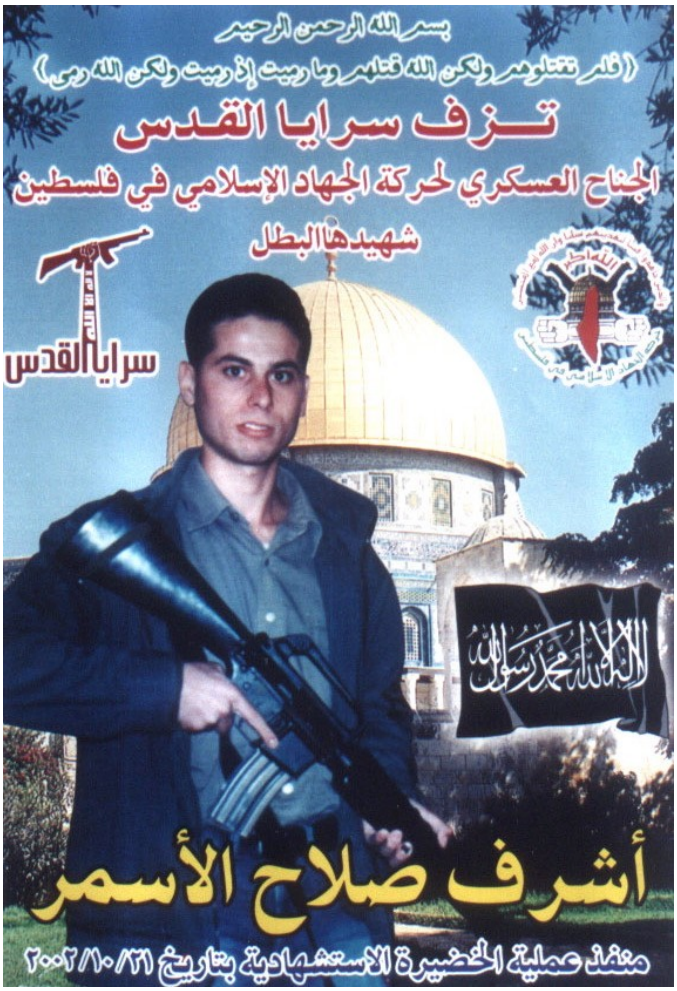
Wykres bazowany na ankiecie Pew Research Center z 2006 roku. Ukazuje opinie amerykańskich muzułmanów na temat samobójczych zamachów bombowych, popełnianych osobno lub w grupach.
Źródło: http://pewresearch.org/assets/pdf/muslim-americans.pdf
commons.wikimedia.org

kobiet w burkach i hidżabie, to właśnie na takiej podstawie kształtuje sobie obraz typowego muzułmanina. 11 września zrodził strach przed islamem, fanatycy religijni nie pozwalają zapomnieć o tym lęku. Relacje medialne z incydentów dotyczących ludności muzułmańskiej podsycają tylko panikę, sprawiają, że żyjemy w ciągłej gotowości na najgorsze. Na słowo „muzułmanin” pojawia się w myślach obraz walącego się WTC i nieuchwytnego bin Ladena.

Wg sprawozdania EUMC z 2006 r. „Muzułmanie w UE: dyskryminacja i islamofobia” wielu muzułmanów jest dyskryminowanych w sferze zatrudnienia (w Wielkiej Brytanii bezrobocie wśród wyznawców islamu jest wyższe niż wśród innych grup religijnych. Pracodawcy wolą zatrudniać osoby nie-muzułmańskiego wyznania), edukacji (różnica wyników między emigrantami a Anglikami) i w mieszkalnictwie (gorsze warunki mieszkaniowe, mała ilość lokali socjalnych)[5]. Mają miejsce akty agresji na tle religijnym.

Wizerunek muzułmanów

Jednym z pierwszych incydentów uderzających w religię islamską było wydanie w 1989 r. „Szatańskich Wersetów" Rushdiego, na którego ajatollah Chomeini nałożył fatwę za obrazę uczuć religijnych. W Bradford miało miejsce publiczne spalenie tej książki[6]. Wydarzenie było wielką gratką dla mediów, które w krzywym zwierciadle wykreowały całą brytyjską mniejszość muzułmańską, na fanatyczną, chcącą cenzurować wolność słowa grupę wyznaniową[7]. Wojna w Zatoce Perskiej ugruntowała pogląd o antydemokratycznych, antyzachodnich i agresywnych cechach islamu. Jednak dopiero 11 września, zamach na londyńskie metro i tragedia w Madrycie doprowadziły do potężnej eksplozji islamofobii. Islam przestał być postrzegany tylko jako seksistowska, prymitywna i zamknięta na postęp, agresywna religia, często wykorzystywana dla celów politycznych. Stał się symbolem zła, krwi niewinnych, podwaliną wojny cywilizacji. Zdawała się spełniać przepowiednia Huntingtona. W Europie niszczono meczety, atakowano muzułmanów lub osoby, które za nich uważano (turbany sikhów sprowadziły na nich ataki, gdyż „upodabniały" ich do talibów)[8].



Na zdjęciu: plakat propagandowy gloryfikujący terrorystę-samobójcę Ashrafa Sallah Alasmara, odnaleziony w mieście Jenin (Autonomia Palestyńska).
Fot: Israel Defense Forces

30.09.2005 r. duński „Jylland-Posten" opublikował 12 karykatur Mahometa, czego skutkiem były demonstracje muzułmanów na Bliskim Wschodzie, nawoływanie do bojkotu duńskich towarów, zniszczenie ambasad Danii i Norwegii w Damaszku[9]. Reakcje w Europie były dwojakie. Krytycznie do karykatur odniósł się m.in. premier Turcji, Biały Dom, patriarcha Konstantynopola, zaś przedruk przez „Rzeczpospolitą" 2 karykatur Mahometa potępił premier Marcinkiewicz[10]. Z drugiej strony pojawili się przedstawiciele mediów, wołający o obronę wolności słowa, protestujący przeciw szczególnemu traktowaniu muzułmanów. Zamiast dialogu o wolności wypowiedzi nienaruszającej uczuć religijnych, społeczeństwa ujrzały wyznawców islamu jako „święte krowy"[11] - fanatyków o szczególnych prawach, którzy wszystko, co pojawia się w mediach, uważają za atak na własną religię.

„Islamizacja Europy"

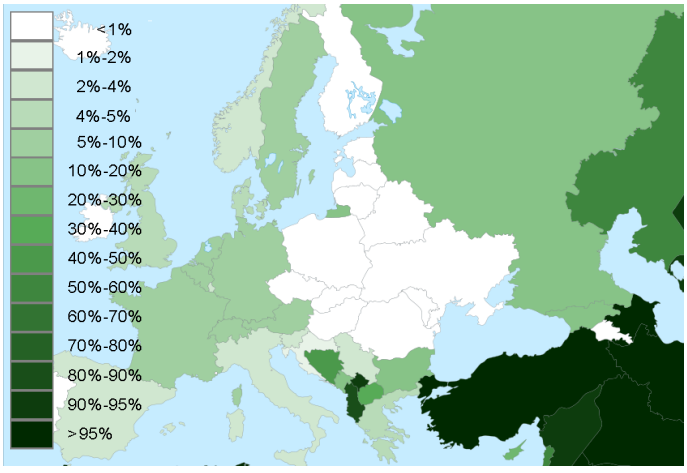
Prócz terroryzmu społeczność europejska obawia się także „zalania" kontynentu przez wyznawców islamu. Dzięki dużemu przyrostowi demograficznemu (ludność Ziemi przyrasta o 2-3% rocznie, ludność muzułmańska o 2,8%) liczba wyznawców Allaha wg prognoz sięgnie w 2050 r. 20% ich udziału w populacji europejskiej (obecnie wynosi on 5%, czyli 24 mln. ludności łącznie z Bałkanami)[12]. Będzie się to przekładało na wzrost aktywności kulturowej i politycznej, na wywieranie przez społeczność muzułmańską większego wpływu na rządy państw, w których zamieszkują.

Strach widać wszędzie. W 2007 r. miała się odbyć demonstracja „Stop the Islamization of Europe", która chciała ostrzec przed zagrożeniem, jakie niosą muzułmanie w sferze wolności słowa i bezpieczeństwa[13]. W 2005 r. 80% Niemców słowo „islam" kojarzyło z terroryzmem i dyskryminacja kobiet[14]. W Polsce niechęć do Arabów deklaruje 70% badanych a 53% do Turków. 30% Polaków nie chciałoby mieszkać obok muzułmanina, Niemców 10%[15]. W 2007 r. 40% mieszkańców Wielkiej Brytanii bało się islamu i spodziewało kolejnego aktu terrorystycznego w przeciągu roku[16]. Twierdzili także, że ludność muzułmańska ma zbyt dużą władzę.

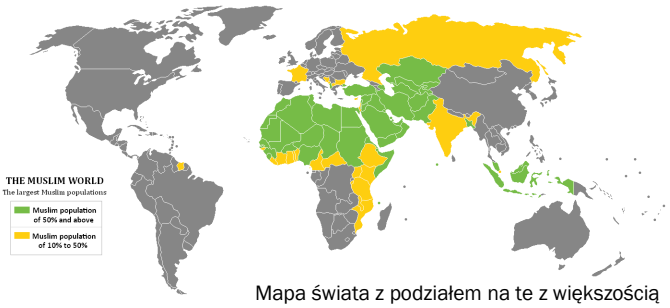
Straszenie islamem.

Daniel Pipes wymienia listę przywilejów domaganych się przez muzułmanów na świecie[17]:

- „Wyłączenie części miejskiego kąpieliska tylko dla kobiet, jak we Francji;
- Wykluczenie Hindusów i Żydów ze składu sądu, w sprawie dotyczącej islamisty, jak w Wielkiej Brytanii;
- Zezwolenie na to, by więzień-muzułmanin nie podlegał przeszukaniom połączonym z rozbieraniem, jak w stanie Nowy Jork;
- Wykorzystywanie finansowanych z podatków szkół i stacji radiowych dla nawracania na islam nie - muzułmanów jak w Ameryce;
- Karanie za poglądy anty-islamskie przymusową indoktrynacją pod rygorem sądowym, proponowane przez islamistę z Kanady;
- Wymaganie, aby kobiety służące w wojsku amerykańskim w Arabii Saudyjskiej nosiły abaye lub suknie do kostek, wydawane im przez władze USA;
- Stosowanie „Reguł przeciwko Rushdiemu" – lub pozwalanie muzułmanom na tłumienie krytyki islamu i muzułmanów".



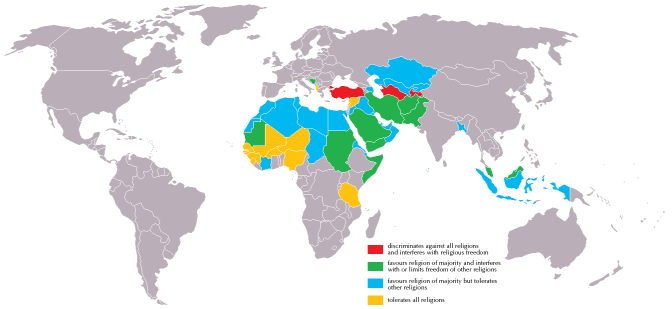
Udział muzułmanów w populacji krajów Europy
Źródło: features.pewforum.org, commons.wikimedia.org



Mapa świata z podziałem na te z większością i ze znaczną mniejszością muzułmańską.
Kolor zielony - populacja muzułmanów powyżej 50%
Kolor żółty - populacja muzułmanów od 10% do 50%
Autor: Mohsin, commons.wikimedia.org

Islamofobia czy islamizmofobia?

Daniel Pipes (który siebie nazywa islamizmofobem -przeciwnikiem radykalnego islamu, islamizmu)[18] pisze, że „brytyjscy muzułmanie mają rzekomo cierpieć z powodu dyskryminowania ich przez policję", zaś wg „aktualnych statystyk policyjnych sporządzonych przez K.Malika (...) islamofobia jest mitem"[19]. Wskazuje także, iż „islamistyczne wyzwanie (zagrożenie) sprowokowało Europejczyków do podtrzymywania własnych tradycji: „zakaz noszenia burki (muzułmański kwef dla kobiet) we Włoszech, zmuszenie niemieckiego ucznia (muzułmanina) do uczestniczenia w koedukacyjnych zajęciach pływackich i zmuszenie (muzułmańskich) mężczyzn, starających się o obywatelstwo irlandzkie, do wyrzeczenia się wielożeństwa. Gdy znany belgijski polityk odmówił spożycia lunchu z delegacją Iranu, kiedy jej członkowie zażądali by nie podawano do posiłku alkoholu, jego rzecznik wyjaśnił: „Nie możecie zmuszać członków władz Belgii do picia wody"[20]. Pipes pokusił się także w 2007 r. o „przepowiadanie" przyszłości: „Wiele przesłanek wskazywało na wojnę, która wybuchła 19.06.2008 (...) 51 bomb wybuchło w ciągu zaledwie kilku godzin w każdym ze stanów i w dystrykcie



Mapa obrazuje rodzaj wolności religijnej w krajach uważanych za muzułmańskie.
Kolor czerwony - dyskryminacja wszystkich religii w oficjalnym życiu państwowym
Kolor zielony - faworyzowana religia większości mieszkańców, ograniczona wolność innych religii
Kolor niebieski - faworyzowana religia większości mieszkańców, ale tolerowane są inne religie
Kolor żółty - brak faworyzacji określonej religii, tolerowane są wszystkie
Autor: Mohsin, commons.wikimedia.org

Kolumbia (...). W 2009 r.(...) Mecca Cola zastąpiła Coca-Colę (...), lalki Fulla i Razanne – Barbie doll (...). Terrorystyczna kampania zakończyła się w 06.2012 (...). Amerykańscy islamiści zdali sobie sprawę z własnych błędów taktycznych i zdecydowali się na zaprzestanie stosowania przemocy. Podobnie jak ich sojusznicy ideowi w Egipcie, Syrii i Algierii, przyjęli metody działania zgodnie z prawem i od tego czasu stali się częścią panującego systemu(...). Czy Konstytucja USA z 1787 r. pozostanie w mocy, czy będzie kiedyś uzupełniona lub nawet zastąpiona przez Koran i prawo szarijatu?"[21].

Na zdjęciu: plakat propagandowy ugrupowania „Islamski Jihad" wychwalający terrorystkę-samobójczyni. Przeprowadziła ona atak na centrum handlowe w mieście Afula (Izrael) zabijając 3 ludzi.
Fot: Israel Defense Forces

Muzułmanów w Europie cechuje zróżnicowane pochodzenie etniczne, językowe, kulturowe i polityczne. Atak na WTC zrodził strach nie tylko przed dżihadem, ale przed całą społecznością islamską. Ujednolica się ją, szufladkuje pojęcia do postaci „Arab-muzułmanin-terrorysta", jak to ujął P. Kłodkowski. Kultura Zachodu rozszerza się na Wschód, islam zdobywa nowych wyznawców oraz „przenosi" się, rozrasta na Zachód. Tym bardziej trzeba zrozumieć, że ta religia to nie tylko zamachowcy. To miliony ludzi, którzy chcą normalnie żyć, kultywować swoją wiarę, wychowywać dzieci. Trzeba walczyć z terroryzmem, ale nie z muzułmanami; mówić o problemie ekstremizmu, ale nie widzieć w każdym wyznawcy Allaha mordercy z ładunkiem na ciele. Gdy tego nie zrozumiemy, ziści się „zderzenie Huntingtona". Będzie to zderzenie naszego strachu przed islamem z cywilizacją muzułmanów.

Ewa Wolska

Przypisy

1 http://www.euroislam.republika.pl/referaty/islamofobia-stawiarska.doc, s.2.
2 http://www.euroislam.republika.pl/referaty/islamofobia-stawiarska.doc, s.3.
3 http://www.euroislam.republika.pl/referaty/islamofobia-mazur.doc, s.1.
4 http://www.euroislam.republika.pl/referaty/islamofobia-mazur.doc, s. 2.
5 http://fra.europa.eu/fra/material/pub/muslim/EUMC-highlights-PL.pdf
6 http://www.euroislam.republika.pl/referaty/islamofobia-stawiarska.doc, s.2.
7 http://www.euroislam.republika.pl/referaty/islamofobia-mazur.doc, s.3.
8 http://www.europa21.pl/Article658.html
9 http://www.kosciol.pl/article.php/20060204155511502
10 tamże
11 http://www.racjonalista.pl/kk.php/s,4665
12 http://www.opoka.org.pl/biblioteka/I/IR/religijnosc_xx_w.html
13 http://islaminfo.pl/index.php/08/10/burmistrz-brukseli-zakazal-demonstracji-przeciwko-szarii-w-europie/
14 http://www.europa21.pl/Article658.html
15 http://www.arabia.pl/content/view/282077/2/
16 http://islaminfo.pl/index.php/08/23/wyspy-strachu-brytyjczycy-boja-sie-islamu/
17 wszystkie cytaty pochodzą ze źródła: http://konserwatyzm.pl/content/view/2911/111/
18 http://pl.danielpipes.org/article/3078
19 http://pl.danielpipes.org/article/3078
20 http://pl.danielpipes.org/article/2927
21 http://pl.danielpipes.org/article/4734

Komunikacja z mediami w sytuacji kryzysowej

Sytuacje kryzysowe to rozmaite wydarzenia. Ich wspólną cechą jest tymczasowość i nagłość wystąpienia (po ewentualnych okresach narastania napięcia) oraz groźne skutki związane z oddziaływaniem zagrożeń. To zdarzenia bardzo emocjonujące i przykuwające uwagę mediów. Sytuacja kryzysowa może dotknąć każdy podmiot, niekoniecznie gminę albo powiat. Wszelkie instytucje oraz przedsiębiorstwa, także nie są od nich wolne. Zmienia się rodzaj zagrożeń oraz ich skala, również inna może być rola i zadania podmiotu odpowiedzialnego za reagowanie na zdarzenie. Nie trzeba powodzi lub katastrofy budowlanej, aby organizacja stanęła przed bardzo trudną i złożoną sytuacją. Wystarczy popełnienie przestępstwa na terenie jednego z jej obiektów, aby po ujawnieniu zdarzenia zjawił się wraz z nim szereg dylematów i trudnych zadań. Jednym z takich problemów może być komunikacja. Jak odpowiadać na pytania mediów? Jak się zachować? Informować, udzielać odpowiedzi, czy zbywać dziennikarzy odmawiając komentarza.

Komunikacja w sytuacjach kryzysowych a wizerunek organizacji

Jedną z największych katastrof ekologicznych było zatonięcie u wybrzeży Hiszpanii tankowca Prestige[1]. Należący do greckiego armatora statek transportował ciężki olej napędowy (mazut - jedna z form destylacji ropy naftowej) w ilości ponad 70 tysięcy ton. Dnia 13 listopada 2002 roku na pokładzie doszło do wybuchu i uwolnienia 5 tysięcy ton ładunku. Statek zaczął dryfować. Załoga została ewakuowana, a rząd hiszpański postanowił pozwolić tankowcowi zatonąć, bagatelizując możliwość dalszego wycieku ładunku. Niecały tydzień później, kadłub przełamał się i statek idąc na dno uwolnił ogromną część mazutu ze zbiorników. Skutki ekologiczne były fatalne. Setki kilometrów wybrzeża zostało zanieczyszczonych, a w wielu regionach zabroniono na długi czas rybołówstwa wywołując lokalnie wielkie straty ekonomiczne wśród ludności żyjącej z połowów.

Czy rząd hiszpański był odpowiedzialny za fatalny stan techniczny okrętu, co doprowadziło do awarii tak groźnej w skutkach? Czy odpowiedzialność za katastrofę spadała na rząd? Zdaniem opinii publicznej – tak. Przyczyniła się do tego opieszałość rządzących w reagowaniu na kryzys oraz oskarżenia ze strony opozycji. Podstawowe błędy popełniono jeśli chodzi o komunikację z mediami. Rząd umniejszał znaczenie problemu, przez bardzo długi czas brak było oficjalnej wersji wydarzeń, czy informacji o podejmowanych działaniach. Wiadomości pochodziły z wielu źródeł. Media ukazywały przede wszystkim skalę zniszczeń środowiska i nieudolność rządu, który, gdy już zaczął oficjalnie się wypowiadać na temat katastrofy, próbował zrzucać winę na innych, w tym na opozycję. Zamiast podjąć próbę kształtowania opinii publicznej poprzez odpowiednio przemyślaną strategię komunikacji, najpierw próbowano udawać jakoby nic się nie stało. Na zarzuty odpowiadano zarzutami. W ten sposób opinia publiczna znalazła winnego za całą sytuację. Winnym stał się hiszpański rząd, bez względu na rzeczywisty stopień przyczynienia się do ostatecznych rozmiarów tej katastrofy[2].

Błędem byłoby jednak sądzić, że tylko „typowe" podmioty takie jak lokalne samorządy lub służby mogą stanąć przed sytuacjami kryzysowymi. Dotykają one także przedsiębiorstwa. Szczególnie dotyczy to katastrof komunikacyjnych, budowlanych, awarii technicznych czy skażeń lub zatruć. Na szali ważą się wtedy wizerunek oraz reputacja firmy, jej przyszłe „być albo nie być", o czym mogą zdecydować klienci. Okazuje się, że nawet jeśli do tragedii doszło z winy przedsiębiorstwa, przy odpowiednim zaplanowaniu komunikacji kryzysowej można z każdej sytuacji wyjść zachowując twarz. Kluczowe okazują się media – to one kształtują opinię publiczną. Media nie są wrogiem, to po prostu pole bitwy[3].

Czy doświadczenia biznesu z komunikacją kryzysową mogą być cenne również dla innych jej potencjalnych uczestników?

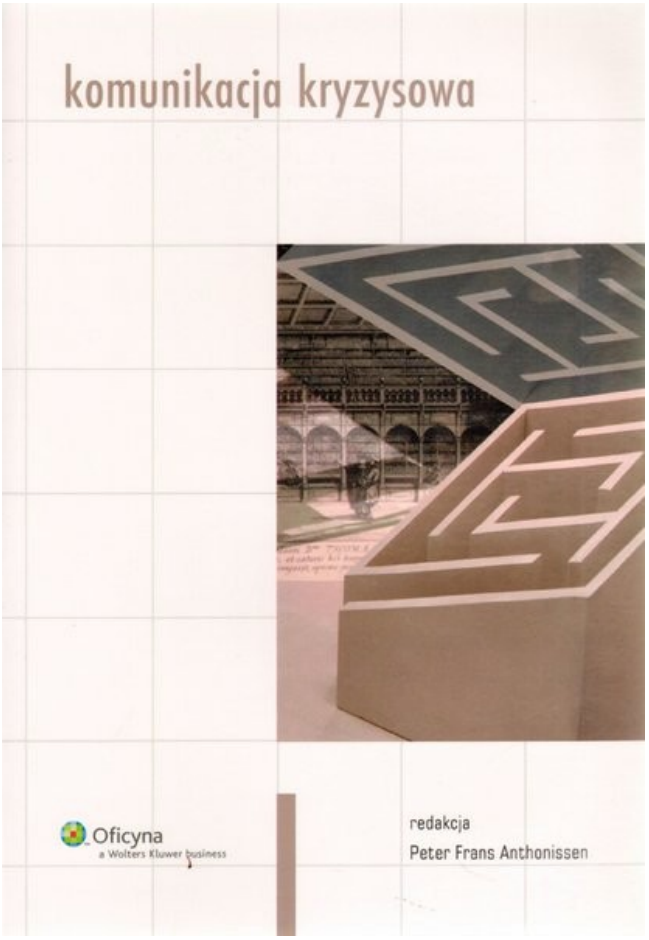
Transport lotniczy jest generalnie uznawany za bezpieczny, do wypadków dochodzi rzadko, biorąc pod uwagę ogólną ilość przelotów. Gdy już jednak dochodzi do katastrofy samolotu, liczba ofiar śmiertelnych często liczona jest w dziesiątkach a nawet setkach. Są to więc jedne z najbardziej medialnych oraz masowych tragedii, mocno działające na emocje. Do takiej katastrofy doszło 31 stycznia 2000 roku u wybrzeży Kalifornii. Samolot linii Alaska Airlines lecący z Puerto Vallarta (Meksyk) do Seattle (USA) rozbił się niespełna dwie godziny po starcie, nurkując z dużej wysokości prosto w wody Oceanu Spokojnego. Na miejscu zginęli wszyscy pasażerowie i członkowie załogi, łącznie 88 osób.

Kierownictwo amerykańskich linii lotniczych natychmiast po pierwszych informacjach o tragedii wystosowało oficjalne komunikaty prasowe[4], tłumacząc je dodatkowo na hiszpański, gdyż sporą część ofiar stanowili obywatele Meksyku. W kontakcie z prasą starano się być cały czas, udzielając szerokich odpowiedzi oraz informacji zarówno w języku angielskim jak i hiszpańskim. Odpowiadano otwarcie na pytania dziennikarzy. Pokazano, że firma nie boi się odpowiedzialności za wypadek, współpracuje z mediami oraz wspomaga dochodzenie śledcze wszczęte przez organy państwowe. Przygotowano się na wiele możliwych pytań: zgromadzono wiele informacji na temat przedsiębiorstwa oraz dotychczasowej polityki bezpieczeństwa, ukazując dotychczasowe loty jako bezpieczne. Na lotnisko w Meksyku skąd wystartował samolot bardzo szybko wysłano przedstawiciela, który udzielał po hiszpańsku wielu wywiadów i był ciągle dostępny dla mediów. Linie lotnicze pokazywały, że także one są w żałobie – wraz z pasażerami zginęli pracownicy firmy. Stworzono grupy ochotników mające zająć się pomocą dla rodzin ofiar. W prasie właściwie brak było sensacyjnych artykułów, gdyż dziennikarze otrzymywali wprost od głównych stron kryzysu najważniejsze i rzetelne informacje. Pomimo, że katastrofa przez pewien czas była głównym tematem w mediach i śledztwo wykazało winę Alaska Airlines (do usterki technicznej doszło przez zaniedbania), linie te nie utraciły swojego wizerunku oraz reputacji. Nadal działają w Meksyku[5]. Klienci nie kojarzą podróżowania nimi z niebezpieczeństwem.

Zaplanowanie komunikacji kryzysowej

Właściwe przygotowanie do sytuacji kryzysowej obejmuje również sporządzenie planu komunikacji. Zdarzenia nieprzewidziane i groźne w skutkach prowadzą do chaosu, wywołują deficyt informacji, które zaczynają być nagle niezwykle pożądane[6]. Jednak co będzie pisane w prasie i przedstawiane publicznie, nie

Biuletyn poleca:



Komunikacja kryzysowa
Peter Frans Anthonissen (red.)
Warszawa 2010. ss. 232.

może wynikać z przypadku, bez próby dostosowania komunikatu i przewidywania jego następstw. Plan komunikacji kryzysowej powinien w skrócie sprowadzać się do takich elementów jak: określenie tego jaka będzie treść wiadomości, do kogo ma ona trafić oraz kto i kiedy ma ją dostarczyć[7]. Przekazywane wiadomości powinny[8] być dla dziennikarzy wiarygodne, dostosowane do „gatunku" publikacji (inne np. dla dzienników o bieżących wydarzeniach, a inne dla np. programów ekonomicznych). Muszą być pozbawione dwuznaczności i dostatecznie proste, co powinno nie dopuścić do wypaczeń treści. Autorzy opracowania „Komunikacja kryzysowa" radzą wręcz, że zamiast twierdzeń w stylu „Nasza organizacja ma najlepsze standardy bezpieczeństwa", lepiej przedstawić jest jakie certyfikaty i dopuszczenia się otrzymało, jakie kontrole i jak często miały miejsce, oraz jak wiele pieniędzy i pracowników firma zainwestowała w przestrzeganie bezpieczeństwa[9]. Będzie to o wiele bardziej przekonujące niż suche ogólnikowe stwierdzenia.

Zespołowa komunikacja kryzysowa

Jest ważne, aby instytucja mówiła publicznie jednym głosem, i wszyscy stali w niej po jednej stronie[10]. Role w zespole niech będą odpowiednio rozdysponowane[11]. Minimalne wymaganie to rzecznik, który dobrze, aby posiadał zastępcę. To w jego rękach spoczywa komunikacja kryzysowa i musi to być jasne dla wszystkich uczestniczących w niej stron. Dla mediów instytucja odpowiedzialna za sytuację kryzysową ma stać się pierwszym i najważniejszym wiarygodnym źródłem, najlepiej jedynym. Nie można także dopuścić, aby przedstawiciele samej organizacji udzielali nieautoryzowanych wywiadów lub wypowiedzi bez naszej zgody i wiedzy. Może to sprzyjać powstawaniu plotek i niedomówień. O naszych oświadczeniach informujmy naszą organizację, aby wszyscy w niej wiedzieli jakie oficjalne informacje krążą w mediach. Możemy też rozważyć krótkie konsultacje z innymi przed publikowaniem wiadomości. Powinniśmy jednocześnie szanować pracę dziennikarzy i uwzględniać jej uwarunkowania w naszej pracy – w końcu to my jesteśmy łącznikiem pomiędzy nimi a instytucją[12]. Jeśli spodziewamy się, że oprócz nas również przedstawiciele instytucji będą kontaktowani z prasą, przeszkolmy[13] ich do tego choćby w minimalnym stopniu. Niech każdy ich kontakt z prasą zostanie zapisany przez rozmówcę: dane kontaktowe gazety i dziennikarza (z numerami telefonów), zadane pytania i udzielone odpowiedzi. Informacja taka powinna następnie trafić do osoby odpowiedzialnej za komunikację (np. rzecznika). Dla dziennikarzy pozostańmy dostępni cały czas, obiecując im kontakt gdy uzyskamy nowe informacje i możemy udzielić odpowiedzi na wcześniej postawione pytania. Trzeba też uwzględniać harmonogram pracy oraz obowiązujące w mediach terminy. Wiadomości trafić muszą na czas, aby zdążyły się ukazać przed zamknięciem np. gazety czy programu telewizyjnego.

Wypełnienie deficytu informacji

Sytuacje kryzysowe charakteryzując się deficytem informacji, są jednocześnie często sensacyjne dla mediów oraz ich odbiorców. Dziennikarze nie otrzymawszy wystarczających wiadomości „u źródła", mogą udać się po nie do innych miejsc, przedstawiając już fakty nieautoryzowane, nie zawsze zgodne z prawdą lub kompletne. W. Macierzyński w publikacji „Rola mediów w komunikacji kryzysowej" wymienia[14] szereg cech pracy dziennikarzy z jakimi należy się liczyć: przedstawiają oni zdarzenia z punktu widzenia ofiary, muszą zebrać jak najwięcej kluczowych dla wydawcy wiadomości w jak najkrótszym czasie, jednocześnie relacje dla szerokiej publiczności zmuszają do uproszczeń językowych. Poszukiwania tego co przykuwa uwagę i jest w jakiś sposób nowością czy sensacją. Kluczem będzie pokierowanie tak mediami, aby zamiast pogorszania sytuacji pełniły one rolę pozytywną, informacyjną, będąc pośrednikiem pomiędzy instytucją zarządzającą w sytuacji kryzysowej, a ewentualnie zagrożoną ludnością. Oprócz fizycznego kontrolowania sytuacji kryzysowej (np. poprzez prowadzenie akcji ratowniczych) trzeba jeszcze panować nad obiegiem informacji i tym co trafia do opinii publicznej. W tym celu osoba odpowia-

Przykłady oficjalnego oświadczenia dla prasy

„Wczoraj z powodu spraw technicznych związanych z samolotem, Wizz Air nie mógł wykonać wieczornego lotu z Luton do Katowic zgodnie z rozkładem. Priorytetem Wizz Air jest bezpieczeństwo swoich pasażerów dlatego dopóki nie zakończono przeglądu samolotu i w 100% nie był gotowy do lotu, linia musiała odwołać przelot. Pasażerami zajęto się i ci, którzy nie mieli noclegu, został im nocleg zaoferowany. Zostali oni również przebukowani na inne loty w zależności od dostępności.

Wizz Air przeprasza za wszelkie niedogodności. Bezpieczeństwo pasażerów jest priorytetem linii i aby zminimalizować ryzyko techniczne, Wizz Air korzysta z floty młodych samolotów typu Airbus A320, których przeglądu dokonuje Lufthansa Technik, jedna z wiodących światowych firm prowadzących obsługę techniczną. Niezawodność techniczna Wizz Air wynosi 99,7%, co stanowi jeden z najwyższych wskaźników na świecie i jest dużo wyższy od wskaźników naszej konkurencji."

Oświadczenie firmy Wizz Air w sprawie odwołanego lotu z Londynu do Katowic, opublikowane za pośrednictwem Actia Forum Sp. z o.o. Zwraca uwagę przykładanie troski do ukazania firmy jako dbającej o bezpieczeństwo pasażerów.
Źródło online: http://www.pasazer.com/in-1256-przewoznik,przeprasza,za,luton.php

„10 maja tego roku, Suchoj Superjet 100 (97004) został znaleziony przez indonezyjskie grupy ratownicze na zboczu góry Salak na wysokości 1700 metrów. Samolot, który wykonywał lot demonstracyjny z lotniska Halima Perdanakusuma w Dżakarcie, zniknął z ekranów radarów 9 maja. Na pokładzie maszyny znajdowało się 45 osób.

W imieniu zarządzających JSC United Aircraft Corporation, JSC Sukhoi Company, JSC Sukhoi Civil Aircraf oraz całego personelu firmy wyrażamy nasze najgłębsze i najbardziej szczere kondolencje dla rodzin i bliskich pasażerów oraz członków załogi, którzy byli na pokładzie tej maszyny."

Oświadczenie prasowe firmy Suchoj, w sprawie katastrofy samolotu SSJ100.
Źródło online: http://www.pasazer.com/in-10405-oficjalne,oswiadczenie,suchoja.php

Komunikacja kryzysowa – dobre i złe ruchy

Tak:

- Posiadać kontakty z prasą już przed zdarzeniem kryzysowym, mieć zaprzyjaźnionych dziennikarzy, mieć przygotowane oficjalne informacje dla mediów nt. samej organizacji (np. wirtualne biuro prasowe).
- Gdy do zdarzenia doszło, wyjść jako pierwszy z oficjalnymi o nim informacjami, nawet jeśli wiadomości są złe i niepokojące.
- Dobro ludzi, ich życie oraz zdrowie jest ważniejsze niż sprawy materialne, pamiętać o tym w wypowiedziach.
- Jeśli zdarzenie wymaga śledztwa ze strony odpowiednich organów, poinformować o gotowości do pełnej z nimi współpracy.
- Powiadomić o rozpoczęciu wewnętrznego dochodzenia w celu wyjaśnienia zdarzenia.
- Dostosować się do godzin działania dziennikarzy oraz terminów prasowych, a terminów dotrzymywać.
- Monitorować sytuację i zbierać kolejne dane, dzielić je na pewne, niepewne oraz niewiadome.

Nie:

- Nie koncentrować się na szczegółach wydarzenia, lecz na działaniach które się podejmuje.
- Nie kłamać, nie tuszować na siłę faktów.
- Nie mogąc udzielić informacji, wyjaśnić dlaczego.
- Nie składać obietnic, których nie można dotrzymać.
- Nie wypowiadać się nieoficjalnie.
- Nie łamać prywatności innych osób, świadków, ofiar, pracowników.
- Nie używać stwierdzeń przesadnie emocjonalnych, nie wdawać się w dyskusje, które są prowokacyjne.
- Nie bagatelizować na siłę zdarzenia, ale i go nie wyolbrzymiać.
- Nie szacować i nie spekulować. Szczególnie ostrożnie posługiwać się liczbami i kosztami. Unikać domysłów.
- Nie faworyzować określonych gazet czy dziennikarzy. Traktować wszystkich równo.
- Nie obwiniać innych, ale i nie przyjmować przesadnie winy na siebie dopóki nie udowodni to śledztwo.

dająca za komunikację kryzysową musi na miejscu zdarzenia zachowywać sie sama jak dziennikarz[15].

Rzecznik zbiera wszelkie możliwe fakty, przeprowadza „wywiady" wśród przedstawicieli organizacji i dowiaduje się co, gdzie, kiedy oraz jak i dlaczego. Z takiej bazy danych faktów o instytucji oraz sytuacji kryzysowej powstaje zasób wiedzy, który posłuży do odpowiadania mediom na ich pytania.

Postawa rzecznika w komunikacji kryzysowej

Gromadząc ciągle fakty o sytuacji kryzysowej i komunikując się z mediami, musimy unikać wszelakich spekulacji oraz kroków nierozważnych[16]. Nie wyceniajmy szkód nie znając ich rzetelnej oceny i ostatecznych rozmiarów, pozostawiając posługiwanie się liczbami na później. Nie kierujmy oskarżeń zarówno do innych, jak i nie obwiniajmy instytucji, którą reprezentujemy. Miejmy na uwadze dobro prywatne innych osób, gdy mówimy coś na ich temat oraz ich udziale w zdarzeniu. Jeśli bliscy ofiar nie zostali jeszcze powiadomieni o ich śmierci, nigdy nie podawajmy personaliów. Generalnie należy pokazywać, że dobro ludzi jest ważniejsze niż wszelkie inne dobra, np. materialne. Najgorszą przy tym publiczną odpowiedzią jest „brak komentarza"[17]. Jeśli czegoś powiedzieć nie możemy, poinformujmy dlaczego i kto oraz kiedy może za nas takiej odpowiedzi udzielić. Gdy pierwsze informacje o zdarzeniu już do nas dotarły, należy wystosować oficjalne oświadczenie do prasy. Powinno ono zawierać fakty (gdzie i kiedy do tego doszło, jakie są skutki, ofiary) oraz informacje o podjętych działaniach (np. śledztwie) i zapewnienie o dalszym powiadamianiu w miarę rozwoju sytuacji i wskazanie osoby odpowiedzialnej za to[18]. Nie ukrywajmy czegoś, czego ukryć się nie da. Wszystko prędzej czy później wyjdzie na jaw. Pamiętajmy przy tym, że niektóre z informacji przedwcześnie ujawnione mogą doprowadzić do niepotrzebnej paniki, co trzeba rozważać. Zapewnienie o współczuciu dla poszkodowanych i ich bliskich będzie bardzo ważne, lecz emocji nie demonstrujmy niepotrzebnie. Zwłaszcza żalu czy strachu przed kamerami. Jeśli nasza instytucja jest odpowiedzialna za reagowanie w sytuacji kryzysowej, może to odebrać innym pewność siebie. Naszym zadaniem oprócz informowania ludności jest również wywieranie pozytywnego wpływu. Zatem warto skupiać się na przekazywaniu wiadomości podbudowujących: opisywanie aktów heroizmu, zaangażowania uczestników a także okazywanie troski i zainteresowania. Traktujmy wszystkie zainteresowane sytuacją media sprawiedliwie i obiektywnie, nie faworyzując żadnego z nich w dostępie do informacji. Członków własnego zespołu, którzy nam pomagają, otwarcie doceniajmy[19].

Komunikacja kryzysowa przy zdarzeniach o charakterze terrorystycznym

Rozważając strategię komunikacji kryzysowej z punktu widzenia organizacji dotkniętej zdarzeniem o charakterze terrorystycznym należałoby poczynić kilka uzupełnień. W krajach europejskich zamachy przyciągają o wiele większą uwagę mediów i opinii publicznej, niż zamachy w krajach np. muzułmańskich. Miesięcznie w Pakistanie czy Iraku dochodzi do co najmniej kilkudziesięciu zdarzeń o charakterze terrorystycznym. W tym czasie do najwyżej kilku w całej Europie. W krajach „przyzwyczajonych" do terroryzmu zdarzenia mogące doczekać się co najwyżej krótkiej wzmianki prasowej, zdominowałyby na wiele dni czołówki gazet europejskich. Wynika to poniekąd z wrażliwości społeczeństwa poprzez jego sposób życia i odczuwanie terroryzmu jako zagrożenia. W Europie jest nieporównywalnie większy udział mediów w życiu społecznym i odmiennego niż w Pakistanie czy Iraku „przyzwyczajenia" do spokoju. Jeśli więc sytuację kryzysową określamy mianem „medialnej", to w krajach zachodnich zamach terrorystyczny w skali medialności osiąga bardzo wysoki, jeżeli nie najwyższy poziom.

Zdarzenie wykracza poza zainteresowanie tylko lokalne, przykuwa uwagę całych krajowych i mediów mediów. Do wypowiadania się na jego temat zapraszani są eksperci i autorytety z różnych dziedzin: socjologowie, politolodzy, kulturoznawcy. Nie możemy

zakładać, że sam komunikat prasowy i dostępność rzecznika pozwoli zapełnić początkową próżnię informacyjną, ten ogromny deficyt wiadomości, który tak „sensacyjne" zdarzenie wytwarza. Klęska żywiołowa dotyka zazwyczaj gminę, powiat, najwyżej województwo lecz zawsze określony wycinek kraju, a czołowymi dla mediów postaciami są władze lokalne, ewentualnie poszkodowaną ludność. Zamach terrorystyczny w zasadzie uderza w całe państwo. Bez znaczenia jest konkretne miejsce jego dokonania. To państwo jako organizm staje się ofiarą zamachu, choćby zdarzył się on w prywatnym miejscu rozrywki (kino, koncert, impreza sportowa, centrum handlowe) czy był dokonany na obiekty państwowe i władzy publicznej (koszary, posterunki, urzędy). Na celowniku pytań pojawiają się osoby z najwyższych władz, premier, ministrowie, szefowie najważniejszych służb oraz ich analitycy. Niektóre z informacji mogą być początkowo celowo nie dopuszczane do opinii publicznej, ze względu na prowadzone śledztwo. Co więcej, już nawet samo podejrzenie zamachu wzbudza w społeczeństwie duże emocje. Nawet jeśli informacje o zamachu okażą się po pewnym czasie fałszywe, a do np. wybuchu doszło w wyniku awarii, wiadomości o zdarzeniu mogą być niedobre dla właściwego funkcjonowania społeczeństwa. Łatwo o zachowania paniczne, masowe rezygnacje z przebywania w określonych miejscach (szczególnie na koncertach, imprezach sportowych, wyjazdy turystyczne). Dojść może do chuligańskich ataków odwetowych na społeczności obwiniane o dokonanie aktu terrorystycznego. Szczególnie groźna może okazać się plotka, pogłoska, rozpowszechniająca się w sposób nie do przewidzenia, a której zneutralizowanie może wymagać bardzo wiele wysiłku.

Kontrola zachowania mediów i opinii publicznej przez organizację dotkniętą zamachem jest zatem bardzo trudna, jeśli w ogóle możliwa. Sytuacja wykracza poza siły jednego lokalnego rzecznika. Nie oznacza to jednak wcale, że jego rola jest wtedy nieważna. Rzecznik organizacji mógłby pozostawać w ścisłym kontakcie ze służbami państwa wyjaśniającymi przyczyny zamachu. Konsultując się z nimi w sprawie określenia tego, co można i należy przedstawiać mediom w odpowiedzi na ich pytania. Należałoby dotrzeć do załogi instytucji w celu jak najszerszego ograniczenia ryzyka wydostania się informacji niesprawdzonej, pogłoski, która mogłaby np. wskazywać na rzekomego sprawcę i jego pochodzenie etniczne. Taka informacja może wywołać zamieszki i ataki w stronę określonych mniejszości narodowych. Instytucja może znaleźć się w bardzo złym świetle w oczach opinii publicznej, gdyby została uznana za źródło fałszywej i destrukcyjnej w następstwach plotki.

Tobiasz Małysa

Przypisy

1 Zob. Komunikacja kryzysowa, red. P. Frans-Anthonissen. Warszawa 2010, s. 125-129.
2 Por. tamże, s. 125-129.
3 A. Dumont, D. Abemathy. When the sky falls: Advance planning key to crisis communications. Rural Cooperatives. Sep/Oct2005, Vol. 72 Issue 5, p27, s. 28.
4 Por. Komunikacja kryzysowa... op. cit., s. 77 - 82.
5 Por. tamże, s. 77 - 82.
6 Zob. W. Macierzyński, Rola mediów w komunikacji kryzysowej [w:] Zarządzanie kryzysowe w Polsce, (red. M. Jabłonowski, L. Smolak) Pułtusk 2007, s. 385.
7 Por. Komunikacja kryzysowa... op. cit., s. 46.
8 Por. tamże, s. 147.
9 Tamże, s. 215.
10 Zob. R. Girt. How do you handle crisis communications. Wyoming Business Report, September 2011, s. 4-5. Źródło online: [http://www.wyomingbusinessreport.com/article.asp?id=59679], dostęp: 2012-05-06.
11 Komunikacja kryzysowa, op. cit., s. 47-51.
12 Por. R. Girt. How do you handle crisis communications... op. cit..
13 Zob. W. Macierzyński, Rola mediów w komunikacji kryzysowej... op. cit., s. 394-397.
14 Tamże, s. 392.
15 Por. . A. Dumont, D. Abemathy. When the sky falls... op. cit., s. 28.
16 Zob. J. A. Ressle. Crisis Communications. Public Relations Quarterly, 2001, s. 10.
17 Zob. R. Girt. How do you handle crisis communications... op. cit.
18 Por. Komunikacja kryzysowa... op. cit., s. 59.
19 Por. J. A. Ressle. Crisis Communications... op. cit., s. 10.

Znaczenie Rosji dla walki z terroryzmem międzynarodowym Regionalna Struktura Antyterrorystyczna Szanghajskiej Organizacji Współpracy

Stosunki pomiędzy Chińską Republiką Ludową i Związkiem Socjalistycznych Republik Radzieckich zostały unormowane w 1989 roku. Ich spokojny rozwój spowodowany był pragmatycznym podejściem obydwu stron do wzajemnych stosunków, uprzedzeń i zaszłości historyczno – politycznych[1].

Chiny i Federacja Rosyjska zaktywizowały swoją współpracę nie tylko z powodów gospodarczych, lecz również politycznych. Jedną z politycznych przyczyn zbliżenia pomiędzy obydwoma krajami była gwałtownie rosnąca ofensywa islamskiego fundamentalizmu na terenie Azji Centralnej[2]. Dodatkowo zagrożenie zwiększa silnie rozwinięta przestępczość transgraniczna, handel i przemyt narkotyków. W wyniku rozwoju współpracy chińsko – rosyjskiej podczas wizyty Borysa Jelcyna w Chinach (24-26.04.1996 r.) doszło do podpisania układu w sprawie środków zaufania militarnego wzdłuż byłej granicy radziecko – chińskiej. Zawarty układ[3] miał charakter wielostronny, gdyż przyłączyły się do niego Kazachstan, Kirgizja i Tadżykistan (tzw. Piątka Szanghajska).

Powyższe porozumienie zostało uzupełnione podpisaną w Moskwie rok później umową o redukcji sił zbrojnych w rejonie wspólnych granic. W dokumencie tym zapisane zostało zobowiązanie się stron umowy do niestosowania siły lub groźby jej użycia wobec sygnatariuszy układu. Zgodne współdziałanie Rosji i Chin doprowadziło do powstania w czasie spotkania na szczycie w Szanghaju w dniach 14 do 15 czerwca 2001 Szanghajskiej Organizacji Współpracy. W trakcie tego spotkania do wcześniej wymienianej piątki uczestników porozumień dołączył Uzbekistan. Nastąpiło zinstytucjonalizowanie współpracy pomiędzy sygnatariuszami układu. Działanie mające na celu powołanie nowej regionalnej struktury politycznej było wyrazem zaniepokojenia Rosji zwiększaniem się wpływów fundamentalizmu muzułmańskiego w rejonie środkowoazjatyckim. Kraje powstałe na gruzach republik radzieckich nie są w stanie zapewnić sobie samodzielnie bezpieczeństwa, uchronić się przed zagrożeniami terrorystyczno – ekstremistycznymi. Chociażby widać to było podczas kryzysów związanych z zamachami w Taszkencie (luty 1999 r.) oraz wtargnięciem uzbeckich islamistów, którzy przekraczając granicę tadżycko – kirgiską chcieli tranzytem dostać się na terytorium Uzbekistanu. Wyparci przez wojska rządowe wycofali[4] się na tereny kontrolowane przez opozycję tadżycką. Rosja doskonale oceniła sytuację w Dolinie Fergańskiej i unikając bezpośredniego wsparcia militarnego udzieliła efektywnej pomocy uczestnikom tego kryzysu. We wrześniu 1999 roku podczas obrad Rady Ministrów Obrony WNP w której uczestniczyli przedstawiciele Rosji, Kirgistanu, Tadżykistanu, Kazachstanu, Armenii, Białorusi i Uzbekistanu powołana została koalicja antyterrorystyczna[5].

Przybierające na sile zagrożenie ze strony terroryzmu i ekstremizmu spowodowało, że jednym z tematów posiedzenia Piątki Szanghajskiej w czerwcu 2001 roku była problematyka przeciwdziałania terroryzmowi, separatyzmowi i ekstremizmowi religijnemu[6]. 15 czerwca 2001 roku ogłoszono deklarację o powstaniu Szanghajskiej Organizacji Współpracy. W tym samym dniu przedstawiono Szanghajską Konwencję[7] o Walce z Terroryzmem, Separatyzmem i Ekstremizmem (Шанхайская конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом)[8].

To liczący 21 artykułów i załącznik dokument. Umawiające się strony uznały, że terroryzm, separatyzm i ekstremizm zagrażają terytorialnej integralności i ich bezpieczeństwu narodowemu. Dotyczy to ich stabilności politycznej, ekonomicznej i socjalnej. Strony

konwencji uznały, iż współpraca w ramach podpisanej konwencji będzie najbardziej efektywną formą walki z terroryzmem, separatyzmem i ekstremizmem. W pierwszym artykule na potrzeby konwencji zdefiniowane zostały terminy: terroryzm. separatyzm i ekstremizm.

Artykuł drugi reguluje obowiązki stron konwencji w zakresie uprzedzania, przerywania działań, które zostały zdefiniowane w poprzednim artykule. Przestępstwa opisane w pierwszym artykule pociągają za sobą wydanie ich realizatorów stronie zainteresowanej. Realizacja niniejszej konwencji związana z wydaniem i pomocą prawną, odbywa się w ramach i w zgodzie z międzynarodowymi porozumieniami oraz wewnętrznymi uregulowaniami prawnymi stron umowy. Trzeci artykuł zobowiązuje strony do podjęcia działań w sferze prawa wewnętrznego, które nie pozwolą na usprawiedliwianie przedstawionych w pierwszym artykule działań, ze względu na ich polityczny, ideologiczny, rasowy czy np. etniczny charakter. Czyny te muszą za sobą pociągać karę zgodnie ze stopniem ciężaru przestępstwa. Kolejny, czwarty ustala sposób postępowania po wypełnieniu wewnętrznych procedur, których celem jest wejście w życie konwencji. Obowiązkiem każdej ze stron w takiej sytuacji jest powiadomienie, za pośrednictwem depozytariusza konwencji, o liście kompetentnych organów państwowych zobowiązanych do wypełniania postanowień konwencji. Strony konwencji po wzajemnej akceptacji mogą prowadzić konsultacje, wymieniać się poglądami, uzgadniać stanowiska związane z działaniami zdefiniowanymi w jej artykule pierwszym. Kolejny artykuł w swoich dziesięciu punktach przedstawia sposób i drogę współpracy pomiędzy kompetentnymi organami państw SOW w walce z terroryzmem, ekstremizmem i separatyzmem. Zaliczamy do nich wymianę informacji, wypełnianie zapytań związanych z prowadzonymi przedsięwzięciami operacyjno – śledczymi, opracowywanie i przyjęcie wspólnych przedsięwzięć dla uprzedzenia, ujawnienia i przerwania działalności opisanej w punkcie 1 pierwszego artykułu konwencji oraz wzajemnego informowania się o rezultatach podjętych działań. Punkt czwarty artykułu mówi o podejmowaniu przeciwdziałania aktom terroru skierowanym przeciwko pozostałym państwom konwencji. W następnym punkcie charakteryzowanego artykułu zapisane zostało zobowiązanie do podejmowania niezbędnych przedsięwzięć dla uprzedzania, ujawniania i przeciwdziałania finansowaniu, dostawom uzbrojenia i sprzętu bojowego oraz okazywania pomocy osobom lub organizacjom dla realizacji zapisów artykułu pierwszego konwencji. Szósty punkt analizowanego artykułu zobowiązuje strony do podejmowania przedsięwzięć służących uprzedzaniu, ujawnianiu, przerywaniu, zakazaniu i przerwaniu działalności lub przygotowaniom osób w celu realizacji punktu 1, artykułu 1 konwencji. Kolejne punkty (7 i 8) regulują obowiązek wymiany obowiązującymi aktami prawnymi i materiałami związanymi z ich stosowaniem oraz wymianę doświadczeń z zakresu zwalczania terroryzmu, separatyzmu i ekstremizmu. Ostatnie dwa punkty opisywanego artykułu omawiają współpracę w dziedzinie przygotowania, edukowania i podwyższania kwalifikacji swoich specjalistów w wielorakich formach. Mówią o osiąganiu przy współpracy stron konwencji porozumiewania się w sprawie innych form współpracy, włączając w to okazywanie praktycznej pomocy dla położenia kresu działalności terrorystycznej, ekstremistycznej i separatystycznej oraz likwidacji jej następstw. Takie porozumienia w myśl konwencji są naturalnymi i regulowanymi odpowiednimi protokołami. Centralne państwowe organa stron konwencji wymieniają się informacjami[9], służącym ich interesom, w tym w szczególności o: przygotowywanych i popełnianych działaniach (terroryzm, ekstremizm, separatyzm), ujawnionych i przerwanych próbach ich realizacji; przygotowaniu w celu dokonania działań (art. 1, pkt. 1 konwencji) skierowanych przeciwko głowom państw, innym państwowym działaczom, pracownikom przedstawicielstw dyplomatycznych, konsulatów, organizacji międzynarodowych, innych osób mających międzynarodową ochronę, uczestników wizyt międzypaństwowych, politycznych, sportowych i innych; organizacjach, grupach i osobach przygotowujących lub dokonujących czynów związanych terroryzmem, ekstremizmem, separatyzmem oraz w inny sposób

uczestniczących w tych działaniach, biorąc od uwagę cele, zadania, związki czy inne informacje; nielegalnym przygotowywaniu, nabywaniu, przetrzymywaniu, sprzedaży, przemieszczaniu przekazywaniu i posługiwaniu się silnymi truciznami, środkami wybuchowymi, materiałami radioaktywnymi, uzbrojeniem, urządzeniami wybuchowymi, uzbrojeniem strzeleckim, amunicją, jądrowymi, chemicznymi, biologicznymi i innymi rodzajami broni masowego rażenia oraz materiałami mogącymi mieć zastosowanie w działalności opisanej w art. 1 pkt. 1 konwencji; ujawnionych lub przypuszczalnych źródłach finansowania terroryzmu, ekstremizmu i separatyzmu; formach, środkach i metodach działalności terrorystycznej.

Następujące po sobie kolejne artykuły 8 i 9 szczegółowo reglamentują współpracę centralnych organów państw stron uczestników konwencji w zakresie wymiany informacji, sposobów ich przekazywania, pisemnych form potwierdzenia przekazanych informacji, ustalania stopnia ich tajności, języka w którym jest przekazywany[10], odmowy przekazania informacji i innych problemów związanych z ich realizacją. Artykuł 10 konwencji zobowiązuje jej strony do podpisania oddzielnego porozumienia oraz pozostałych niezbędnych dokumentów w celu powołania i zabezpieczenia funkcjonowania regionalnej struktury antyterrorystycznej w Biszkeku celem prowadzenia efektywnej walki z terroryzmem, ekstremizmem i separatyzmem. Następujące po sobie kolejno trzy artykuły[11] określają techniczne warunki współpracy państw stron konwencji. Pomoc i współpracę w zakresie materialnej i technicznej pomocy, przekazywanie środków, wyposażenia i techniki niezbędnej dla realizacji umowy. Zezwalają na podpisywanie, przez centralne organa państwowe realizujące konwencję, wspólnych porozumień, regulujących szczegóły wypełniania zobowiązań wynikających z układu. Ostatni z omawianych trzech artykułów określa sposoby postępowania z informacjami o charakterze niejawnym otrzymanymi od stron konwencji, których stopień utajnienia określany jest przez stronę przekazująca informację. Czternasty artykuł stanowi o sposobach ponoszenia kosztów realizacji konwencji. Pozostałe artykuły konwencji dopuszczają i nie ograniczają uczestnictwa państw jej stron w innych porozumieniach międzynarodowych, w dziedzinie nią objętej. Wskazują depozytariusza umowy[12], którym jest Chińska Republika Ludowa, ustalają czas jej wejścia w życie. Kolejny, dziewiętnasty artykuł reguluje możliwość przyłączania się do konwencji innych zainteresowanych państw. Artykuł dwudziesty określa dopuszczalność i sposób wnoszenia zmian do tekstu konwencji oraz reguluje technikę wyjścia państwa strony z konwencji. Ostatni 21 artykuł konwencji reguluje i opisuje postępowanie związane z załącznikiem do niej.

Załącznik do Szanghajskiej Konwencji o Walce z Terroryzmem, Separatyzmem i Ekstremizmem jest spisem międzynarodowych konwencji i protokołów, w liczbie 10, regulujących stosunki międzynarodowe w zakresie objętym uregulowaniami konwencji szanghajskiej. W momencie przekazywania powiadomienia o wypełnieniu wewnątrzpaństwowych procedur wymaganych do wejścia w życie Konwencji Szanghajskiej, przekazywana jest również informacja o uczestnictwie, bądź nie, w wymienionych powyżej konwencjach i protokołach. Załącznik Konwencji Szanghajskiej może być rozszerzany o umowy spełniające następujące kryteria: otwartość na uczestnictwo wszystkich państw, wszedł życie, był ratyfikowany, przyjęty lub zatwierdzony, do którego przyłączyły się co najmniej trzy państwa SOW. Przedstawiona powyżej konwencja jest międzynarodowym porozumieniem, które jest kolejnym krokiem w zacieśnianiu współpracy międzynarodowej w zakresie zwalczania niezwykle groźnych zjawisk dla pokoju, bezpieczeństwa narodowego i międzynarodowego, takich jak terroryzm, ekstremizm i separatyzm.

Działaniami Szanghajskiej Organizacji Współpracy zainteresowane obecnie są inne państwa m in.: Mongolia, Pakistan, Iran, Afganistan oraz Indie.

Podczas kolejnego szczytu Szanghajskiej Organizacji Współpracy[13] przyjęte zostały postanowienia do których należą m in.: deklaracja szefów państw SOW, postanowienie o zatwierdzeniu Koncepcji współpracy państw członków Szanghajskiej Organizacji Współpracy w Walce z Terroryzmem, Separatyzmem Ekstremi-

zmem, postanowienie o zatwierdzeniu decyzji w sprawie ustalenia stałych przedstawicieli członków SOW przy Regionalnej Strukturze Antyterrorystycznej oraz zatwierdzenie sprawozdania Rady Regionalnej Struktury Antyterrorystycznej.

Innym ważnym dokumentem jest Koncepcja Współpracy Państw – Członków Szanghajskiej Organizacji Współpracy w Walce z Terroryzmem, Separatyzmem i Ekstremizmem (Концепция сотрудничества государств – членов Шанхайской организации сотрудничества в борбье с террлризмом, сепаратизмом и экстремизмом)[14]. W jej pięciu częściach; Ogólne regulacje, Podstawowe cele, zadania i zasady współpracy, Podstawowe kierunki współpracy, Podstawowe formy współpracy i Mechanizm realizacji koncepcji ustalone zostały metody działania, system współpracy jej formy oraz mechanizmy użytkowane w realizacji zadań wynikających z koncepcji i konwencji z 2001 roku. Najbardziej istotne są trzy ostatnie części koncepcji, które systematyzują praktyczną współpracę państw SOW. Podstawowe kierunki współpracy zostały ujęte w dwadzieścia dwa tematy (problemy). Należą do nich m. in.: 1. formowanie wspólnej polityki państw członków SOW w sferze walki z terroryzmem, separatyzmem i ekstremizmem wraz z urzeczywistnianiem międzynarodowej współpracy w tym zakresie, 2. opracowanie wspólnego podejścia do zwalczania działalności terrorystycznych, separatystycznych i ekstremistycznych organizacji na terytoriach państw SOW, 3. stworzenie wspólnej listy takich organizacji, likwidacji ich majątku oraz środków finansowych, 4. rozwijanie i korzystanie z antyterrorystycznego potencjału państw stron koncepcji, 5. zapewnienie nieuchronności kar za działalność terrorystyczną, ekstremistyczną i separatystyczną, 6. stworzenie i wprowadzenie w życie wspólnego rejestru (listy poszukiwanych) osób ogłoszonych w międzynarodowej liście podejrzewanych o przestępstwa o charakterze terrorystycznym, 7 doskonalenie prawnych podstaw współpracy w walce z przedstawianymi tutaj zjawiskami, 8. opracowanie i wdrożenie międzypaństwowego systemu przedsięwzięć dla walki z terroryzmem, ekstremizmem i separatyzmem. Niezwykle ważnym elementem współpracy jest opracowanie prawnych, organizacyjnych oraz innych przedsięwzięć skierowanych na wzmocnienie kontroli granicznej i celnej. Celem jest zapobieganie przenikaniu terrorystów na terytoria państw SOW oraz przemieszczania przez ich granice środków służących terroryzmowi. Strony koncepcji zajmują się współpracą na polu naukowo - technicznym, informacyjnym i analitycznym, mającą na celu zabezpieczenie walki z terroryzmem, separatyzmem i ekstremizmem. Omawiana koncepcja zobowiązuje do pomocy w likwidacji skutków działań oraz rehabilitacji osób, które ucierpiały z powodu działalności terrorystycznej lub ekstremistycznej. Współdziałające strony nie dopuszczą terrorystów do broni masowego rażenia, środków ich przenoszenia, materiałów radioaktywnych, toksycznych oraz technologii ich produkcji. Koncepcja przewiduje współpracę mającą na celu przeciwdziałanie wszelkim możliwym sposobom finansowania działalności terroryzmu, ekstremizmu lub separatyzmu. W ramach podstawowych kierunków walki przewidywane jest współdziałanie ze środkami masowego przekazu, organizacjami społecznymi w celach przeciwdziałania propagandzie zjawisk określonych w koncepcji. Innymi działaniami są: walka z terroryzmem informatycznym; uogólnianie i rozpowszechnianie doświadczeń wspólnej walki z terroryzmem; okazywanie pomocy stronom trzecim w tej walce; wypracowywanie wspólnych ustaleń dla uczestnictwa w międzynarodowych organizacjach i międzynarodowych forach poświęconych problemom zwalczania terroryzmu, separatyzmu i ekstremizmu. Uczestnicy SOW zobowiązani są do doskonalenia bazy materialno – technicznej niezbędnej dla skutecznej walki z terroryzmem, w tym doskonalenia wyposażenia oddziałów antyterrorystycznych. W ramach SOW współpracują w przygotowaniu i szkoleniu, w celach podwyższania kwalifikacji kadr organów zajmujących się zwalczaniem terroryzmu.

Formami realizacji współpracy w zakresie realizacji zadań przedstawionych w koncepcji jest prowadzenie wspólnych przedsięwzięć profilaktycznych, operacyjno – dochodzeniowych i śledczych. Zalecone jest

przeprowadzanie wspólnych działań antyterrorystycznych, wymiana informacji w zakresie działalności operacyjno – dochodzeniowej, kryminalistycznej, w tym wiadomości o przygotowywanych i przeprowadzonych akcjach terrorystycznych, ekstremistycznych oraz separatystycznych, także związanych z nimi osób i organizacji. Pomocnym jest powstanie wspólnych banków danych i rozbudowany system łączności, w tym łączności tajnej. Umawiające się strony zobowiązane są do okazywania sobie nawzajem pomocy prawnej oraz organizowania i prowadzenia wspólnych ćwiczeń, przygotowywania kadr, wymiany doświadczeń i literatury fachowej związanej z problematyką walki z terroryzmem, separatyzmem i ekstremizmem oraz prowadzonych badań naukowych w tej dziedzinie. Przedstawione dokumenty ukazują jak skomplikowanym, niezmiernie trudnym do rozwiązania problemem jest międzynarodowa współpraca w tym zakresie.

Mechanizmem realizującym zadania koncepcji, w tym opracowywanie w ramach SOW międzynarodowych umów, programów i działań w celu realizacji ustaleń z niej wynikających zajmuje się Komitet Wykonawczy Regionalnej Struktury Antyterrorystycznej SOW. Jest on zobowiązany do wykonywania zadań koordynacyjnych, współpracy prawnej i analityczno – informacyjnej dla realizacji wspólnych ustaleń państw SOW w walce z terroryzmem. Komitet Wykonawczy przygotowuje propozycje i zalecenia dla Rady Regionalnej Struktury Antyterrorystycznej, Rady Szefów Państw i Rady Szefów Rządów SOW. Regionalna Struktura Antyterrorystyczna jest stale działającym organem SOW, której istnienie uregulowane jest artykułem 10 Karty Szanghajskiej Organizacji Współpracy[15]. Umowa o powstaniu i działalności RSA została podpisana jednocześnie z Kartą SOW w dniu 7 czerwca 2002 r. i weszła w życie 14 listopada 2003 r. W tym samym roku zatwierdzony został regulamin, struktura i stan osobowy Komitetu Wykonawczego RSA. W grudniu 2003 r. oraz w kwietniu 2004 r. w Taszkencie odbyły się posiedzenia Rady RSA – kierowniczego organu Regionalnej Struktury Antyterrorystycznej, która to zajmuje się wszystkimi problemami działalności struktury. Na jeden rok, zgodnie zasadą rotacji przewodniczenie Radzie RSA objął przedstawiciel Republiki Kirgiskiej[16]. Decyzją Rady Szefów Państw SOW pierwszym dyrektorem Komitetu Wykonawczego RSA został Wiaczesław Kasymow[17], zastępca przewodniczącego Służby Bezpieczeństwa Narodowego Uzbekistanu. Komitet Wykonawczy RSA rozpoczął swoje funkcjonowanie w Taszkencie w styczniu 2004 r. Do osiągnięć KW RSA współpracującego z ekspertami państw członkowskich zaliczyć można przygotowanie m. in. siedmiu projektów dokumentów prawnych, w tym: o trybie organizacji i przeprowadzania wspólnych działań antyterrorystycznych na terytoriach państw SOW, o technicznej ochronie informacji w ramach RSA, regulacji posługiwania się tajnymi informacjami. W wyniku prac Komitetu Wykonawczego przygotowana została propozycja[18] wprowadzenia stałych przedstawicieli państw członkowskich przy Regionalnej Strukturze Antyterrorystycznej dla zabezpieczenia efektywnej współpracy RSA z kompetentnymi organami władzy państw członków SOW. Rada RSA zatwierdziła listę terrorystycznych, separatystycznych i ekstremistycznych organizacji, których działalność jest zakazana w państwach SOW, spis osób uznanych przez służby specjalne państw członkowskich za uczestników bądź podejrzanych o uczestnictwo w aktach terrorystycznych oraz działalności separatystycznej i ekstremistycznej. Rada RSA podjęła decyzję o przeprowadzeniu wspólnych ćwiczeń antyterrorystycznych przy udziale właściwych resortów Uzbekistanu, Tadżykistanu i Kirgistanu w 2005[19] r. Za stronę organizacyjną odpowiadały wspólnie Uzbekistan oraz Komitet Wykonawczy RSA. Przedstawiciele Komitetu Wykonawczego RSA uczestniczyli na zaproszenie Centrum Antyterrorystycznego krajów WNP w m in. ćwiczeniach Rubież – 2004 w Kirgizji oraz w Mołdawii (ćwiczenia Antyterror – 2004). Komitet Wykonawczy RSA przygotował i przekazał do właściwych organów państw SOW informacyjno – analityczne dokumenty, m in. o przedsięwzięciach podejmowanych za granicą dla przeciwdziałania terroryzmowi międzynarodowemu, o działalności religijno – ekstremistycznej organizacji Hizb - ut- Tahrir, o źródłach i przyczynach przejawów

międzynarodowego terroryzmu i religijnego ekstremizmu w rejonie Centralnej Azji. Regionalna Struktura Antyterrorystyczna utrzymuje m in. robocze kontakty z regionalnym przedstawicielstwem administracji ONZ zajmującym się narkotykami i przestępczością, misjami dyplomatycznymi w Uzbekistanie. W ramach działalności odbyły się robocze spotkania z kierownikami misji dyplomatycznych USA, Francji, Jordanii, Egiptu, Indonezji, Arabii Saudyjskiej podczas których podzielono się wiedzą na temat problemów walki z terroryzmem, separatyzmem i ekstremizmem członków SOW oraz działalności RSA. Wiaczesław Kasymow uczestniczył w dwóch spotkaniach poświęconych zabezpieczeniu granic. Pierwsze odbyło się w ramach OBWE w Wiedniu, a drugie pod egidą departamentu ONZ zajmującego się problematyką walki z przestępczością i handlem z narkotykami. Charakteryzowana organizacja aktywnie współuczestniczyła w czwartym, specjalnym spotkaniu Komitetu Kontrterrorystycznego ONZ w styczniu 2005 r w Ałma - Acie z organizacjami międzynarodowymi regionalnymi i subregionalnymi. W Brukseli RSA brała udział w corocznej (drugiej) konferencji w sprawach bezpieczeństwa organizowanej przez Instytut Wchód – Zachód i Światową Organizację Handlu. Regionalna Struktura Antyterrorystyczna podjęła także współpracę z Zespołem Monitorującym[20] ONZ zajmującym się problemami Al-Kaidy i Talibów. Umawiające się strony uzgodniły dalsze dwustronne kontakty oraz wymianę informacji w interesującej ich problematyce. Regionalna Struktura Antyterrorystyczna działa już 8 rok.

Z dostępnych informacji wynika, że struktura i jej kierownik aktywnie uczestniczą w przedsięwzięciach związanych z międzynarodową współpracą w zakresie zwalczania terroryzmu i separatyzmu. W. Kasymow w swoich wystąpieniach mówił o ścisłych związkach organizacji przestępczych z organizacjami terrorystycznymi, ekstremistycznymi i separatystycznymi. Zorganizowana przestępczość jego zdaniem finansuje pozostałe formy działalności. Dyrektor Komitetu Wykonawczego RSA Myrzakan Subanow[21] przejawiał sporą aktywność, tak jak jego poprzednik. W 2007 roku uczestniczył m in. w 57 spotkaniu dowódców wojsk ochrony pogranicza państw członkowskich WNP w Erewaniu, w ćwiczeniach kontrterrorystycznych odbywających się na Białorusi, seminarium w sprawie przeciwdziałania aktom terroryzmu jądrowego w Taszkencie zorganizowanego przez ONZ i OBWE. Podczas szóstego spotkania kierowników służb specjalnych, organów bezpieczeństwa i porządku[22] w Chabarowsku przedstawił referat o funkcjonowaniu banku danych RSA SOW. Podczas dziesiątego spotkania Rady RSA omówione i ocenione zostały dotychczasowe osiągnięcia RSA. Ocenione zostały przeprowadzone ćwiczenia antyterrorystyczne na terytorium Kirgizji (Issyk – Kul Antyterror 2007) oraz w Rosji – Misja – Pokojowa 2007. Przyjęty został program współpracy państw SOW w walce z terroryzmem, separatyzmem, ekstremizmem na lata 2007 – 2009 i plan pracy Komitetu Wykonawczego RSA na 2008 r. Podkreślono potrzebę wsparcia Chin dla zapewnienia bezpieczeństwa podczas Olimpiady w Pekinie w 2008 r. W czerwcu 2008 w Ałma – Acie przeprowadzone zostały kolejne ćwiczenia operacyjno – taktyczne pod kryptonimem Atom – Antyterror 2008. Celem było przećwiczenie praktycznych nawyków związanych z oceną sytuacji, podjęcie decyzji w celu organizacji operacji specjalnej dla lokalizacji aktu terrorystycznego i likwidacji jego następstw na jednym z obiektów kompleksu atomowego. Od 2010 r. dyrektorem Regionalnej Struktury Antyterrorystycznej jest generał lejtnant Dżenisbek Dżumanbekow[23]. Pod kierownictwem Dżumanbekow a RSA kontynuuje organizację i przeprowadzanie ćwiczeń. Ostatnimi były ćwiczenia Tian – Szan 2 w maju 2011 r. W dniach 2 – 5 czerwca bieżącego roku przeprowadzone zostały ćwiczenia Wostok – Antyterror 2012.

Ponieważ Szanghajska Organizacja Współpracy skupia członków oraz państwa – obserwatorów, niekoniecznie wcześniej pozostających w dobrych stosunkach politycznych, należy się spodziewać nieporozumień w trakcie rozwijającej się współpracy. SOW skupia oprócz państw potężnych, również państwa, które możemy nazywać upadłymi, np. Tadżykistan czy Kirgistan. Jednym z poważniejszych incydentów w trakcie

funkcjonowania RSA była wypowiedź W. Kasymowa, który w wywiadzie dla *Независимой газеты* dał do zrozumienia, że Kazachstan nie przeciwdziała finansowaniu terroryzmu i stwierdził, iż na jego terytorium istnieją enklawy wykupione przez firmy należące do terrorystów (dosł. ben ladenów). Spowodowało to replikę innego generała, przedstawiciela Kazachstanu Beksułtana Sarsiekowa, który kategorycznie zaprzeczył ich istnieniu i uznał, że jeżeli Kasymow ma takie informacje to powinien je przekazać na forum RSA. Wystąpienie Kasymowa pokazuje sprzeczności interesów i pewną dozę nieufności, występującą wśród partnerów, gdyż taka sprawa powinna być wyjaśniona wewnątrz samej organizacji. O ile współpraca służb większości państw WNP, może odbywać na zasadzie zaufania, gdyż gros ich funkcjonariuszy, szczególnie wyższych kadr, wywodzi się z szeregów KGB[24]. Brak pełnego zaufania pomiędzy służbami bezpieczeństwa Rosji i Chin, oraz pozostałych państw SOW, z racji historycznych zaszłości, może negatywnie rzutować na ich współdziałanie w walce z terroryzmem. Może się to przełożyć na możliwości, sprawność i skuteczność Regionalnej Struktury Antyterrorystycznej. Szanghajska Organizacja Współpracy, której stale działającym organem jest RSA będzie przechodziła wiele kolejnych zawirowań, wynikających ze ścierających się wpływów, obecnie dwóch największych i najsilniejszych jej członków: Chin i Rosji, z rysującą się przewagą, szczególnie ekonomiczną, tych pierwszych.

Kazimierz Kraj

Przypisy

1 Zob. Kukułka J., Historia współczesna stosunków międzynarodowych 1945 – 1996, Warszawa 1998, s. 603 – 605.
2 Dla Rosji jest to obszar Północnego Kaukazu, poradzieckich republik środkowoazjatyckich: Kazchstanu, Kirgizji i Tadżykistanu (miękkie podbrzusze Rosji), dla Chin to separatyzm ujgurski we Wschodnim Turkiestanie (Xinjiang). O separatyzmie ujgurskim zob. Mroziewicz K., Moc, niemoc i przemoc, Warszawa 2005, s. 277 – 279. Więcej o meandrach w stosunkach chińsko – rosyjskich czytaj np.: Jakowlew A., Partnerstwo zaufania, /w:/ Dziś, Przegląd społeczny, nr 11/1997, s. 80-85; tamże, Lichaczow W., Strategiczne partnerstwo, s. 85 – 89. Szafarz S., Chiny w 21. wieku, /w:/ Dziś, Przegląd społeczny, nr 10/2001, s. 61 – 62; zob. także Kaczmarski M., Rosyjska polityka dalekowschodnia, /w:/ Raport, wojsko, technika, obronność nr 1 z 2005 r., s. 60 – 63.
3 Oprócz tego układu podpisanych zostało szereg porozumień międzyrządowych w takich dziedzinach jak ochrona praw własności intelektualnej, współpraca w sferze bezpieczeństwa jądrowego czy ustanowienie gorącej linii.
4 Ponownie ten scenariusz został przećwiczony prawie rok później, w kwietniu 2000 roku, kiedy bojownicy uzbeccy starli się wojskami Kirgistanu i zostali ponownie wyparci do Tadżykistanu.
5 Wcześniej podpisano umowę o zwalczaniu terroryzmu, którą charakteryzowaliśmy w tym rozdziale.
6 Tematyka ta jest uwidoczniona w dokumentach ze spotkań w Ałma-Acie w 1998 r., Biszkeku w 1999 r. i Duszanbe w lipcu 2000 r.
7 Umowa międzynarodowa, wspólne oświadczenie państw lub ich pełnomocników powodujące skutki prawne np. w dziedzinie polityki zagranicznej, bezpieczeństwa czy ekonomiki.
8 Tekst konwencji został sporządzony w dwóch językach, chińskim i rosyjskim, w jednym oryginalnym egzemplarzu.
9 Art. 7 charakteryzowanej konwencji.
10 Zob. art. 15 konwencji.
11 Są nimi art. 11, 12 i 13.
12 Art. 18 konwencji.
13 Astana - Kazachstan lipiec 2005 r.
14 Zob. tekst koncepcji: w ww.president.kremlin.ru/text/docs/2005/07/90911.shtml.
15 Zob. tekst www.kremlin.ru/text/docs/2002/06/46246.shtml
16 Jako pierwszy był nim W.T. Połuektow – pierwszy zastępca przewodniczącego ówczesnej Służby Bezpieczeństwa Narodowego Republiki Kirgiskiej.
17 Wiaczesław Kasymow, ur. w 1947 roku w rejonie Buchary, ponad trzydzieści lat służby w organach bezpieczeństwa, generał major, brak bliższych informacji o przebiegu służby i wykształceniu. Wg informacji z oficjalnej strony internetowej RAS SOW zawodowo zajmował się walką ze zorganizowaną przestępczością, terroryzmem i ekstremizmem.
18 Przygotowane zostały propozycje odpowiednich aktów prawnych.
19 W 2005 r. przeprowadzone zostały także wspólne ćwiczenia rosyjsko – chińskie pod kryptonimem Misja Pokojowa. Uczestniczyły w nim lotnictwo, wojska lądowe oraz marynarka wojenna. Łącznie około 10 tys. żołnierzy. Celem ćwiczeń było przywrócenie ładu i porządku na hipotetycznej wyspie, gdzie doszło do zamieszek i rewolty w wyniku których władzę przejęli terroryści. Zaskakującym było użycie w ćwiczeniach strategicznych bombowców rosyjskich zdolnych do przenoszenia ładunków jądrowych (m in.Tu-95MS i Tu-22M3).
20 Powołany na mocy rezolucji nr 1617 Rady Bezpieczeństwa ONZ w 2005 roku.
21 Myrzakan Subanow, generał pułkownik, doktor nauk politycznych, były minister obrony Kirgizji w latach 1993 – 1999, ostatnio przewodniczący służby pogranicza Kirgizji . Absolwent Akademii Wojskowej im. M. Frunzego i Akademii Sił Zbrojnych ZSRR.
22 W spotkaniu brali udział przedstawiciele 53 państw i 4 organizacji międzynarodowych.
23 Dżenisbek Dżumanbekow, generał lejtnant, absowent Moskiewskiego technologicznego Instytutu Przemysłu Żywnościowego, absowlwent wyższych kusrsów KGB przy RM ZSRR, pracownik KGB a następnie Komitetu Bezpieczeństwa Narodowego Kazachstanu, m in. zstępca przewodniczącego tego komitetu i zastępca dyrektora Służby „Barłau" (wywiad) Republiki Kazachstan.
24 Przykładem takich personalnych powiązań był przewodniczący Komitetu Bezpieczeństwa Narodowego Kazachstanu, generał lejtnant Nartaj Dutbajew, absolwent Wyższych Kursów KGB w Mińsku i Moskwie, zaczynający swoją służbę w organach bezpieczeństwa w Zarządzie KGB Kraju Stawropolskiego. Dutbajew w swojej karierze był także szefem służby wywiadu Kazachstanu zwanej Barłaj.

Cyberterroryzm i bezpieczeństwo informatycznej infrastruktury krytycznej

cz. I, Informatyczna infrastruktura krytyczna państwa i jej ochrona prawna

Wstęp

Rozwój oznacza postęp, czyli najczęściej technologie i ich upowszechnianie się. Związane są z tym nowe wyzwania, które stają oko w oko z dotychczasowym stanem i pojmowaniem bezpieczeństwa państw oraz społeczeństw. Jednym z takich wyzwań jest zwrócenie uwagi na bezpieczeństwo tzw. infrastruktury krytycznej. Wyodrębniamy ją bowiem coraz częściej spośród pozostałych krajowych obiektów. Infrastruktura ta i związane z nią obiekty nie pozostają w izolacji od zmieniającego się świata i również czerpią szerokimi garściami z postępu technologicznego. Co za tym idzie, w wyniku poszerzającej się informatyzacji tych obiektów i włączaniu ich do ogólnoświatowej sieci informacyjnej – Internetu – pojawia się kolejne wyzwanie. To sprawa zapewnienia bezpieczeństwa tym obiektom od strony informatycznej.

Powszechna informatyzacja to nie zaledwie sam rozwój dostępu do Internetu. To jeszcze większa obecność komputerów połączonych siecią, w wielu instytucjach państwowych, pozarządowych oraz przedsiębiorstwach. Dziś ich informacje są składowane nie tylko w formie papierowej, zajmując miejsce w przepastnych archiwach; ilości danych niemożliwe do oszacowania są już przechowywane w postaci cyfrowej na podobnie niezliczonych serwerach. Sieć internetowa pozwala na szybką i łatwą ich wymianę pomiędzy uprawnionymi instytucjami. Również obywatele coraz chętniej poprzez komputer załatwiają wiele swoich urzędowo-administracyjnych spraw, które wcześniej wymagały złożenia bezpośredniej wizyty w odpowiedniej placówce. A przeniesienie działalności urzędów administracji i ich kontaktu z petentami do Internetu, jest tylko jednym z wielu w praktyce już funkcjonujących przykładów informatyzacji działania państwa. Z tym wszystkim wiąże się i wzrost umiejętności informatycznych ogółu społeczeństwa, gdzie jeszcze więcej osób posiada i poznaje wiedzę na temat rzeczywistych prawideł funkcjonowania różnych systemów, dowiadując się tak o ich mocnych i pożytecznych aspektach, jak i tych słabych i możliwych do wykorzystania tylko we własnym interesie. W XXI wieku przy niewielkim wysiłku przecież niemal każdy może stać się zarówno sprawnie poruszającym się w cyberprzestrzeni człowiekiem, jak i groźnym dla innych cyberprzestępcą-hackerem. W jaki sposób to wszystko przekłada się więc na bezpieczne funkcjonowanie całego państwa? Czym są elementy informatycznej infrastruktury krytycznej, jakie istnieją dla niej zagrożenia? Jak zapobiegać i przeciwdziałać zagrożeniom?

Artykuł poświęcony jest próbie odpowiedzi, co należy rozumieć poprzez bezpieczeństwo informatycznej infrastruktury krytycznej. Jest to chęć wyjaśnienia jakie awarie, ataki czy inne zdarzenia mogą zakłócić jej funkcjonowanie, i jaka jest organizacja jej ochrony wraz z niektórymi regulacjami prawnymi. W części pierwszej podjęty został cel opisania czym jest infrastruktura krytyczna oraz jej informatyczna część, co się na nią może składać, jaka jest jej charakterystyka i jakie są podstawy prawne jej ochrony. Część druga wyjaśni z jakimi zagrożeniami może spotkać się informatyczna infrastruktura krytyczna. W części trzeciej i ostatniej, opisane zostaną praktyczne sposoby i proces ochrony tej infrastruktury, zaczynając od form instytucjonalno-organizacyjnych, po fazy obrony oraz praktyczne środki zaradcze. Ważnym aspektem podczas pisania było zwrócenie uwagi na zagadnienie cyberterroryzmu, i rozpatrywania go jako jednego z niebezpieczeństw grożących

informatycznej infrastrukturze krytycznej, stąd wyróżnienie tej kwestii w tytule artykułu. Praca przedstawia zarówno poglądy zaczerpnięte z literatury, opinie ekspertów na ten temat, jak też własne uwagi oraz komentarze autora.

Informatyczna infrastruktura krytyczna państwa i jej ochrona prawna.

Czym jest infrastruktura krytyczna? Polska *Ustawa o zarządzaniu kryzysowym* rozumie przez to pojęcie „systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców”[1].

Według ustawy, infrastruktura krytyczna obejmuje systemy:

- Zaopatrzenia w energię i paliwa;
- Łączności i sieci teleinformatycznych;
- Finansowe;
- Zaopatrzenia w żywność i wodę;
- Ochrony zdrowia;
- Transportowe i komunikacyjne;
- Ratownicze;
- Zapewniające ciągłość działania administracji publicznej;
- Produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Ochronę infrastruktury krytycznej, wedle ustawy rozumieć należy jako „wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie”[2].

W Ustawie o ochronie osób i mienia wymienia się obszary i obiekty podlegające obowiązkowej ochronie. Również *Rozporządzenie RM z dnia 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony* wylicza szereg takich obiektów. Wśród przykładów wskazuje się na strategicznie ważne zakłady produkcyjne i magazyny, zapory wodne, obiekty telekomunikacyjne, porty morskie i lotnicze oraz inną infrastrukturę transportowo-logistyczną, a także większe banki, i obiekty elektroenergetyczne.

Wszystko, czego uszkodzenie bądź zniszczenie może drastycznie zagrozić funkcjonowaniu państwa na jakimś jego obszarze, jest więc obiektem infrastruktury krytycznej. Przeciwieństwem są tzw. obiekty miękkie, jak centra handlowe, miejsca rozrywki, czy edukacji oraz miejsca pracy, których uszkodzenie lub zniszczenie także wywierałoby negatywne skutki, ale, nie ograniczało w istotnym stopniu działania i bezpieczeństwa państwa.

Można podzielić infrastrukturę krytyczną ze względu na formę własności albo miejsce zlokalizowania, wyróżniając:

- Cywilną lub wojskową;
- Prywatną albo państwową;
- Rządową lub pozarządową;
- Krajową albo zagraniczną;

Lub też, mówić o ogólnej infrastrukturze krytycznej, albo szczególnej, takiej jak:

- Logistyczna (transport, przesył, zaopatrzenie);
- Energetyczna (dostawy energii);
- Zasoby (surowce);
- Administracyjna (zarządzanie i kierowanie);
- Informatyczna (informatyka, telekomunikacja).

Takich kryteriów może być więcej, zależnie od potrzeb. Informatyczna infrastruktura krytyczna jest jednym z jej elementów.

Informatyczna infrastruktura krytyczna i jej rodzaje

Obecna *Ustawa o zarządzaniu kryzysowym* „nie definiuje pojęcia krytycznej infrastruktury teleinformatycznej państwa i w żaden sposób nie rozpatruje jej specyfiki"[3].

W listopadzie 2004 r. zespół ds. Krytycznej Infrastruktury Teleinformatycznej powołany przez premiera stwierdził, że „systemy i sieci teleinformatyczne, których nieprawidłowe funkcjonowanie lub uszkodzenie - niezależne od przyczyn i zakresu - może spowodować istotne zagrożenie dla życia lub zdrowia ludzi, interesów obronności oraz bezpieczeństwa państwa i obywateli, albo narazić te interesy na co najmniej znaczną szkodę"[4] to infrastruktura krytyczna.

E. Lichocki, w opracowaniu *Cyberterrorystyczne Zagrożenie Dla Bezpieczeństwa Teleinformatycznego Państwa Polskiego* wymienia następujące szczególnie narażone na cyberataki teleinformatyczne i teleinformacyjne systemy:[5]

- Kontrola ruchu lotniczego (lotniska cywilne);
- Nadzór ruchu statków (VTS Gdynia, VTS Gdańsk i VTS Szczecin - Świnoujście);
- Łączność cywilna oraz łączność wojskowa (teleinformatyczna, teleinformacyjna i satelitarna);
- Teleinformatyka wykorzystująca komercyjne linie transmisyjne (zwłaszcza bazy danych osobowych);
- Powiadamianie służb ratowniczych i reagowania kryzysowego;
- Teleinformatyka stosowana w sektorze bankowości i finansów.

Uderzenie w takie systemy może być w skutkach katastrofalne dla funkcjonowania państwa. Nie będą to jedyne możliwe rodzaje infrastruktury informatycznej, których zniszczenie lub uszkodzenie takie może mieć takie skutki. W zasadzie, niemal każdy obiekt infrastruktury krytycznej posiada jakieś systemy informatyczne. Jeśli za obiekt taki uznajemy na przykład gazociąg, to atak na komputery nim sterujące może doprowadzić do zmian ciśnienia i w konsekwencji wybuchów oraz poważnych zniszczeń[6]. Podobnie, każdy inny obiekt infrastruktury krytycznej posiada wrażliwe informatycznie elementy, a ich ilość oraz zasięg zależne są od jego funkcji.

Według K. Baniaka, „Krytyczną infrastrukturą telekomunikacyjną (KIT) nazywamy zespół sieci oraz struktur komunikacyjnych, które uszkodzone lub zniszczone, w sposób istotny wpłynęłyby na funkcjonowanie państwa (społeczeństwa)"[7].

Wśród przykładowych systemów wchodzących w skład krytycznej infrastruktury teleinformatycznej, inny autor, Grzegorz Krasnodębski w opracowaniu *Zagrożenia krytycznej infrastruktury teleinformatycznej w dobie rozwoju społeczeństwa informacyjnego* wymienia takie rzeczy jak:[8]

- Systemy ewidencyjne;
- Systemy finansowe;
- Systemy bankowe;
- Systemy logistyczne;
- Systemy medyczne;
- Systemy transportowe;
- Systemy administracji państwowej;
- Systemy bezpieczeństwa;
- Systemy zarządzania kryzysowego.

Omawiany wcześniej Ernest Lichocki, w innym swoim opracowaniu *Ochrona krytycznej infrastruktury teleinformatycznej w aspekcie infrastruktury krytycznej państwa* podaje[9] taki podział tej infrastruktury, z umiejscowieniem w niej i teleinformatyki:[10]

1. Energia;
2. Woda;
3. Transport;
4. Systemy i technologia teleinformacyjna, łączność, ICT (Technologia informacyjno- komunikacyjna):
   - sieci teleinformatyczne, oprogramowanie, procesy i ludzie dbające o prawidłowe działanie i bezpieczeństwo. Instalacje służące

pierwotnemu przechowywaniu i składaniu danych;
- Systemy automatyki (SCADA, itd.);
- Internet;
- Stacjonarne systemy telekomunikacyjne. Centrale telefoniczne;
- Mobilne systemy telekomunikacyjne (telefonia komórkowa);
- Łączność i nawigacja radiowa;
- Łączność i nawigacja satelitarna;
- Systemy powiadamiania (Broadcasting);

5. Zdrowie;
6. Żywność;
7. Bankowość i finanse;
8. Administracja państwowa;
9. Narodowe pomniki i pamiątki;
10. Istotny przemysł gospodarki;
11. Wymiar sprawiedliwości;
12. Przestrzeń kosmiczna, eksploracja kosmosu;
13. Kluczowe zasoby.

Ten sam autor, z punktu widzenia natomiast Sił Zbrojnych RP, problematykę opisuje w pracy *Bezpieczeństwo danych w krytycznej infrastrukturze teleinformatycznej* wskazując, że „krytyczna Infrastruktura Teleinformatyczna Sił Zbrojnych Rzeczypospolitej Polski (KITI SZ RP) obejmuje systemy teleinformatyczne i teleinformacyjne niezbędne dla prowadzenia podstawowych działań i prawidłowego funkcjonowania Sił Zbrojnych RP”[11]. Wśród szeregu innych czynników istotnych dla ogólnej infrastruktury krytycznej Sił Zbrojnych (takich jak woda, energia, transport, żywność, administracja, przemysł) wymienia też rzeczy takie jak „systemy i technologia teleinformatyczna oraz teleinformacyjna, łączność”, oraz, technologię komunikacyjno-informacyjną, i wchodzące właśnie w skład KITI[12].

Zapoznając się z tym opracowaniem, możemy w składzie wojskowej krytycznej infrastruktury teleinformatycznej wyliczyć:[13]
- Satelitarne i radiowe systemy nawigacyjne;
- Systemy Dowodzenia i Kierowania Obronnością Sił Zbrojnych (Państwa);
- Systemy Kierowania Systemami Walki;
- Systemy kontroli i naprowadzania lotnictwa;
- Systemy łączności cyfrowej;
- Systemy łączności radiowej;
- Systemy łączności satelitarnej;
- Systemy opto-elektroniczne techniki bojowej;
- Systemy powiadamiania (Broadcasting);
- Systemy rozpoznania;
- Systemy teleinformatyczne, bazy danych, oprogramowanie;
- Stacjonarne i mobilne systemy telekomunikacyjne (sieci wymiany informacji);
- Zautomatyzowane Systemy Dowodzenia.

Charakterystyka informatycznej infrastruktury krytycznej

Pojęcia „informatyczna”, „teleinformatyczna” oraz „telekomunikacyjna” odnoszące się do wyszczególnienia infrastruktury krytycznej można używać zamiennie na potrzeby niniejszego artykułu, jako synonimy. Z drugiej strony, ustawowe uściślenie i ujednolicenie pojęć oraz klasyfikacji tego co wchodzi w skład infrastruktury krytycznej i na co się ona dzieli, byłoby pożądane, na co zwraca uwagę wielu autorów. W końcu technicznie można byłoby podzielić informatyczną infrastrukturę krytyczną na telekomunikacyjną, bazo-danową, obliczeniową, użytkową, itd. To przecież zarówno informatyka, jak i telekomunikacja oparta na informatyce oraz inne wykorzystanie elektroniki i komputerów. Mogą to być też warstwy sprzętu czy oprogramowania oraz urządzeń pomocniczych, które wciąż można odpowiednio dzielić. Stąd, konieczne w pracach nad programami jej ochrony jest przemyślane i jasne sklasyfikowanie wszystkich składowych.

Z wcześniejszych rozważań można wysunąć chyba wniosek, że samo ogólne pojęcie informatycznej infrastruktury krytycznej może być rozpatrywane dwojako. Albo, będzie to infrastruktura sama w sobie ogromnie zinformatyzowana, taka jak telefonia

komórkowa (której całkowita awaria wywołałaby poważne skutki), lub stanowić będzie tylko element tej infrastruktury nie najważniejszy dla jej funkcjonowania (np. komputerowe systemy przesyłowe w gazociągu), lecz nadal ogromnie istotny dla jego bezpieczeństwa i działania. Informatyczna infrastruktura krytyczna jest więc albo sektorem wśród wielu innych infrastruktur (obok energii, transportu, administracji, itp.), albo tylko elementem każdego z tych sektorów, bo trudno wyobrazić sobie funkcjonowanie niemal ich wszystkich, bez systemów informatycznych. Zależności ciekawie przedstawiają autorzy projektu *Rządowy program ochrony cyberprzestrzeni RP na lata 2011-2016*, uznając, że informatyczna infrastruktura krytyczna pozostając elementem infrastruktury krytycznej jest także „częścią cyberprzestrzeni o krytycznym znaczeniu dla jej (infrastruktury krytycznej) funkcjonowania”[14].

Ostatecznie, to i sam Internet będzie w tym rozumieniu infrastrukturą krytyczną. Poważny atak na działanie sieci mógłby być paraliżujący w efektach dla nowoczesnego społeczeństwa i gospodarki oraz bardzo wielu obiektów infrastruktury krytycznej.

Czym różni się zapewnianie bezpieczeństwa infrastrukturze krytycznej państwa, od zabezpieczania podobnie działających systemów informatycznych, ale nie będących już infrastrukturą krytyczną? Wydaje się, że w sprawach technicznych zajdzie przede wszystkim rozszerzenie skali użycia i skomplikowania stosowanej informatyki. Wszystkie instytucje eksploatujące postęp informatyczny, będą przecież korzystały z elektroniki i komputerów, serwerów, stacji roboczych, przewodów i metod przesyłu danych oraz używały oprogramowania i nośników informacji.

W przypadku infrastruktury krytycznej, często rozbudowanej, zmienią się co najwyżej rodzaje oprogramowania na bardziej specjalistyczne, ilość oraz moc obliczeniowa, albo rozmiary baz danych w których składowane są informacje. Zwiększa się zatem stopień rozbudowania całego systemu informatycznego, oraz komplikuje sprawa odpowiedniego jego zabezpieczenia. Większe są i wymagania prawne co do zakresu ochrony. Jednak co do spraw czysto technicznych, związanych z zagrożeniami oraz sposobami przeciwdziałania i zapobiegania, można bardzo często – choć nie zawsze – mówić o tym samym.

To co więc dobrze zabezpiecza mało ważny system informatyczny, może być dobre i do zabezpieczania znacznie poważniejszego systemu, ale samo może okazać się niedostateczne. Żeby zabezpieczyć zwykłe komputery, najczęściej wystarczy dobre oprogramowanie antywirusowe, zapora sieciowa, i przestrzeganie odpowiednich reguł. Te same wskazówki należałoby dać administratorom komputerów i systemów wchodzących w skład infrastruktury krytycznej, lecz zastosować oprogramowanie bardziej profesjonalne, a procedury bezpieczeństwa rozszerzyć i to istotnie. I nadal nie będzie to wszystko co trzeba zrobić, aby dobrze zabezpieczyć system infrastruktury krytycznej, prawie zawsze o wiele bardziej skomplikowany od tych systemów, które infrastrukturą krytyczną nie są. Czy zatem to co stanowi optimum zabezpieczeń dla zwykłej infrastruktury informatycznej, nie jest absolutnym minimum dla tych systemów, które są niezbędne lub ogromnie ważne dla funkcjonowania państwa? Zmienia się jeszcze i skala zagrożenia, oraz możliwe ich źródła. Układem sterowania światłami na skrzyżowaniu któregoś z powiatowych miast, zainteresuje się w najlepszym razie cybernetyczny wandal, albo któryś z przestępców, dopatrzywszy się w tym być może metody na łatwiejszą ucieczkę w chaosie po rabunku. Czy w miejsce takie natomiast, chętnie uderzą cyberterroryści? Co innego, komputerowe systemy zarządzające przesyłem energii elektrycznej, w odróżnieniu od poprzedniego przykładu wchodzące już w skład informatycznej infrastruktury krytycznej. Atak na takie ważne węzły mógłby nawet na kilka dni niemal całkowicie pozbawić energii elektrycznej znaczną część kraju, wywołując bardzo złowieszcze skutki. Należy zauważyć przy tym, że z reguły, wraz ze skalą zagrożenia, rośnie stopień zabezpieczenia danego systemu, ograniczając znacznie szanse i źródła potencjalnego skutecznego uderzenia. Ataku na infrastrukturę krytyczną raczej nie dokona ama-

tor, a jeśli, świadczyć to będzie o tragicznie niskim poziomie zabezpieczenia jej.

Podsumowując, dla zapewniania bezpieczeństwa informatycznej infrastrukturze krytycznej czerpanie z doświadczeń ochrony zwykłych systemów informatycznych będzie słuszne, jednak należy wziąć solidną poprawkę uwzględniając znaczenie tego, co się zabezpiecza.

Ochrona prawna

W jaki sposób informatyczne systemy niezbędne dla funkcjonowania państwa, lub których uszkodzenie mogłoby wywołać fatalne dla niego skutki, są chronione w prawie?

Po pierwsze, należałoby zwrócić uwagę, że z reguły prawo odnoszące się do ochrony ogólnej infrastruktury krytycznej oraz ochrony przed terroryzmem, a także cyberprzestępczością, będzie miało wpływ na bezpieczeństwo informatycznej infrastruktury krytycznej. Dlatego właśnie prawne kwestie zarządzania kryzysowego, zwalczania przestępczości zorganizowanej oraz terroryzmu, są tym co może nas interesować. Wybór pod tym względem okazuje się bardzo szeroki, więc trzeba ograniczyć się do wyliczenia najistotniejszych kwestii, związanych z tematem – czyli ochroną informatycznej infrastruktury krytycznej.

Z konwencji międzynarodowych mających znaczenie dla bezpieczeństwa teleinformatycznego, a których stroną jest Polska, warto wymienić następujące dokumenty:[15]

- Konwencja o zwalczaniu cyberprzestępczości RE z dnia 23 listopada 2001 r. (ETS No. 185);
- Decyzja Rady Ministerialnej OBWE nr 3/04 z dnia 7 grudnia 2004 r., nr 7/06 z 5 grudnia 2006 r. w sprawie działań związanych ze zwalczeniem wykorzystywania Internetu do celów terrorystycznych.

Unia Europejska przyjęła własne prawa i dokumenty, mające organizować ochronę infrastruktury krytycznej, w tym, zwrócenie uwagi na informatyczną ich część. Z inicjatyw UE należy wymienić tu tzw. zieloną księgę w sprawie Europejskiego Programu Ochrony Infrastruktury Krytycznej (2005), komunikat KE w sprawie Europejskiego Programu Ochrony Infrastruktury Krytycznej (2006), i w 2008 roku dyrektywę w sprawie rozpoznania i wyznaczenia europejskiej infrastruktury krytycznej oraz potrzeb w zakresie poprawy jej ochrony.

Oto z kolei polskie ustawy oraz rozporządzenia, najistotniejsze[16] dla tematu rozważań:

- Ustawa z dnia z 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. Nr 182, poz. 12-28);
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2002 nr 101, poz. 926 ze zm.);
- Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz.U. z 2001 r. nr 128, poz. 1402);
- Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2004 r. Nr 171, poz.1800, z późn. zm.);
- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005 r. Nr 64, poz. 565, z późn. zm.);
- Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 roku w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego Dz.U.2011.159.948
- Decyzja Ministra Obrony Narodowej nr 357/MON z dnia 29 lipca 2008 roku w sprawie organizacji systemu reagowania na incydenty komputerowe w resorcie obrony narodowej.

Zobacz więcej:

- Ustawy i rozporządzenia dotyczące bezpieczeństwa teleinformatycznego m. in. w świetle ochrony przetwarzanych w nich informacji niejawnych
  http://www.iniejawna.pl/przyciski/tele_info.html

Rządowy Program Ochrony Cyberprzestrzeni RP

Jeżeli chodzi o praktyczne rozwiązania prawne w Polsce, najbardziej interesujące wydają się *Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2009 – 2011* (RPOC) oraz projekt tego dokumentu, na lata 2011 - 2016 (obecnie w wersji 1.1).

Jak czytamy w projekcie programu, jego przedmiotem „są propozycje działań o charakterze prawno-organizacyjnym, technicznym i edukacyjnym, których celem jest zwiększenie zdolności do zapobiegania i zwalczania zagrożeń ze strony cyberprzestrzeni. Program nie obejmuje swoim obszarem zadaniowym niejawnych sieci i systemów teleinformatycznych. Należy podkreślić, że obszar ochrony informacji niejawnych posiada własne regulacje prawne i stosowne mechanizmy ochronne. Posiada struktury organizacyjne dedykowane do ochrony informacji niejawnych wytwarzanych, przetwarzanych, przechowywanych w wydzielonych systemach i sieciach teleinformatycznych. Podstawowym dokumentem prawnym jest ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. z 2005 r. Nr 196, poz.1631 z późn. zm.)."[17]

Adresatami tego projektu, oprócz organów władzy publicznej w postaci administracji rządowej i samorządowej oraz państwowej, są i „operatorzy infrastruktury krytycznej, których działalność jest zależna i nie zależna od prawidłowego funkcjonowania cyberprzestrzeni"[18].

Na temat operatora infrastruktury krytycznej w projekcie napisano, że jest to „właściciel oraz posiadacz samoistny i zależny obiektów, instalacji, urządzeń i usług infrastruktury krytycznej, wyodrębnionych w systemie łączności i sieci teleinformatycznych i ujawnionych w wykazie infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy o zarządzaniu kryzysowym"[19]. Krytyczna infrastruktura teleinformatyczna natomiast, rozumiana jest jako „wyodrębniona w systemie łączności i sieciach teleinformatycznych i ujawniona w wykazie Infrastruktury Krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy o zarządzaniu kryzysowym". Za realizację celów programu, odpowiadają również, odpowiednio co do swoich kompetencji i „przedsiębiorcy – właściciele zasobów stanowiących krytyczną infrastrukturę teleinformatyczną państwa"[20]. Program można moim zdaniem uważać za konkretny krok do przodu w dziedzinie zabezpieczania infrastruktury krytycznej w Polsce. To zwrócenie uwagi na jej informatyczną jej stronę oraz źródło zagrożeń i konieczność ochrony.

Zostańmy na koniec tej części, przy polskim prawie karnym. Mimo wszystkich podstaw prawnych wyżej wymienionych, brakuje w nim jasnej definicji cyberterroryzmu[21]. Można jedynie wymieniać ogół przestępstw komputerowych albo o charakterze terrorystycznym. Według RPOC, w kodeksie karnym ściganie przestępstw komputerowych dotyczy:[22]

- Przestępstw przeciwko Rzeczypospolitej Polskiej (Rozdział XVII),
- Przestępstw przeciwko bezpieczeństwu powszechnemu (Rozdział XX),
- Przestępstw przeciwko ochronie informacji (Rozdział XXXIII),
- Przestępstw przeciwko wiarygodności dokumentów (Rozdział XXXIV),
- Przestępstw przeciwko mieniu (Rozdział XXXV).

Wszystkie z tych czynów „mogą być potraktowane jako akty terroru, jeżeli ich charakter odpowiadać będzie ustawowej definicji przestępstwa mającego charakter terrorystyczny ustalonej w art. 115 § 20 kk"[23].

Zobacz więcej:

- Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011 - założenia
  http://cert.gov.pl/portal/cer/30/23/Rzadowy_program_ochrony_cyberprzestrzeni_RP_na_lata_2009 2011__zalozenia.html
- Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2011-2016
  http://bip.msw.gov.pl/portal/bip/6/19057

Ochrona infrastruktury krytycznej przed uszkodzeniem (także w wyniku działań cyberterroryzmu) podlega również Ustawie o zarządzaniu kryzysowym, która nakłada na administrację publiczną obowiązki takie jak[24] zapobieganie sytuacjom kryzysowym i przygotowanie do przejmowania nad nimi kontroli, reagowanie w przypadku ich wystąpienia, usuwania skutków takich sytuacji oraz odtwarzania infrastruktury krytycznej.

Już w następnym numerze: Cz. II, Zagrożenia dla informatycznej infrastruktury krytycznej.

Tobiasz Małysa

Przypisy

1 Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2007 nr 89 poz. 590).
2 Tamże.
3 Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011. Założenia, s. 10. Warszawa, marzec 2009. Źródło online: [http://www.cert.gov.pl/download.php?s=3&id=40], dostęp: 2011-12-27.
4 zob. G. Krasnodębski, „Zagrożenia krytycznej infrastruktury teleinformatycznej w dobie rozwoju społeczeństwa informacyjnego", Zakład Zarządzania Kryzysowego, Akademia Marynarki Wojennej. Źródło online: [„http://www.uwm.edu.pl/mkzk/upload/referaty/42_zagrozeniateleinformatycznejinfrastruktury krytycznejw-dobierozwojuspoleczenstwainformacyjnego.doc"], dostęp: 2011-12-30.
5 Por. E. Lichocki, „Cyberterrorystyczne zagrożenie dla bezpieczeństwa teleinformatycznego państwa polskiego", Centrum Symulacji i Komputerowych Gier Wojennych Akademii Obrony Narodowej, Źródło online: [http://www.csikgw.aon.edu.pl/index.php/pl/pobieranie/Publikacje/Cyberterrorystyczne-zagrożenie- dla-bezpieczeństwa-teleinformatycznego-państwa-polskiego-PAN-Warszawa-2008./] Dostęp: 2011-12-26.
6 Tamże.
7 K. Baniak, „Analiza zagrożeń telekomunikacyjnych sektora publicznego". Źródło online: [http://www.bbn.gov.pl/download.php?s=1&id=1000], dostęp: 2011-12-26.
8 Zob. G. Krasnodębski, „Zagrożenia krytycznej infrastruktury teleinformatycznej w dobie rozwoju społeczeństwa informacyjnego", Zakład Zarządzania Kryzysowego, Akademia Marynarki Wojennej. Źródło online: [http://www.uwm.edu.pl/mkzk/upload/referaty/42_zagrozeniateleinformatycznej infrastrukturykrytycznejwdobierozwojuspoleczenstwainformacyjnego.doc], dostęp: 2011-12-30.
9 E. Lichocki, „Ochrona krytycznej infrastruktury teleinformatycznej w aspekcie infrastruktury krytycznej państwa", s. 156-158 [w:] „Ochrona infrastruktury krytycznej", red. Tyburska Agata. Wydawnictwo Wyższej Szkoły Policji, Szczytno 2010.
10 Opracowane przez E. Lichockiego na podstawie: Trusted Information Sharing Network for Critical Infrastructure Protection in Australia, Australia 25 March 2003 r., Zielona księga w sprawie europejskiego programy ochrony infrastruktury krytycznej, COM/2005/576 końcowy, Bruksela, 17 listopada 2005 r. oraz K. Liedel, P. Piasecka, „Jak przetrwać w dobie zagrożeń terrorystycznych. Elementy edukacji antyterrorystycznej", Warszawa 2007.
11 E. Lichocki, „Bezpieczeństwo danych w krytycznej infrastrukturze teleinformatycznej", s. 3.
12 Tamże, s. 1-2.
13 Tamże, s. 2-3
14 Rządowy program ochrony cyberprzestrzeni RP na lata 2011-2016, projekt, wersja 1.1, s. 12. Warszawa, czerwiec 2010. Źródło online: [http://bip.msw.gov.pl/download.php?s=4&id=7445], dostęp: 2011-12-27.
15 Za: Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016, Wersja 1.1, s. 10. Źródło online: [http://bip.msw.gov.pl/download.php?s=4&id=7445], dostęp: 2011-12-26.
16 Tamże.
17 RPOC na lata 2011-2016..., s. 5.
18 Tamże, s. 8.
19 Tamże, s. 6.
20 Tamże, s. 9.
21 Zob. A. Baworowski, „Cyberterroryzm w prawie karnym materialnym - przyczynek do dyskusji na gruncie analizy dogmatycznej". Źródło online: [http://www.dobrauczelnia.pl/upload/File/KONFERENCJE/Cyberrteroryzm/baworowski.pdf], dostęp: 2011-12-26.
22 Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011. Założenia, s. 9. Warszawa, marzec 2009. Źródło online: [http://www.cert.gov.pl/download.php?s=3&id=40], dostęp: 2011-12-27.
23 Tamże, s. 9.
24 J. Świątkowska, I. Bunsch. „Cyberterroryzm - nowa forma zagrożenia bezpieczeństwa międzynarodowego w XXI wieku", s. 4-5. Brief Programowy Instytutu Kościuszki. Źródło online: [http://ik.org.pl/pl/publikacja/nr/4298/], dostęp: 2011-12-26.

Bezpieczeństwo interwencji policyjnych

Wstęp

Zawód policjanta nie należy do najłatwiejszych. Nie każdy może nim zostać. Po przejściu wieloetapowych badań: m.in. fizycznych, psychologicznych, wiedzy ogólnej, lekarskich, kierowany jest do szkoły policyjnej. Młody adept rzemiosła zapoznaje się z charakterem pracy, którą będzie wykonywał. Poza wszelkimi rodzajami regulaminów, umiejętnościami stosowania środków przymusu bezpośredniego, jest uczony technik i taktyk interwencyjnych. Dzięki prawnym możliwościom interweniowania, zawód policjanta jest tak szczególny, ale i niebezpieczny.

Poprawność wykonywanych interwencji, podjęcie ich, zaniechanie, wszystko to może prowadzić do np. zachowania lub utraty zdrowia, życia osób znajdujących się w pobliżu. Zdrowie lub życie policjanta jest także narażone. Wielokrotnie słyszy się o przypadkach źle wykonywanych przez policjantów czynności interwencyjnych. Nie zawsze jednak błędy popełniają młodzi służbą stróże prawa, którzy z braku odpowiedniego doświadczenia mogli niepoprawnie wykonywać czynności interwencyjne. Zdarza się to u doświadczonych, z wieloletnim stażem policjantów, których często gubi rutyna w wykonywaniu czynności interwencyjnych. Bezpieczeństwo wykonywanej interwencji nie jest uzależnione tylko od znajomości przez policjanta przepisów z tym związanych, umiejętności zastosowania środków przymusu bezpośredniego, czy sprawności fizycznej. Podobno żadna z przeprowadzanych interwencji nie jest taka sama. Uważam, że nie jest możliwe, aby regulaminy i kodeksy zawierały stu procentową receptę na skuteczność każdej podejmowanej przez policjanta interwencji. Policjant poza znajomością kodeksów, regulaminów, umiejętności zastosowania środków przymusu bezpośredniego i odpowiedniej sprawności fizycznej, powinien cechować się jasnością

Funkcjonariusz Immigration and Customs Enforcement (USA) dokonuje zatrzymania osoby podejrzanej. **Źródło:** commons.wikimedia.org

i trzeźwością umysłu, sprytem i spostrzegawczością. Wszystkie wymienione cechy mogą mieć wpływ na jakość wykonywanych interwencji.

Celem artykułu jest przedstawienie wybranych taktyk i technik interwencyjnych. Podstawowych czynności, które policjant poznaje w trakcie swojego szkolenia w szkołach policyjnych i którymi się para podczas wykonywania zawodu. Pragnę przedstawić istotę i cele interwencji, a także regulacje prawne ich przeprowadzania. Postaram się wyszczególnić i opisać sposób ich właściwego przeprowadzania, zasad bezpieczeństwa oraz potencjalne mogące wystąpić zagrożenia.

Regulacje prawne

Wymieniając prawne podstawy wykonywania czynności interwencyjnych należy na samym początku przedstawić *Ustawę o Policji z dnia 6 kwietnia 1990 roku (Dz. U. tj. z 2007 r. nr 43, poz. 277 z późń. zm.)* dzięki, której policjant z mocy prawa może wykonywać określone czynności służbowe będące w zakresie jego zadań i uprawnień.[1]

Uregulowania prawne, które bardziej szczegółowo przedstawiają czynności interwencyjne wykonywanych przez policjantów to m. in. *Rozporządzenie Rady Ministrów z dnia 26 lipca 2005 r. w sprawie sposobu postępowania przy wykonywaniu niektórych uprawnień policjantów*. W wymienionym rozporządzeniu znaleźć można uregulowania dotyczące legitymowania osób, ich zatrzymywania, pobierania wymazu ze śluzówki policzków oraz pobierane materiału biologicznego z ludzkich zwłok o nieustalonej tożsamości, kontroli osobistej, przeglądania zawartości bagaży i sprawdzania ładunków w portach, na dworcach. W środkach transportu lądowego, powietrznego i wodnego, obserwowanie i rejestrowanie obrazu i dźwięku zdarzeń w miejscach publicznych i żądania pomocy oraz zwracanie się o niezbędną lub doraźną pomoc[2].

Innymi regulacjami prawnymi odnoszącymi się do czynności interwencyjnych, sposobu i okoliczności ich użycia jest *Rozporządzenie Rady Ministrów z dnia 17 września 1990 r. w sprawie określenia przypadków oraz warunków i sposobów użycia przez policjantów środków przymusu bezpośredniego*. Według rozporządzenia policjant ma prawo zastosować takie środki przymusu bezpośredniego jak:

- *siłę fizyczną w postaci chwytów obezwładniających oraz podobnych technik obrony lub ataku,*
- *urządzenia techniczne w postaci kajdanek, prowadnic, kaftanów bezpieczeństwa, pasów i siatek obezwładniających, a także kolczatek drogowych i innych przeszkód umożliwiających zatrzymanie pojazdu,*
- *chemiczne środki obezwładniające,*
- *pałki służbowe zwykłe, szturmowe i wielofunkcyjne,*
- *wodne środki obezwładniające,*
- *psy i konie służbowe,*
- *pociski niepenetracyjne miotane z broni palnej*[3].

Z przepisów o charakterze wykonawczym warto wymienić jeszcze *Rozporządzenie Rady Ministrów z dnia 21 maja 1996 r. w sprawie szczegółowych warunków i sposobu postępowania przy użyciu broni palnej przez policjantów* oraz *Zarządzenie nr 494 Komendanta Głównego Policji z dnia 25 maja 2004 r. w sprawie metod i form wykonywania zadań przez policjantów pełniących służbę patrolową*. Ponadto uregulowania prawne dotyczące czynności interwencyjnych posiadają dokumenty instrukcyjne w formie pism, wytycznych, instrukcji wydawanych przez Komendanta Głównego Policji, poszczególnych dyrektorów biur Komendy Głównej Policji, komendantów wojewódzkich lub rejonowych, czy inne kompetentne podmioty. Zaznaczyć można, że regulacje prawne pośrednio odnoszące się do czynności interwencyjnych policji występują w wybranych artykułach kodeksu wykroczeń, kodeksu karnego, kodeksu postępowania karnego i kodeksu postępowania w sprawach o wykroczenia. Dodatkowe regulacje można znaleźć w ustawach *o postępowaniu w sprawach nieletnich*, *ustawie o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi*, *ustawie o ewidencji ludności i dowodach osobistych*, a także *ustawie o cudzoziemcach* i wielu innych[4].

Istota, cechy i cele interwencji

Z pośród wszystkich znanych definicji interwencji policyjnych zazwyczaj wymienia się dwie:

Według Z. Wiernego: „jest to przybycie funkcjonariusza Policji na miejsce zdarzenia, podjęcie działać zamierzających do ustalenia charakteru, rodzaju i okoliczności powstałego zdarzenia i przedsięwzięcie czynności przywracających porządek prawny".

Według W. Bednarka i Z. Stoickiego: „jest to szybkie włączenie się policjanta w tok społecznego zdarzenia, naruszającego normy prawa lub zasady współżycia społecznego w celu czynnego przeciwdziałania mu lub wywarcia nań wpływu i przywrócenia stanu poprzedniego".

Natomiast w przepisach interwencję policyjną określa się jako „czynności polegające na ustaleniu rodzaju zdarzenia i podjęciu na miejscu zdarzenia czynności policyjnych usuwających powstałe zagrożenia oraz przekazaniu w tym zakresie informacji dyżurnemu właściwej miejscowo jednostki policji”[5].

Interwencję przeprowadzić może każdy policjant po ukończeniu podstawowego szkolenia. W praktyce interwencje najczęściej przeprowadzają policjanci z pionu prewencji, głównie pododdziały patrolowo – interwencyjne. Służby prewencji w realizacji stawianych im zadań wykorzystują różne formy i środki, często pracują w niebezpiecznych warunkach przez co ich działania muszą być szybkie i zdecydowane.

Celem czynności interwencyjnych jest głównie *przywrócenie takiego stanu, który jest akceptowany przez prawo oraz ogół społeczeństwa, albo niedopuszczalne do zaistnienia określonych zdarzeń*. Podjęcie czynności interwencyjnych pozwala m. in. zatrzymać sprawcę, nie dopuścić do eskalacji zagrożenia lub jego wystąpienia, wstępnie zabezpieczyć miejsce zdarzenia, W sposób praktyczny podnieść ogólną efektywność działań policji i zaspokoić społeczne oczekiwania na sprawne działanie policji[7].

Podział interwencji

Interwencje są podejmowane przez policjantów w ramach zaistniałych zdarzeń, którymi mogą być – kradzież, bójka, awantura domowa, zakłócanie porządku publicznego, zaginięcie dziecka itp. Za podręcznikiem K. Łagody i R. Częścika „Vademecum interwencji policyjnych” interwencje policyjne możemy podzielić na:

Źródło - przyczynę interwencji:
- *przestępstwa, lub wykroczenia,*
- *naruszenie zasad współżycia społecznego,*
- *prawo cywilne,*
- *klęski, katastrofy, zdarzenia losowe.*

Podstawę formalną:
- *polecenia przełożonych,*
- *własna inicjatywa policjantów,*
- *wezwanie osób poszkodowanych i osób trzecich.*

Miejsce interwencji:
- *w miejscu publicznym, lub prywatnym,*
- *w miejscach należących do osób prawnych.*

Sposób działania :
- *wymagające użycia określonych środków lub ich zaniechania*

Sposób załatwiania:
- *zakończenie na miejscu rozpoczęcia, lub poza miejscem rozpoczęcia,*
- *zakończenie bezrepresyjne,*
- *ukaranie mandatem karnym,*
- *zatrzymanie, doprowadzenie osoby*[8].

Uwagi ogólne o bezpieczeństwie interwencji policyjnych

Zadaniem policji jest zapewnienie bezpieczeństwa i porządku publicznego. Podczas wykonywania czynności interwencyjnych policjant poza doprowadzeniem do stanu, *który jest akceptowany przez prawo i ogół społeczeństwa* musi działać w sposób najbezpieczniejszy tj. zapewnić bezpieczeństwo sobie i innym osobom. Żyjemy w czasach znacznego zagrożenia przestępczością. Przestępcy uciekają się do coraz to bezwzględniejszych metod, nie wahają się używać broni palnej. Jak skutecznie zapewnić bezpieczeństwo obywateli na miejscu interwencji? Sądzę, że można ograniczyć zagrożenie kilkoma zasadami właściwego interweniowania. Policjant powinien być dobrze wyszkolony i posiadać fachową wiedzę potrzebną do wykonywania swojej profesji. Musi działać szybko i zdecydowanie, ale nie bezmyślnie i pochopnie. Na miejscu zdarzenia powinien umiejętnie analizować i oceniać sytuację. Ustalić kto jest sprawcą, a kto ofiarą. Ponadto powinien utrzymywać stałą łączność z jednostką policji oraz w razie potrzeby wezwać wsparcie, wykorzystywać swoje doświadczenie zawodowe. Bezpieczne wykonanie czynności interwencyjnych jest możliwe, gdy zostanie zapewnione bezpieczeństwo osób postronnych, policjanta wykonującego czynności, jego partnera lub kolegów z zespołu.[9]

Elementy sytuacji interwencyjnej

Bezpieczeństwo interwencji nie zależy tylko od umiejętności wykonywania jej przez policjanta. Wielki wpływ na jej przebieg mają czynniki obiektywne. Od czynników tych zależne jest jakich taktyk i technik interwencyjnych użyje policjant. Czynniki obiektywne, niezależne od wykonującego interwencję policjanta to:

- *charakter zdarzenia w tym zagrożenia,*
- *miejsce interwencji,*
- *osoby objęte interwencją,*
- *czas interwencji,*
- *niektóre okoliczności sytuacyjne,*
- *cel interwencji,*
- *informacje o przyczynach interwencji,*
- *obowiązujące przepisy*[10].

Rozwijając czynniki wpływające na bezpieczeństwo przeprowadzanej przez policjanta interwencji, trzeba uzupełnić wcześniej wymienione, o tzw. czynniki subiektywne:

- *wiedza ogólna i zawodowa policjanta,*
- *sprawność fizyczna,*
- *komunikatywność,*
- *analiza i ocena sytuacji,*
- *ocena stanów emocjonalnych ludzi,*
- *odporność na stres,*
- *postępowanie w sytuacjach konfliktowych,*
- *opanowanie emocji (zdenerwowania, strachu),*
- *umiejętności zawodowe policjanta w tym taktyka i techniki interwencyjne, oraz wykorzystywanie doświadczenia własnego i innych,*
- *wyposażenie, uzbrojenie*[11].

Reguły interwencyjnego postępowania

Zdarza się, że policjanci podejmujący czynności interwencyjne narażają na niebezpieczeństwo siebie i ludzi, powodu lekceważenia zagrożenia i niewłaściwego podchodzenia do wykonywanych czynności. Najczęstsze błędy popełniane przez policjantów podczas wykonywania czynności interwencyjnych to: brak odpowiedniej koncentracji, bagatelizowanie informacji lub ustaleń, zwłoka w podejmowaniu decyzji, nieutrzymywanie łączności z dyżurnym jednostki policji, prowokacyjne zachowanie, nadużywanie siły oraz uprawnień, brak lub niewłaściwe przeszukanie, nadmierne zaufanie, rutyna, pośpiech, brak przygotowania do użycia środków przymusu bezpośredniego, broni, ich zły stan techniczny. Ponadto można wymienić inne zachowania takie jak brak odwagi i stanowczości, brak sprawności fizycznej, psychicznej, stres, nieodpowiedzialność, problemy z wymową, brak wyobraźni i inne[12].

Podczas podjęcia czynności interwencyjnych policjant powinien zachować ostrożność, być skoncentrowany oraz utrzymywać łączność z partnerem, drużyną lub dyżurnym jednostki policji. Są to podstawowe zasady, które każdy policjant powinien przestrzegać. Ponadto powinien stosować się do reguł interwencyjnego postępowania wydanych przez Komendanta Głównego Policji:

- *w każdej KPP (KMP) powinien być wydzielony przynajmniej jeden radiowóz wyposażony w kamizelki kuloodporne, hełmy ochronne i radiotelefony nasobne,*
- *do załóg radiowozów interwencyjnych należy obligatoryjnie wyznaczyć co najmniej dwóch policjantów,*
- *w rejony szczególnie zagrożone, odludne oraz w porze wieczorowo - nocnej należy kierować głównie patrole zmotoryzowane,*
- *żądać podniesienia rąk przez osobę podejrzaną podczas wykonywania czynności policyjnych, gdy okoliczności tego wymagają,*
- *w przypadku jw. żądać od osób podejrzanych oparcia się mur lub samochód z rozstawionymi nogami np. w celu ułatwienia przeszukania,*
- *zawsze posiadać broń służbową przygotowaną do ewentualnego natychmiastowego użycia,*
- *utrzymywać stałą łączność radiową z dyżurnym jednostki Policji - w szczególności przy interwencjach domowych, przed i po zakończeniu,*

- *używać w uzasadnionych przypadkach urządzeń nagłaśniających do wymuszenia określonego zachowania się osób objętych interwencją,*
- *używać radiowozów policyjnych jako osłony interweniujących policjantów,*
- *nie używać wszystkich radiowozów (patroli) będących w służbie do obsługi jednego zdarzenia*[13].

Aby bezpiecznie wykonywać czynności interwencyjne musi być zachowanych kilka zasad: utrzymanie kontaktu wzrokowego z partnerem, szybkie ustalenie napastnika i ofiary, rewizja osobista podejrzanych osób, blokada ewentualnej drogi ucieczki. W niektórych państwach zachodnich stopień zagrożenia podczas dokonywania czynności interwencyjnych określa się za pomocą kolorów sygnalizacji świetlnej – czerwony, żółty i zielony:

Kolor czerwony – oznacza niebezpieczeństwo np. na miejscu zdarzenia występuje osoba zdesperowana, gwałtownie reaguje, jest agresywna, posiada broń lub niebezpieczne narzędzie, napastnik jest osobą poszukiwaną listem gończym, wysokie zagrożenie dla życia i zdrowia oraz mienia.

Kolor żółty – należy zachować wysoką czujność, istnieje realna możliwość wystąpienia zagrożenia, miejsce zdarzenia – odludzie, pora nocna , zaciemnienie, interwencja może dotyczyć osób chorych psychicznie, chorych na AIDS, narkomanów, samobójców, u osób objętych interwencją widoczne są zmiany zachowania, próby ucieczki.

Kolor zielony – występuje względne bezpieczeństwo, należy zachować podstawowe zasady bezpieczeństwa określone w regulaminach policyjnych, działać ostrożnie oraz nie rutynowo.

Właśnie dzięki tej metodzie policjanci oceniają sytuację interwencyjną pod kątem bezpieczeństwa. Jest bardzo pomocna, w praktyce ratująca nieraz życie i zdrowie policjantom oraz osobom postronnym. Innymi metodami działającymi na rzecz bezpieczeństwa jest tzw. metoda zegarowa. Za pomocą określenia godzin wskazujemy z której strony może nadejść zagrożenie, na którą stronę trzeba zwrócić szczególną uwagę, a która jest bezpieczna. Do określania, sygnalizowania nadchodzącego niebezpieczeństwa służy również metoda znaków umownych, głównie rąk i dłoni[14].

Funkcjonariusze polcicji Hamburga podczas zatrzymania podejrzanego.
Źródło: commons.wikimedia.org

Taktyka i techniki interwencyjne

Taktykę interwencyjną możemy określić jako metodę działania, która ma na celu doprowadzenie do zakończenia interwencji w sposób możliwie najbezpieczniejszy. Elementami taktyki interwencyjnej są m. in.: przepisy prawa, doświadczenie zawodowe, sprawność fizyczna, wyposażenie policjanta, reguły interwencyjnego postępowania, umiejętność zastosowania technik interwencyjnych. Technikami interwencyjnymi są środki, które policjant wykorzystuje do jej przeprowadzenia. Np. wymienione wcześniej sprawność fizyczna, wyposażenie i uzbrojenie policjanta, znajomość i skuteczne wykorzystanie środków przymusu bezpośredniego[15].

Pościg za przestępcami

Policjanci w celu ujęcia lub zatrzymania osoby biorą udział w pościgu, który może być pieszy lub z użyciem środków lokomocji. W trakcie pościgów pieszych, ze względów bezpieczeństwa policjant nie powinien ich wykonywać po stropach, dachach i na

wysokości bez odpowiedniego specjalistycznego sprzętu. Nie powinien wchodzić do nieznanych i podejrzanych budynków bez wsparcia. Powinien w miarę możliwości podczas pokonywania przeszkód np. wysokich płotów, murów, rowów dokonywać ich sprawdzenia pod kątem bezpieczeństwa. Ostrożnie wybiegać zza rogu w trakcie pościgu.

Podczas podejmowania pościgu środkami lokomocji, policjant musi wziąć pod uwagę, że pojazd, którym porusza się przestępca może zawierać ukrytą broń lub niebezpieczne dla życia przedmioty. Po decyzji wzięcia udziału w pościgu za osobami przemieszczającymi się pojazdami samochodowymi policjant powinien mieć na uwadze: warunki drogowe, topograficzne i atmosferyczne, przyczynę i kierunek ucieczki, możliwości techniczne ściganego pojazdu oraz pojazdu własnego, wyposażenie i uzbrojenie. Ocenić możliwość otrzymania wsparcia i zagrożenie ze strony osoby ściganej[16].

Zatrzymywanie i doprowadzanie osób oraz pojazdów

Podczas dokonywania zatrzymania osób, policjant zawsze powinien brać pod uwagę okoliczności podejmowanej interwencji, takie jak miejsce, charakter zdarzenia, pora dnia. Może bowiem dojść do zatrzymania osoby podejrzanej o popełnienie niebezpiecznego przestępstwa, w miejscu bardzo zaludnionym, ruchliwym, lub np. na odludziu. *Policjant podczas dokonywania zatrzymania osoby jest obowiązany podjąć następujące czynności:*

- *sprawdzić, czy osoba zatrzymywana posiada przy sobie broń lub inne niebezpieczne przedmioty mogące służyć do popełnienia przestępstwa lub wykroczenia albo przedmioty mogące stanowić dowody w postępowaniu lub podlegające przepadkowi,*
- *odebrać broń i przedmioty,*
- *wylegitymować osobę zatrzymywaną,*
- *poinformować osobę zatrzymywaną o zatrzymaniu oraz uprzedzić o obowiązku podporządkowania się wydawanym poleceniom, a także o możliwości użycia środków przymusu bezpośredniego w przypadku niepodporządkowania się wydanym poleceniom,*
- *doprowadzić osobę zatrzymaną do jednostki organizacyjnej Policji*[17].

Policjant podczas zatrzymywania osoby szczególnie niebezpiecznej, w trosce o swoje bezpieczeństwo powinien przestrzegać następujących zasad: zachować szczególną czujność i koncentrację, przewidywać zachowanie sprawcy, w każdej chwili być gotowym do użycia środków przymusu bezpośredniego lub broni. Dokonać z partnerem podziału ról na legitymującego i ubezpieczającego, przejąć kontrolę nad sytuacją i osłabić pewność siebie osoby zatrzymanej, uwzględnić podstawowe cechy zatrzymanego, podczas zbliżania się zachować ostrożność. Po dokonaniu zatrzymania, policjanci doprowadzają osoby zatrzymane do komisariatu policji. Jest to niebezpieczne, bo zazwyczaj w trakcie doprowadzania dochodzi do obniżenia ich czujności. Policjanci w trakcie doprowadzenia powinni nie dopuszczać do kontaktowania się doprowadzanego z osobami postronnymi, Środkiem transportu powinien być pojazd służbowy. Należy przedstawić prawa doprowadzonemu. Prowadzić stałą kontrole jego zachowania. Zatrzymywanie pojazdów przez funkcjonariuszy powinno odbywać się w sposób nienarażający bezpieczeństwa własnego, uczestników ruchu oraz innych osób. Pamiętać należy o kamizelkach odblaskowych szczególnie po zapadnięciu zmroku oraz przy słabej widoczności. Posterunek kontrolny powinien znajdować się w pobliżu oświetlonego obszaru. Ponadto fakt podjęcia zatrzymania pojazdu należy zgłosić dyżurnemu jednostki Policji podając miejsce kontroli, markę oraz numer rejestracyjny pojazdu, a później informację o zakończeniu kontroli[18].

Sprawdzanie osób, pojazdów i budynków

W trakcie przeprowadzania czynności interwencyjnych, sprawdzania, przeszukania osoby, zazwyczaj chodzi o ustalenie czy posiada przy sobie broń, niebezpieczne narzędzia lub niedozwolone środki, mogące stanowić zagrożenie dla życia. Podczas przeprowadzania przeszukania, policjant powinien być ubezpieczany przez partnera. Przeszukanie należy przeprowadzić w sposób najbardziej wygodny dla policjanta, a zarazem niewygodny dla przeszukiwanego. Aby nie mógł podjąć ucieczki lub zaatakować. Czynności należy przeprowadzać w miejscach odpowiednich, najbardziej bezpiecznych. W miarę możliwości należy wydawać zrozumiałe, stanowcze i krótkie polecenia osobie kontrolowanej. Być w ciągłej gotowości do użycia środków przymusu bezpośredniego, chronić je aby przeszukiwany nie mógł ich odebrać. Dokonać przeszukania szybko, ale dokładnie oraz zawiadomić partnera, zespół lub innych policjantów o ewentualnym odnalezieniu broni lub niebezpiecznego narzędzia[19].

Podstawowymi zasadami podczas kontrolowania pojazdów jest podchodzenie do nich z tyłu lub z lewego boku. Kontrolę przeprowadzać w jak najbardziej dogodnym i bezpiecznym miejscu. W warunkach słabej widoczności starać się oświetlić pojazd, kontrolować pojazd razem z partnerem, ubezpieczać się wzajemnie. Nie należy się nachylać nad oknami, być w ciągłej gotowości do ewentualnego odskoczenia od pojazdu lub do skoku za niego.[20]

Przeszukiwanie budynków jest bardzo niebezpieczne z uwagi na nieznajomość konstrukcji. Istnieje wiele pomieszczeń, w których czyhać może na policjanta niebezpieczeństwo. Policjant przy podjęciu decyzji o przeszukaniu budynku powinien ten fakt zawsze zgłosić dyżurnemu jednostki Policji podając szczegółowe dane miejsca w którym się znajduje i okoliczności dotyczące przeszukania. Wykorzystywać dostępną pomoc np. zapewnić sobie informacje na temat budynku od dozorcy. W nieoświetlonych miejscach używać latarki taktycznej, ale w sposób nie dający zlokalizować swojego położenia, zmieniać położenie latarki oraz stosować oświetlanie przerywane[21].

Postępowanie z osobami chorymi na AIDS

Policjanci w trakcie wykonywania swoich czynności służbowych powinni zawsze traktować osobę wobec której następuje interwencja za potencjalnego nosiciela wirusa HIV. Profilaktycznymi środkami ostrożności podczas dokonywania czynności interwencyjnych jest używanie np. rękawiczek lateksowych, bawełnianych, winylowych, gumowych. Należy zachować wysoką czujność oraz postępować w sposób przemyślany, nie pochopny. Trzeba uwzględniać odpowiedni dystans i odległość. Należy zwracać uwagę na zachowanie osób objętych interwencją oraz czy nie ma w pobliżu charakterystycznych przedmiotów jak igły czy strzykawki.

Postępowanie przedlekarskie po potencjalnym zarażeniu się wirusem HIV – należy wycisnąć jak największą ilość krwi z miejsca skaleczenia, przemywać ranę bieżącą wodą z mydłem. Założyć jałowy opatrunek na ranę, a następnie udać się do poradni profilaktyczno – leczniczej najbliższego szpitala chorób zakaźnych[22].

Zobacz więcej:

- Reguły interwencyjnego postępowania
  http://www.policja.swinoujscie.pl/pomocnik/data/pr/interwencje/int_3.html
- Rozporządzenie Rady Ministrów z dnia 26 lipca 2005 r. w sprawie sposobu postępowania przy wykonywaniu niektórych uprawnień policjantów
  http://isap.sejm.gov.pl/DetailsServlet?id=WDU20051411186
- Rozporządzenie Rady Ministrów z dnia 17 września 1990 r. w sprawie określenia przypadków oraz warunków i sposobów użycia przez policjantów środków przymusu bezpośredniego
  http://www.elblag.policja.gov.pl/?m=121&h=spb
- Rozporządzenie Rady Ministrów z dnia 19 lipca 2005 r. w sprawie szczegółowych warunków i sposobu postępowania przy użyciu broni palnej przez policjantów oraz zasad użycia broni palnej przez oddziały i pododdziały zwarte Policji
  http://www.podlaska.policja.gov.pl/_baza/artykuly/zalaczniki/1618_5.pdf

Wnioski

Zapoznając się z czynnościami interwencji policyjnych, można stwierdzić, że samo ich podjęcie może stworzyć niebezpieczeństwo dla policjantów oraz osób postronnych. Umiejętne postępowanie policjanta przy podejmowaniu czynności interwencyjnych nie jest gwarantem przeprowadzenia jej bezpiecznie. Wpływa na to wiele czynników, które zostały wymienione. Takich jak miejsce i czas zdarzenia, oświetlenie lub jego brak, stan psychiczny sprawcy, a nawet warunki atmosferyczne. Przedstawione informacje na temat przeprowadzania w najbardziej bezpieczny sposób interwencji policyjnych poza wspieraniem się źródłami pochodzącymi z książek i aktów prawnych, są wsparte nabytym, niewielkim doświadczeniem w ich wykonywaniu. Z racji czynności interwencyjnych Autor w ramach zasadniczej służby wojskowej w Żandarmerii Wojskowej – pion prewencyjny oraz pracy w Specjalistycznych Uzbrojonych Formacjach Ochrony wykonywał interwencje typu policyjnego.

Tomasz Tylak

Przypisy

1 R. Częścik, K. Łagoda, Vademecum interwencji policyjnych, Szczytno 2010, s. 14.
2 Rozporządzenia Rady Ministrów z dnia 26 lipca 2005 r. w sprawie sposobu postępowania przy wykonywaniu niektórych uprawnień policjantów (Dz. U. z 2005r. nr 141 poz. 1186).
3 Rozporządzenie Rady Ministrów z dnia 17 września 1990 r. w sprawie określenia przypadków oraz warunków i sposobów użycia przez policjantów środków przymusu bezpośredniego (Dz.U. Nr 70, poz. 410 z późn. zm.).
4 R. Częścik, K. Łagoda, Vademecum interwencji..., op. cit., s.15.
5 Tamże s.11.
6 Tamże s.13.
7 Tamże s.14.
8 Tamże s.16-20.
9 Tamże s. 28-29.
10 Tamże s. 30.
11 Tamże s. 32.
12 Tamże s. 33-35.
13 Na podstawie pisma dyrektora departamentu Policji Ruchu Drogowego i Prewencji KGP z 4 maja 1992 r. „Taktyczne formy postępowania policjantów głównie służb patrolowo – interwencyjnych w sytuacjach mogących zagrażać życiu lub zdrowiu" - l.dz. Gb-1011/92 oraz pisma zastępcy komendanta głównego Policji z 26 kwietnia 1994 r. m.in. przypominającego komendantom wojewódzkim Policji o zasadach bezpieczeństwa podczas interwencji policyjnych - l.dz. E-IV-211/94. Źródło online: [http://www.policja.swinoujscie.pl/pomocnik/data/pr/interwencje/int_3.html], dostęp 10.01.2012 r.
14 R. Częścik, K. Łagoda, Vademecum interwencji..., op. cit., s. 35-38.
15 Tamże s. 43-44.
16 Tamże s. 47-50.
17 Rozporządzenie Rady Ministrów z dnia 26 lipca 2005r. w sprawie sposobu postępowania przy wykonywaniu niektórych uprawnień policjantów (Dz. U. z 2005r. nr 141 poz. 1186). Roz. 3. § 8. 1.
18 R. Częścik, K. Łagoda, Vademecum interwencji..., op. cit., s. 51 – 54.
19 Tamże s. 55-57.
20 Tamże s. 57-58.
21 Tamże s. 59.
22 Tamże s. 94-99.

Biuletyn poleca:

Vademecum interwencji policyjnych. Interwencje od A do Z
Łagoda K., Częścik R.
Szczytno 2010, ss. 248.

Cel studiowania

Cel studiowania, edukowania się, to nie tylko znalezienie pracy, lecz własny rozwój intelektualny. Poznawanie nowych dziedzin wiedzy. W mojej opinii najlepszymi doradcami są nasze pasje, własny rozum. W czasach pełnych gwałtownych zmian w gospodarce, pewnego chaosu społecznego, mentalnego, w większości wypadków nie da się przewidzieć, że po ukończeniu konkretnego kierunku studiów znajdzie się natychmiast pracę. Należy studiować to, co nas wciąga, interesuje, ma interdyscyplinarny charakter. W trakcie studiów rozwiniesz się, dojrzejesz i poćwiczysz myślenie, poznasz nowych interesujących ludzi, nawiążesz przyjaźnie, często na całe życie. Ten bagaż doświadczeń, jeśli będziesz aktywnym studentem pomoże Ci w przyszłym życiu osobistym i zawodowym.

Jednym z kierunków studiów, na których możesz rozwijać swoje różnorodne zainteresowania jest bezpieczeństwo wewnętrzne. Studia o interdyscyplinarnym charakterze. Poznasz tajniki kryminalistyki i kryminologii. Zapoznasz się historią terroryzmu, technikami terrorystycznymi. Zdobędziesz wiedzę na temat ochrony informacji niejawnych. Będziesz znał problematykę bezpieczeństwa w komunikacji i transporcie publicznym. Znajomość struktur i procedur zarządzania kryzysowego będzie pomocna nie tylko w pracy zawodowej, ale również życiu codziennym. Odkryjesz tajemnice funkcjonowania organów ochrony porządku publicznego, prawa policyjnego i regulacji związanych ochroną osób i mienia.

W ramach studiów zdobędziesz wiedzę na temat funkcjonowania służb specjalnych Polski, ich historii, osiągnięć, ale i niepowodzeń. Możesz, przyszły nasz Studencie stać się specjalistą w zakresie bezpieczeństwa systemów informatycznych czy fachowcem w dziedzinie bezpieczeństwa i porządku publicznego. Masz możliwość zdobycia umiejętności walki wręcz, walki z narzędziami, z której to niegdyś znani byli *bojcy* KGB. Opanujesz podstawy sztuki strzeleckiej.

Wystarczy tylko złożyć niezbędne dokumenty, aby stać się studentem Wyższej Szkoły Informatyki i Zarządzania w Rzeszowie na kierunku bezpieczeństwo wewnętrzne. Polecam studia nie tylko tegorocznym maturzystom, ale również wszystkim, którzy chcą podnieść swoje kwalifikacje w celu zwiększenia swoich szans na rynku pracy.

Bezpieczeństwo wewnętrzne to studia, ale również jedna z ciekawszych przygód życia.

Oprócz studiowania możesz rozwijać swoje pasje w kołach naukowych funkcjonujących na uczelni, w tym Kole Naukowym Centrum Studiów nad Terroryzmem. Czekają na Ciebie spotkania z ciekawymi ludźmi, szeroka paleta wykładów otwartych i wiele innych przedsięwzięć, które możesz współorganizować i w nich uczestniczyć.

Twoimi wykładowcami będą pracownicy Katedry Bezpieczeństwa Wewnętrznego oraz inni nauczyciele akademiccy naszej uczelni. W naszej katedrze pracują wykładowcy z wielkim doświadczeniem, osiągnięciami zawodowymi i naukowymi.

gen. bryg. rez. dr inż. Tomasz Bąk

Do naukowego boju prowadzi nas dziekan Pan Tomasz Bąk, generał brygady rezerwy, jeden z najmłodszych członków korpusu generalskiego. Doktor nauk wojskowych, weteran wielu długotrwałych misji zagranicznych np. w Iraku czy Bośni i Hercegowinie. Absolwent tzw. *Zmechu* we Wrocławiu, gdzie zdobywał szlify w dziedzinie rozpoznania wojskowego. Żołnierz *Czerwonych Beretów*, dowódca brygad 12 w Szczecinie i 21 w Rzeszowie. Prywatnie miłośnik psów i kotów, twórca jedynego w Rzeszowie Muzeum Techniki i Militariów. Podczas kolejnych spotkań w trakcie studiów Pan Generał, być może, zaznajomi swoich Studentów np. z problematyką wydobywania niezbędnych informacji od pojmanych przez grupy rozpoznawcze nieprzyjacielskich żołnierzy, włącznie ze sposobami ich wiązania.

Wspierają go niżsi rangą, byli żołnierze i policjanci oraz klasyczni cywile jak nasza specjalistka w dziedzinie terroryzmu czeczeńskiego oraz *smiertnic* Pani mgr Ewa Wolska, politolog, absolwentka naszej uczelni oraz Uniwersytetu Rzeszowskiego. To nie koniec zainteresowań naukowych Pani Ewy, która może Ciebie, przyszły studencie, zapoznać z zagadnieniami z zakresu bezpieczeństwa państwa, problematyką Kaukazu Północnego lub konfliktami asymetrycznymi. Nie bądź też pewny czy pokonasz ją w turnieju strzeleckim, a warto próbować. Kontynuując przedstawianie pracowników katedry poznajmy naszych specjalistów w dziedzinie kryminalistyki i kryminologii Panów Józefa Kubasa i Jana Swoła.

Mgr Ewa Wolska

Mł. insp. w st. spocz. mgr Józef

Pierwszy to były szef sztabu Komendy Wojewódzkiej Policji w Rzeszowie. Ponad trzydzieści lat w służbie policyjnej. W młodości żołnierz *Niebieskich Beretów*, naszej piechoty morskiej, absolwent szkoły oficerskiej w Szczytnie i Akademii Spraw Wewnętrznych. Pan Józef przeszedł w swojej karierze zawodowej wszystkie szczeble od szeregowego milicjanta do młodszego inspektora policji. Zorganizował i prowadzi w naszej uczelni laboratorium kryminalistyczne. Jest jednym ze współtwórców lotnictwa policyjnego oraz pilotem śmigłowców. Oprócz tajników kryminologii czy kryminalistyki może Cię nauczyć zarządzania kryzysowego i niezbędnych w rzemiośle policyjnym umiejętności.

Kompetencje konieczne w służbie policyjnej możesz także poznać podczas zajęć z drugim *gliną* Panem Janem Swołem. Pan Jan to nie tylko doktor nauk prawnych i uczeń profesora Tadeusza Hanauska, ale w młodości czynny sportowiec, zapaśnik w stylu, jak by powiedzieli nasi dziadkowie, francuskim, innymi słowy klasycz-

dr Jan Swół (drugi z lewej, górny rząd)

nym. Wielokrotny drużynowy mistrz Polski, członek kadry narodowej, dwukrotny indywidualny wicemistrz Polski. Zawodnik KS „Wisłoka". Jednocześnie znawca przestępczości gospodarczej, funkcjonariusz drużyn specjalnych milicji, płetwonurek, ratownik znający podstawy karate. Wykorzystując swoje doświadczenie nauczy Cię fachowo organizować przedsięwzięcia ochronne obiektów oraz VIP - ów. Dzięki temu Studentko i Studencie będziesz mógł profesjonalnie przedyskutować tę problematykę z *gorylam*i z Biura Ochrony Rządu oraz Secret Service, jeżeli spotkasz ich na swojej drodze.

kpt. rez. dr inż. Maciej Milczanowski

Kontynuując opowieść o Twoich nauczycielach akademickich nie można nie przywołać kolejnego wykładowcy doktora historii i wojskowego łącznościowca, Pana Macieja Milczanowskiego, weterana misji na Wzgórzach Golan i w Iraku. Pan Maciej nauczy Cię historii terroryzmu, metod jego zwalczania, podniesie kompetencje w dziedzinie bezpieczeństwa państwa. Jednocześnie można Go zapytać, jakiej maści był Bucefał, koń Aleksandra Macedońskiego i czy faktycznie Brutus był zabójcą Cezara i kto za nim stał. Po zdobyciu tej wiedzy poznasz jeszcze pod kierunkiem dr. Milczanowskiego tajniki terenoznawstwa i tajemnice pierwszych terrorystów Zelotów oraz ludzi Starca z Gór. Dowiesz się, kim byli sztyletnicy w Powstaniu Styczniowym i jak działali.

Wśród pracowników jest jeszcze jeden wojskowy łącznościowiec, co prawda niskiej rangi, bo starszy kapral. Jego zainteresowania skupiają się wokół problematyki zwalczania terroryzmu w Federacji Rosyjskiej, historii jej służb specjalnych, historii KGB i jego prekursorów, honorowy członek *Klubu Weteranów Bezpieczeństwa Państwowego i Pododdziałów Antyterrorystycznych Alfa* w Moskwie. Może Cię nauczyć jak chronić obiekty infrastruktury krytycznej i informacje niejawne przed terrorystami oraz obcymi służbami specjalnymi. Jak będziesz miał kłopoty ze swoimi kotami czy psami, zwróć się do niego, – czyli dr. Kazimierza Kraja, właściciela wielkiej sfory tych czworonogów, z najgroźniejszym

dr Kazimierz Kraj (z lewej) w szkolnym muzeum wywiadu i kontrwywiadu w Moskwie.

z nich Edmundem, zwanym Muńkiem.

dr Leszek Baran

Kolejny z Twoich przyszłych wykładowców to dr Leszek Baran, socjolog, dziennikarz i znawca poglądów mieszkańców Podkarpacia na temat zagrożeń terrorystycznych. Innym słowy wie, jakie są *strachy na Lachy* związane z zagrożeniami terrorystycznymi. Słuchając Jego wykładów i prowadzonych ćwiczeń poznasz podstawowe zagadnienia z socjologii, problematykę bezpieczeństwa społeczności lokalnych oraz przestępczości. Pan Leszek Baran jest opiekunem koła naukowego Centrum Studiów nad Terroryzmem. Jeżeli zechcesz to np. podczas wykładów otwartych opiekuna koła będziecie przyszła Studentko i przyszły Studencie mogli poznać tajniki warsztatu dziennikarskiego, gdyż oprócz specjalności naukowej Pan dr Leszek Baran jest wytrawnym dziennikarzem prasowym.

płk rez. mgr Sławomir Adamczyk

Problematykę pracy operacyjno – rozpoznawczej poznasz podczas zajęć z płk. rez. mgr. Sławomirem Adamczykiem byłym oficerem Żandarmerii Wojskowej, z niemal 26 – letnim stażem w służbie. Nasz wykładowca pełnił funkcje dowódcze na stanowiskach Komendanta Wydziału i Oddziału ŻW w kilku rejonach kraju. Był Szefem Wydziału i Oddziału - Zastępcą Szefa Zarządu Komendy Głównej ŻW. W toku służby wykonywał m.in. zadania z zakresu tzw. „działań policyjnych" oraz z zakresu przeciwdziałania terroryzmowi. Pracował w zespołach resortowych i międzyresortowych - analizujących zagrożenia typu terrorystycznego i koordynujących podejmowane działania. Posiada tytuł zawodowy detektywa oraz licencję pracownika ochrony II stopnia.

Mili kandydaci na studentów, oprócz wymienionych wyżej wykładowców spotkasz się z innym nauczycielami akademickimi: dr. Witoldem Skomrą, pracownikiem Rządowego Centrum Bezpieczeństwa, byłym Komendantem Głównym Państwowej Straży Pożarnej, wybitnym znawcą prawa pracy dr. Marianem Liwo, byłym wiceszefem Państwowej Inspekcji Pracy, dr. Wojciechem Szczurowskim z Akademii Obrony Narodowej, czy doświadczonym oficerem Wojska Polskiego mgr inż. Arturem Surmaczem.

Drodzy Państwo, aby uzyskać dodatkowe informacje wystarczy nas odwiedzić, a każdy z obecnych w tym momencie pracowników Katedry Bezpieczeństwa Wewnętrznego udzieli Wam konsultacji w sprawie studiów.

Przed wami przyszli Studenci kierunku bezpieczeństwo wewnętrzne jedna z ciekawszych przygód życia. Możecie ją zacząć już od października bieżącego roku.

Zapraszamy na stronę WWW rekrutacji:

http://kandydaci.wsiz.rzeszow.pl/

Lub osobiście:

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

STUDIA PODYPLOMOWE
DLACZEGO NA WSIIZ:

WYSOKA JAKOŚĆ KSZTAŁCENIA
Najlepsza uczelnia niepubliczna w Polsce południowej – wg rankingu „Rzeczpospolitej" i „Perspektyw" oraz jedna z 6 najlepszych w kraju.

PROFESJONALNA KADRA
Wysoki poziom kształcenia zapewnia odpowiednia kadra, stanowiąca połączenie doświadczonych i utalentowanych profesorów - mistrzów z młodymi, kreatywnymi pracownikami nauki i praktykami.

CERTYFIKATY MIĘDZYNARODOWE
Możliwość zdobycia licznych certyfikatów informatycznych, biznesowych i trenerskich uznawanych w Polsce i za granicą. (m.in Practitionera In the Art of NLP, Coacha ICI (International Association of Coaching Institiutes), LUQAM FMEA, Germanischer Lloyd, Cisco Certified Network Associate (CCNA), IPMA, CIMA).

UCZELNIA DLA POKOLEŃ
W strukturach uczelni funkcjonują: Akademickie Liceum Ogólnokształcące, Studia licencjackie i magisterskie, Studia podyplomowe, Akademia 50+.

MOŻLIWOŚĆ ZDOBYCIA DYPLOMÓW INNYCH UCZELNI
m.in. Akademii Ekonomicznej w Krakowie i Politechniki Krakowskiej, Uniwersytetu Szczecińskiego, Wyższej Szkoły Zarządzania i Administracji w Zamościu.

INFRASTRUKTURA NAJNOWSZEJ GENERACJI
67 laboratoriów specjalistycznych wyposażonych w najnowocześniejszy sprzęt, w tym liczne laboratoria komputerowe, badawcze i nowoczesnych technologii: laboratorium grafiki komputerowej i sztuki cyfrowej, automatyki i robotyki, finansowe czy kryminalistyki.

PŁATNOŚCI W SYSTEMIE RATALNYM
Czesne można rozbić na raty miesięczne bez dodatkowych kosztów.

TYSIĄCE ZADOWOLONYCH ABSOLWENTÓW
Ponad 11 tysięcy absolwentów studiów podyplomowych, 250 przeprowadzonych edycji studiów, 11 lat na rynku.

Bliższe informacje na:
www.podyplomowe.wsiz.pl
oraz w siedzibie uczelni
ul. Sucharskiego 2, 35-225 Rzeszów,
tel. 17 866 12 85, 17 866 14 86
e-mail: csp@wsiz.rzeszow.pl

CENTRUM STUDIÓW PODYPLOMOWYCH
Wyższej Szkoły Informatyki i Zarządzania
z siedzibą w Rzeszowie

STUDIA PODYPLOMOWE I KURSY W ZAKRESIE BEZPIECZEŃSTWA

WYŻSZA SZKOŁA INFORMATYKI i ZARZĄDZANIA
z siedzibą w Rzeszowie

STUDIA PODYPLOMOWE

ANTYTERRORYZM
Program studiów obejmuje zagadnienia związane z zasadami prowadzenia działań antyterrorystycznych we współczesnych uwarunkowaniach społeczno–politycznych, zaznajamiając jednocześnie z genezą terroryzmu, koncentrując się szczególnie na procesach prowadzących do postaw ekstremalnych.

BEZPIECZEŃSTWO MIĘDZYNARODOWE
Podczas studiów zaprezentowane zostanie całe spektrum zagadnień związanych z tematyką bezpieczeństwa międzynarodowego, które ma na celu umożliwić opracowywanie koncepcji oraz wyrobienie zdolności przewidywania przyszłych zagrożeń na podstawie dostępnych przesłanek oraz radzenia sobie z nimi.

KONFLIKTY ETNICZNE I MIGRACJE MIĘDZYNARODOWE
Program studiów obejmuje tematykę przygotowania Polaków do nadejścia fali imigrantów, w pierwszej kolejności zaś przygotowania urzędników i pracowników socjalnych do rozwiązywania problemów powstających na styku kultur, a także zapobiegania napięciom wynikającym z powiększania się liczby imigrantów w naszym kraju.

LOGISTYKA BEZPIECZEŃSTWA I STANÓW KRYZYSOWYCH
Słuchacze studiów poznają zasady działalności logistycznej, zadania logistyczne, istotę podejścia systemowego, sieciowego i procesowego w logistyce, zasady sterowania przepływami zasobów i towarzyszącymi im informacjami, a także istotę procesów logistycznych w zakresie realizacji zadań bezpieczeństwa narodowego oraz zarządzania sytuacją kryzysową.

OCHRONA GRANIC I ADMINISTRACJA CELNA
Zakres tematyczny studiów obejmuje problematykę związaną z organizacją i zasadami prawnymi funkcjonowania Straży Granicznej oraz służb celnych. Słuchacze poznają prawo celne, dewizowe, transportowe, procedury stosowane w ochronie granic, postępowaniu celnym, ruchu granicznym oraz granicznej kontroli weterynaryjnej i sanitarnej, a także wybrane aspekty międzynarodowych standardów regulacji prawnych w powyższym zakresie.

OCHRONA INFRASTRUKTURY PORTÓW LOTNICZYCH
Słuchacze studiów zapoznają się m.in. ze specyfiką zadań Służby Ochrony Lotnisk, prawnymi regulacjami bezpieczeństwa lotniczego i procedurami ich stosowania, Ponadto przedmiotem kształcenia są systemy komunikacji, nawigacji, dozorowania i zarządzania ruchem lotniczym, podstawy teorii lotu i ograniczeń eksploatacyjnych statków powietrznych w zakresie, w jakim ma to związek z procedurami lotniskowymi.

POLITYKA OBRONNA I BEZPIECZEŃSTWO NARODOWE
Program studiów obejmuje wszystkie najważniejsze zagadnienia dotyczące uwarunkowań polityki obronnej państwa oraz zasady działalności związanej z zachowaniem bezpieczeństwa narodowego i postępowania w sytuacjach kryzysowych.

STUDIA PODYPLOMOWE

USŁUGI DETEKTYWISTYCZNE
Studia przygotowują słuchaczy do pracy w zawodzie detektywa i uzyskania niezbędnej wiedzy do pozytywnego złożenia egzaminu na licencję w powyższym zakresie.

ZARZĄDZANIE OCHRONĄ OSÓB I MIENIA
Studia przygotowują menedżerów bezpieczeństwa oraz ochrony osób i mienia z pionów MSWiA, MON, BOR, Policji, Straży Miejskich, Straży Granicznej, Poczty Polskiej itp. oraz komórek bezpieczeństwa w urzędach państwowych, starostwach, gminach, bankach i koncesjonowanych przez MSWiA agencjach ochrony osób i mienia.

ZARZĄDZANIE SYTUACJAMI KRYZYSOWYMI I RATOWNICTWEM
W trakcie studiów słuchacze zapoznają się z uwarunkowaniami prawnymi zarządzania w sytuacjach kryzysowych, a także zasadami ochrony informacji niejawnych i danych osobowych oraz organizacją ratownictwa. Ponadto zdobywają wiedzę w zakresie kierowania zespołami ludzkimi w stanach kryzysowych, stosowania niezbędnych procedur, a także organizacyjnymi i technicznymi zasadami działania ratownictwa.

KURSY

- BEZPIECZEŃSTWO SPOŁECZNE
- BEZPIECZEŃSTWO SPOŁECZNOŚCI LOKALNYCH
- BEZPIECZEŃSTWO SYSTEMÓW IT
- POLICYJNE PROCEDURY ZABEZPIECZENIA IMPREZ O CHARAKTERZE MASOWYM
- POSTĘPOWANIE POLICJI W PRZYPADKU ZAGROŻEŃ NARUSZANIA I ZBIOROWEGO ZAKŁÓCENIA PORZĄDKU PUBLICZNEGO
- PROCEDURY DZIAŁAŃ POŚCIGOWYCH POLICJI
- ZASADY OCHRONY LUDNOŚCI I OBRONA CYWILNA
- ZARZĄDZANIE POTENCJAŁEM LUDZKIM W INSTYTUCJACH ODPOWIEDZIALNYCH ZA BEZPIECZEŃSTWO WEWNĘTRZNE

BEZPIECZEŃSTWO WEWNĘTRZNE

WYŻSZA SZKOŁA INFORMATYKI i ZARZĄDZANIA
z siedzibą w Rzeszowie

znajdziesz pracę w:
- służbach mundurowych (policja, wojsko, straż pożarna, straż graniczna)
- służbach specjalnych (ABW, CBA, Agencja Wywiadu)
- agencjach ochrony i detektywistycznych
- zespołach ds. bezpieczeństwa informatycznego
- centrach zarządzania kryzysowego

W programie studiów m.in.:
- obozy szkoleniowe
- trening w zakresie walki wręcz
- walki z użyciem narzędzi
- szkolenie strzeleckie
- zarządzanie bezpieczeństwem systemów informatycznych
- zarządzanie w sytuacjach kryzysowych

SPECJALNOŚCI

antyterroryzm

bezpieczeństwo i porządek publiczny

bezpieczeństwo systemów informatycznych

ochrona informacji niejawnych

zarządzanie kryzysowe

Studenci mają możliwość pogłębiania swych zainteresowań poprzez uczestnictwo w kołach naukowych (antyterrorystycznym, historycznym i wielu innych).

facebook.com/bezpieczenstwo.wewnetrzne

szczegóły na
www.wsiz.rzeszow.pl

Dział Rekrutacji WSIiZ, pok. RA8, ul. Sucharskiego 2, 35-225 Rzeszów
tel. 17 866 11 88, 17 866 11 99, rekrutacja@wsiz.rzeszow.pl

Archiwalne numery e-Terroryzm.pl

– zapraszamy do zapoznania się!

Nr 1, styczeń 2012, a w nim m. in.:

- Magazyn INSPIRE, jako przykład groźnej propagandy terrorystycznej
- Narodowy Komitet Antyterrorystyczny i jego działalność
- Koran a terroryzm
- Akty terrorystyczne w Federacji Rosyjskiej w latach 2005 – IX 2011
- Niebezpieczne luki w prawie
- Nowy wymiar cyberprzestrzeni

Nr 2, luty 2012, a w nim m. in.:

- Płaszczyzny systemu zwalczania terroryzmu
- Zwalczanie terroryzmu w dokumentach ONZ, NATO i Unii Europejskiej
- Broń chemiczna w rękach terrorystów
- Ekoterroryzm, Bioterroryzm
- Metody wykorzystywane w cyberataku
- Metody zwiększania cyberbezpieczeństwa
- Matieżewojna Jewgienija Messnera
- Zwroty w języku farsi (perski)

Nr 3, marzec 2012, a w nim m. in.:

- Irhabi 007, sylwetka terrorysty
- Ataki terrorystyczne na świecie – styczeń 2012 r.
- Ochrona praw człowieka podczas zwalczania terroryzmu
- Zarys historii rosyjskich służb specjalnych
- Psychologiczne aspekty pomocy przedmedycznej
- Postępowanie w przypadku alarmu bombowego
- Zwroty w języku farsi (perski), część II

Nr 4, kwiecień 2012, a w nim m. in.:

- Ataki terrorystyczne na świecie – luty 2012 r.
- Terroryzm kryminalny, incydenty bombowe w statystyce
- Skutki wybuchów jądrowych, cz. I
- Zagrożenie IED w Afganistanie
- Pododdziały wojskowe w unieszkodliwianiu zardzewiałej śmierci
- Rozmowa z chor. Grzegorzem Grucą, dowódcą patrolu rozminowania nr 30
- Kiedy obywatel jest chroniony jak funkcjonariusz publiczny

Chcesz dostarczyć artykuł do publikacji?

Wyślij go na e-mail: **redakcja@e-terroryzm.pl**

Zwyczajowa objętość artykułu to od 3 000 znaków (jedna strona) do 20 000 znaków (co odpowiada około 7-8 stronom).

Możesz dostarczyć fotografie oraz tabele, wymagane są ich podpisy.

Nie musisz w ogóle formatować tekstu – formatowania dokonuje Redakcja.

Tematyka artykułu może poruszać sprawy powiązane z terroryzmem i bezpieczeństwem, a także politologią, zarządzaniem kryzysowym i ratownictwem, ochroną informacji niejawnych i infrastruktury krytycznej.

Nie jesteś pewien czy Twój artykuł odpowiada tematyce czasopisma? Przekonaj się o tym. Na pewno odpowiemy na Twój list.

Redakcja zastrzega sobie prawo do skrótów, korekty oraz publikacji wybranych nadesłanych artykułów.

Nr 5, maj 2012, a w nim m. in.:

- Zasady postępowania z przesyłkami niewiadomego pochodzenia
- Libero II – ostatni sprawdzian przed Euro 2012
- Znaczenie Rosji dla walki z terroryzmem międzynarodowym
- Kwestia bezpieczeństwa Stanów Zjednoczonych Ameryki w latach 2004-2008
- Polityka zagraniczna USA po ataku na WTC
- Postępowanie przy oparzeniach, odłamkach i przygnieceniach
- Szacowanie, analiza i zarządzanie ryzykiem

Archiwalne numery dostępne na naszej stronie:

http://e-terroryzm.pl

Zapraszamy
na stronę
internetową:

www.e-terroryzm.pl

Zobacz także
archiwalne
numery

Czasopismo tworzą studenci
Wyższej Szkoły Informatyki
i Zarządzania w Rzeszowie,
pracownicy Centrum Studiów
nad Terroryzmem
i zaprzyjaźnieni entuzjaści
poruszanej problematyki

Internetowy Biuletyn
Centrum Studiów
nad Terroryzmem
wydawany jest
od stycznia 2012 r.

Fot. U.S. Marine Corps photo by Cpl. Ryan Walker