TERRORISM PREVENTION
Centre of Excellence

PORADNIK PREWENCJI TERRORYSTYCZNEJ

PORADNIK PREWENCJI TERRORYSTYCZNEJ

Skład i łamanie:
Studio DTP Academicon | Patrycja Waleszczak
dtp@academicon.pl | dtp.academicon.pl

© Copyright by Agencja Bezpieczeństwa Wewnętrznego
Centrum Prewencji Terrorystycznej

TERRORISM PREVENTION
Centre of Excellence

00-993 Warszawa, ul. Rakowiecka 2A
tel. 22 564 65 87, fax. 22 564 65 88 | www.tpcoe.gov.pl

Zdjęcia zamieszczone w poradniku pochodzą z:
https://pl.depositphotos.com/
https://stock.adobe.com/
https://pixabay.com/

Autorami grafik są:
Mira Zyśko
Patrycja Waleszczak

Poradnik został opracowany w ramach projektu: *Podnoszenie kompetencji służb bezpieczeństwa państwa, pracowników administracji publicznej i ośrodków naukowo--badawczych oraz rozwój ich współpracy w obszarze bezpieczeństwa narodowego,* realizowanym w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020. POWR.04.03.00-00-0001/12

Fundusze Europejskie Wiedza Edukacja Rozwój
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Społeczny

Warszawa 2021

Szanowni Państwo!

Niniejszy poradnik jest rezultatem pracy Centrum Prewencji Terrorystycznej Agencji Bezpieczeństwa Wewnętrznego. Powstał na podstawie wiedzy eksperckiej funkcjonariuszy ABW, konsultacji z ekspertami krajowymi i zagranicznymi oraz doświadczeń zbieranych podczas spotkań z przedstawicielami służb i instytucji w kraju i za granicą. Uwzględniono w nim najlepsze praktyki i rekomendacje, które stosuje się obecnie na całym świecie. W przystępnej formie zaprezentowano najważniejsze zagadnienia dotyczące prewencji terrorystycznej, których znajomość jest kluczowa na rzecz zapewnienia bezpieczeństwa RP, a w sytuacji zagrożenia może uratować zdrowie lub życie naszych obywateli.

Wyrażam głębokie przekonanie, że zapoznanie się z tą publikacją poszerzy Państwa wiedzę w zakresie reagowania na zdarzenia o charakterze terrorystycznym.

Szef Agencji Bezpieczeństwa Wewnętrznego
płk Krzysztof Wacławek

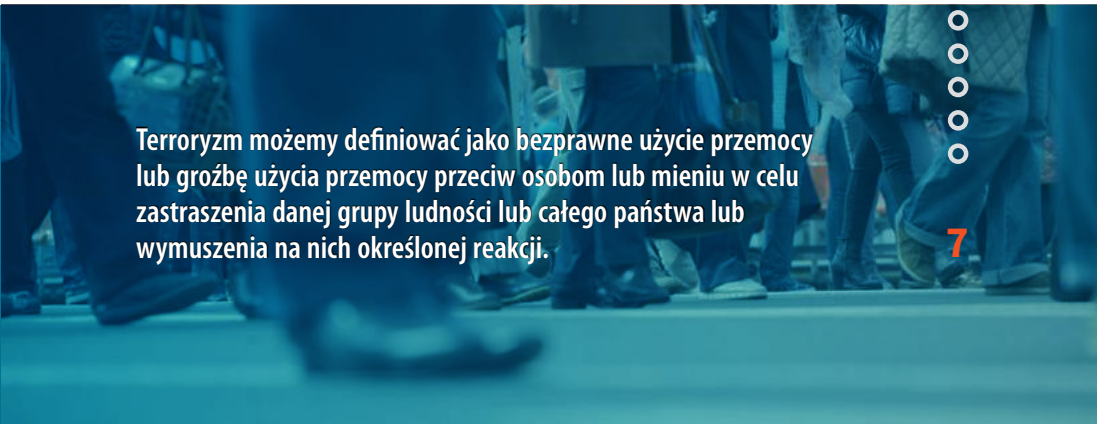
Spis treści

1. Dlaczego powstał ten poradnik? 7
2. Czego dowiesz się z tego poradnika? 10
3. Radykalizacja 12
3.1. Jak rozpoznać radykalizację? 21
3.2. Jak przeciwdziałać radykalizacji? 26
4. Mobilizacja 28
5. Formy zdarzenia o charakterze terrorystycznym 37
6. Procedura 4U! 42
7. Urządzenia i materiały wybuchowe 45
7.1. Niebezpieczny przedmiot 45
7.2. Podejrzana przesyłka 48
8. Uzbrojony sprawca 51
8.1. Atak masowego zabójcy 53
8.2. Sytuacja zakładnicza 62
9. Powiadamianie służb 64
10. Przybycie służb (działania kontrterrorystyczne) 65
11. Ratownictwo w warunkach zagrożenia 66
11.1. Apteczka ratunkowa 67
11.2. Zasady udzielania pomocy w sytuacji zagrożenia 70
11.3. Tamowanie krwawień 71
12. Cyberbezpieczeństwo 75
12.1. Zagrożenia bezpośrednio związane z terroryzmem 75
12.2. Bezpieczeństwo danych osobowych użytkownika i informacji wrażliwych w miejscu pracy 77
12.3. Higiena pracy w Internecie 78
13. Przygotowanie obiektu na wypadek zagrożeń terrorystycznych 82
14. Zarządzanie ryzykiem w obiektach 88
14.1. Przyjęcie informacji o zagrożeniu 91
14.2. Algorytm postępowania zarządzającego budynkiem w przypadku podłożenia materiałów wybuchowych 98
14.3. Algorytm postępowania zarządzającego budynkiem w przypadku ataku masowego zabójcy 101
15. Komunikacja strategiczna 102
16. Podsumowanie 113
17. Materiały 115

„Kształtowanie kultury bezpieczeństwa poprzez budowanie świadomości antyterrorystycznej w społeczeństwie”

1 Dlaczego powstał ten poradnik?

Centrum Prewencji Terrorystycznej Agencji Bezpieczeństwa Wewnętrznego realizując swoją misję zwiększania świadomości antyterrorystycznej w społeczeństwie, dąży do **uczynienia Polski jeszcze bezpieczniejszym miejscem** w szybko zmieniającym się świecie. Obecnie Polska jest krajem bezpiecznym, a **poziom zagrożenia terrorystycznego** określany jest jako **niski**. Należy jednak pamiętać, że nawet niewielkie ryzyko ataku terrorystycznego nie oznacza, że takie zdarzenie nigdy nie wystąpi. Wystarczy jedna zradykalizowana osoba, która nie zostanie dostrzeżona i powstrzymana w odpowiednim czasie. Dlatego tak **ważnym elementem każdego systemu antyterrorystycznego jest społeczeństwo obywatelskie. Wysoka świadomość antyterrorystyczna obywateli zwiększa poziom bezpieczeństwa i wspiera wysiłki struktur państwowych w walce z terroryzmem.**



Terroryzm możemy definiować jako bezprawne użycie przemocy lub groźbę użycia przemocy przeciw osobom lub mieniu w celu zastraszenia danej grupy ludności lub całego państwa lub wymuszenia na nich określonej reakcji.

Aktualny stopień alarmowy obowiązujący na terytorium RP możesz sprawdzić pod adresem https://www.gov.pl/web/mswia/system-antyterrorystyczny-rp lub korzystając z kodu QR.

Pomimo niewielkiego prawdopodobieństwa wystąpienia zagrożenia, w ostatnich latach na terytorium RP doszło jednak do kilku incydentów o charakterze terrorystycznym. Polskie służby **zatrzymały kilka osób** pod zarzutem usiłowania popełnienia tego typu przestępstw. Dlatego też Agencja Bezpieczeństwa Wewnętrznego pragnie dołożyć wszelkich starań, aby w jak najbardziej skuteczny sposób **zapobiegać** i **reagować** na zagrożenia o charakterze terrorystycznym.

W tym celu konieczna jest **współpraca społeczeństwa** z instytucjami odpowiedzialnymi za bezpieczeństwo, ponieważ sprzyja ona kształtowaniu optymalnego **systemu antyterrorystycznego**.

Rolę wiodącą w zakresie zwiększania świadomości antyterrorystycznej w społeczeństwie odgrywa Agencja Bezpieczeństwa Wewnętrznego, a zwłaszcza powołane w 2018 roku **Centrum Prewencji Terrorystycznej ABW**.

Poradnik został opracowany w celu zwiększenia świadomości antyterrorystycznej obywateli Polski. Służy poszerzeniu **wiedzy** i podniesieniu **umiejętności** jego odbiorców w zakresie reagowania na zdarzenia o charakterze terrorystycznym, **zmniejszając** tym samym **ryzyko utraty zdrowia lub życia** w sytuacji zagrożenia. **Kształtuje** również pożądany proces współpracy społeczeństwa z instytucjami odpowiedzialnymi za bezpieczeństwo w Polsce oraz **wspiera** istniejący na terytorium RP system antyterrorystyczny.

Terroryzm jest zjawiskiem międzynarodowym i może stanowić zagrożenie nie tylko w kraju, lecz także **za granicą**. Wielu Polaków wyjeżdża na wakacje do Wielkiej Brytanii, Francji, Niemiec czy Hiszpanii, a przecież to właśnie tam dochodziło do najbardziej tragicznych zamachów ostatnich lat, które dotknęły Europę. Niestety, ofiarami niektórych z tych wydarzeń byli również obywatele Polski. Stąd też podstawowa wiedza w zakresie zapobiegania i reagowania na tego typu zdarzenia może okazać się przydatna nawet wtedy, gdy najmniej się tego spodziewamy.

Poradnik stanowi uzupełnienie dla dwudniowego szkolenia opracowanego w ramach unijnego projektu PO WER. Szkolenia realizowane przez CPT ABW składają się z 16 godzin specjalistycznych wykładów i ćwiczeń, omawiających zagadnienia związane z szeroko pojętą profilaktyką antyterrorystyczną, której elementy zostały zawarte w poradniku.

2 Czego dowiesz się z tego poradnika?

Materiały zawarte w poradniku pozwolą zrozumieć proces **radykalizacji** oraz przygotowań do ataku terrorystycznego **(mobilizacja)**. Wbrew ogólnemu przekonaniu przeprowadzenie zamachu w sposób spontaniczny nie jest zjawiskiem powszechnym. Ataki terrorystyczne są poprzedzone procesem radykalizacji danej osoby, która przyjmuje coraz bardziej skrajne poglądy, oraz fazą przygotowań, czyli opracowaniem planu zamachu i zebraniem potrzebnych środków.

Kształtowaniu kultury bezpieczeństwa służy m.in. wprowadzona przez Centrum Prewencji Terrorystycznej ABW Kampania Społeczna 4U! – Uważaj! Uciekaj! Ukryj się! Udaremnij atak!

4U UWAŻAJ UCIEKAJ UKRYJ SIĘ UDAREMNIJ ATAK !

Z kampanią 4U! możesz zapoznać się pod adresem www.4u.tpcoe.gov.pl lub wykorzystując kod QR.

W publikacji przedstawiono rekomendowane sposoby postępowania w przypadku wystąpienia ataku masowego zabójcy, na wypadek wykorzystania przez sprawców materiałów wybuchowych lub substancji chemicznych i biologicznych (tzw. niebezpieczna przesyłka). Zawarto w niej wskazówki, jak zachować się podczas sytuacji zakładniczej i tzw. szturmu ratunkowego, czyli działań jednostek kontrterrorystycznych. Omówiono zagadnienia związane z cyberbezpieczeństwem oraz przygotowaniem i zabezpieczeniem obiektów na wypadek wystąpienia zdarzenia o charakterze terrorystycznym. Scharakteryzowano pojęcie komunikacji strategicznej i wyjaśniono jej rolę w przeciwdziałaniu terroryzmowi. Przedstawiono również podstawy udzielania pierwszej pomocy w warunkach zagrożenia.

Niniejszy poradnik jest więc zbiorem praktycznych porad dotyczących szeroko pojętej prewencji terrorystycznej, a nie naukową rozprawą dotyczącą aspektów prawnych i psychologicznych.

W sytuacji zagrożenia trudno jest ocenić, czy ma ono związek z terroryzmem, czy jest raczej działaniem o charakterze kryminalnym. Będąc świadkiem aktu przemocy, podstawowym zadaniem jest ratowanie siebie i swoich bliskich.

3 Radykalizacja

**Nikt nie rodzi się terrorystą.
Terrorystą człowiek może się stać w wyniku procesu radykalizacji.**

Radykalizacja jest **procesem**, w którym osoba lub grupa pod wpływem różnych czynników przybiera coraz bardziej **skrajne poglądy** i zaczyna **akceptować wykorzystanie przemocy** w celu realizacji swoich zamiarów lub zamanifestowania swoich przekonań.

Prawo do wyrażania swojej opinii czy do demonstracji to jedno z podstawowych elementów demokracji. **Aktywizm** obejmuje wszelkie działania zmierzające do zmian społecznych i politycznych, które mieszczą się w granicach określonych przez prawo. Nie należy mylić go z **ekstremizmem**, który polega na hołdowaniu skrajnym poglądom i w najbardziej radykalnych przypadkach dopuszcza użycie **przemocy** oraz wykorzystanie **innych bezprawnych środków** (tzw. brutalny ekstremizm).

Radykalizująca się osoba może przyjmować coraz bardziej skrajne poglądy, a w dalszej kolejności uznać, że jedynym sposobem realizacji swoich zamiarów jest **terroryzm**. Motywacje mogą być różne – polityczne, religijne, ideologiczne albo osobiste, jednak czynnikiem wspólnym jest chęć **bezprawnego użycia siły lub przemocy** przeciw osobom lub mieniu w celu zastraszenia i (lub) wymuszenia określonej reakcji na danej grupie ludności lub całym państwie.

Jak przebiega proces radykalizacji?

Opinia/debata ▶ Aktywizm ▶ Ekstremizm ▶ Terroryzm

Rys. 1. Proces radykalizacji (opracowanie własne).

Nie istnieje jedna, zdefiniowana droga radykalizacji. Co więcej, każda osoba może radykalizować się z innych przyczyn, w inny sposób i w różnym czasie. Proces radykalizacji **może trwać miesiącami,** ale może nastąpić nawet w przeciągu **kilku dni** (np. pod wpływem traumatycznego wydarzenia). Poziom zradykalizowania danej osoby może się zmieniać, tj. może zarówno wzrastać, jak i maleć. Jeśli uda Ci się rozpoznać, że dana osoba się radykalizuje, powinieneś zareagować, dzięki czemu będzie można powstrzymać eskalację agresji.

Rys. 2. Etapy prowadzące do terroryzmu – opracowanie własne.

Zamachów terrorystycznych nie dokonują tylko osoby określane często przez opinię publiczną jako „chore psychicznie". Na decyzję o przeprowadzeniu zamachu może wpłynąć wiele różnych czynników, a sprawcą ataku może zostać osoba, która nie wyróżniała się wcześniej agresywnym zachowaniem. Niezależnie od tego, czy radykalizacja jest krótka i gwałtowna, czy też długofalowa, może prowadzić właśnie do terroryzmu.

Dlaczego ludzie się radykalizują?

Istnieje wiele dróg prowadzących do radykalizacji, m.in.: wykluczenie społeczne, polaryzacja, piętnowanie odmienności, teorie spiskowe, mowa i przestępstwa motywowane nienawiścią. Jednak **proces radykalizacji wygląda bardzo podobnie dla wszystkich form ekstremizmu**. Miejsce zamieszkania, sytuacja rodzinna czy doświadczenia z dzieciństwa i młodości to jedne z najważniejszych, ale nie jedyne czynniki.

Wybrane czynniki sprzyjające radykalizacji:

1. Indywidualne czynniki społeczno-psychologiczne:

- kryzys tożsamości;
- odczuwany żal;
- poczucie wykluczenia;
- poczucie niesprawiedliwości;
- poczucie upokorzenia;
- wiara w teorie spiskowe;
- poczucie bycia ofiarą.

2. Czynniki społeczne:

- marginalizacja;
- dyskryminacja;
- ograniczona mobilność społeczna;

- słaba edukacja;
- bezrobocie;
- przeszłość kryminalna.

3. **Czynniki polityczne:**
   - przeświadczenie o wojnie pomiędzy cywilizacjami;
   - dążenie do odłączenia się danego rejonu od państwa.

4. **Czynniki ideologiczne i religijne:**
   - wiara w przepowiednie o zbliżającej się apokalipsie;
   - poczucie, że wyznawana religia lub ideologia są zagrożone przez innych ludzi;
   - wiara w śmierć męczeńską podczas zamachu terrorystycznego.

5. **Czynniki kulturowe i problemy z identyfikacją:**
   - kulturowa marginalizacja;
   - poczucie braku przynależności.

6. **Traumatyczne wydarzenia:**
   - urazy doświadczone w dzieciństwie i w okresie dorosłości;
   - rozwód rodziców;
   - śmierć lub choroba członków rodziny oraz osób najbliższych.

Formy radykalizacji

Rozróżnia się trzy podstawowe formy radykalizacji:

Radykalizacja o podłożu politycznym charakteryzuje się przyjmowaniem skrajnych poglądów politycznych oraz agresją wobec innych grup społecznych i politycznych. Zazwyczaj dotyczy środowisk ekstremistycznych, wywodzących się ze skrajnej lewicy i skrajnej prawicy.

Posiadanie – nawet skrajnych – poglądów politycznych nie powinno być kojarzone z ekstremizmem. Za aktywność ekstremistyczną należy uznać wszelkiego rodzaju działalność legitymizującą przemoc lub mowę nienawiści, które są traktowane jako środek podważenia wartości demokratycznych lub obalenia rządów prawa.

Radykalizacja religijna jest oparta na politycznej interpretacji religii. Przybiera formę obrony przez stosowanie przemocy. Tożsamość religijna jest postrzegana jako obiekt ataku. Jedną z przyczyn współczesnych konfliktów na tle religijnym i terroryzmu motywowanego religijnie jest fundamentalizm.

Radykalizacja indywidualna, której podstawą może być pojedynczy problem. Do tej kategorii można zaliczyć również:

- radykalne grupy obrońców środowiska lub praw zwierząt;
- ruchy antyaborcyjne czy proaborcyjne, używające przemocy.

Sposoby radykalizacji

Trzy podstawowe sposoby radykalizacji, które mogą się uzupełniać i zachodzić jednocześnie:

- radykalizacja indywidualna;
- radykalizacja w grupie;
- radykalizacja przez lidera.

Radykalizacja indywidualna

Radykalizacja w grupie

Radykalizacja przez lidera

Katalizatory radykalizacji

Rola Internetu i mediów społecznościowych:

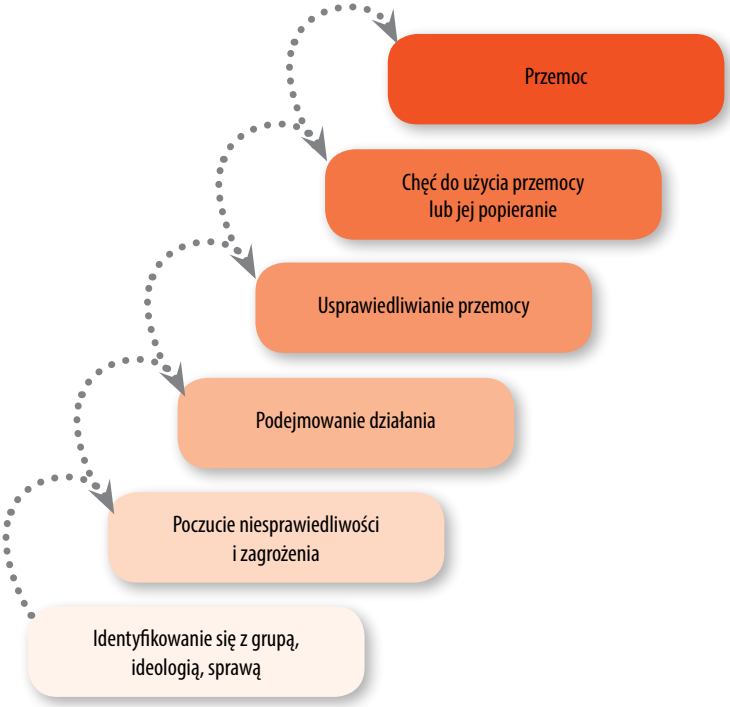
- łatwe nawiązywanie kontaktów z osobami o podobnych poglądach;
- wirtualna partycypacja – łatwiejsze dołączenie do wspólnoty;
- dostęp do radykalnych treści;
- możliwość rekrutacji do ugrupowania terrorystycznego;
- instrukcje zakupu broni lub wytworzenia materiałów wybuchowych.

Osoby radykalizujące:

- osoby nakłaniające do nienawiści i agresji;
- manipulatorzy;
- osoby wykorzystujące słabość innych;
- współwięźniowie.

Dynamika grupy:

- charyzmatyczny przywódca;
- więzi braterskie;
- myślenie grupowe;
- samoizolacja;
- elementy kontrkulturowe.



Rys. 3. Fazy radykalizacji (opracowanie własne).

Pamiętaj!

Na każdym etapie radykalizacji można zareagować przez działania prewencyjne, edukacyjne, przeciwdziałanie lub deradykalizację.

3.1. Jak rozpoznać radykalizację?

Zmiany w zachowaniu, takie jak: nagłe zerwanie długo budowanych relacji przy jednoczesnym nawiązaniu nowych znajomości, izolowanie się, rosnąca agresja i nietolerancja oraz nagły wzrost zaangażowania w nowe (nietypowe) zainteresowania, mogą świadczyć o gwałtownej radykalizacji danej osoby.

Rozpoznanie zmiany zachowania u osób z naszego otoczenia i zakwalifikowanie jej jako elementu procesu radykalizacji nie jest proste. Poniżej przedstawiono przykłady zachowań i podzielono je na kategorie, aby umożliwić poprawne identyfikowanie wskaźników radykalizacji. Jest to „Barometr Zachowań" przygotowany przez kanadyjskie Centrum Prewencji Radykalizacji Prowadzącej Do Przemocy (*Centre for the Prevention of Radicalization Leading to Violence*).

Więcej informacji nt. kanadyjskiego Centrum Prewencji Radykalizacji Prowadzącej Do Przemocy (Centre for the Prevention of Radicalization Leading to Violence) znajdziesz pod adresem https://info-radical.org/en/ lub wykorzystując kod QR.

Niegroźne zachowanie

Kategoria obejmuje różnorodne zachowania związane z zaangażowaniem politycznym, religijnym i wspólnotowym, które charakteryzują się pokojową formą i wykorzystaniem demokratycznych środków wyrazu. Jeżeli dana osoba zachowuje się w opisany poniżej sposób, nie powinno budzić to Twoich obaw.

- Kłóci się z bliskimi osobami aby bronić swoich racji i przekonań.
- Przyjmuje widoczne znaki (tradycyjne ubrania, długa broda, ogolona głowa, symbole religijne, określone tatuaże itp.), aby wyrazić swoją tożsamość lub poczucie przynależności do wybranej grupy.
- Jest aktywna w mediach społecznościowych.
- Zajmuje wyraźnie określone stanowisko i dyskutuje o sprawach związanych ze społecznością, daną grupą lub indywidualnymi osobami.

- Wyraża żywe zainteresowanie bieżącymi sprawami krajowymi i międzynarodowymi.
- Zwiększa swoje zaangażowanie w praktyki religijne lub w aktywność polityczną.
- Zmienia wyznanie lub nabiera nowe przekonania ideologiczne lub polityczne.
- Nalega na przestrzeganie określonej diety i innych zakazów wynikających z przekonań religijnych lub politycznych.
- Wyraża potrzebę doznania nowych wrażeń i przygód.
- Wyraża potrzebę walczenia z niesprawiedliwością.

Problematyczne zachowanie

Ta kategoria obejmuje zachowania, które świadczą o złym samopoczuciu danej osoby. Jeżeli zachowuje się ona w opisany poniżej sposób, to oznacza, że coraz mocniej utożsamia się z wybraną sprawą lub ideologią, co prowadzi do istotnych zmian w jej stylu życia.

- Wyraża spolaryzowane poglądy, których nie chce poddać pod dyskusję.
- Jej zachowanie zaczyna powodować konflikty w życiu rodzinnym.

- Fascynuje się teoriami spiskowymi i opowiada o nich.
- Zaczyna izolować się od rodziny i (lub) znajomych.
- Nagle zmienia swoje nawyki.
- Ma poczucie odrzucenia i bycia ofiarą.
- Uporczywie głosi swoje religijne lub polityczne przekonania.
- Odrzuca zasady obowiązujące w organizacji, z którą była związana (szkoła, praca, drużyna sportowa itp.).
- Odmawia udziału w zajęciach grupowych lub rezygnuje z kontaktów z innymi osobami z powodu: poglądów, rasy, koloru skóry, wyznania lub płci.
- Wyraża potrzebę dominacji lub kontroli nad innymi osobami.
- Nie chce zmienić swoich poglądów i uznać innych punktów widzenia.

Niepokojące zachowanie

Kategoria obejmuje zachowania, które można wiązać z początkiem zaangażowania danej osoby w radykalną działalność. Charakteryzuje się dużą nieufnością do świata zewnętrznego oraz przewagą poglądów legitymizujących użycie przemocy do osiągnięcia własnych celów.

- Całkowicie zrywa więzi z rodziną i (lub) znajomymi oraz utrzymuje relacje wyłącznie z nowo poznanymi osobami.
- Usprawiedliwia użycie przemocy w celu obrony sprawy lub ideologii.
- Ukrywa nowy styl życia lub system wartości przed członkami rodziny i bliskimi.
- Nawiązuje relacje z osobami lub grupami o poglądach ekstremistycznych.
- Nagle traci zainteresowanie szkołą lub pracą.
- Używa symboli i znaków związanych z ekstremistycznymi ugrupowaniami.
- Wierzy w nagły koniec świata, męczeństwo lub inne mesjanistyczne wizje.
- Wyraża nienawiść wobec innych osób lub grup.

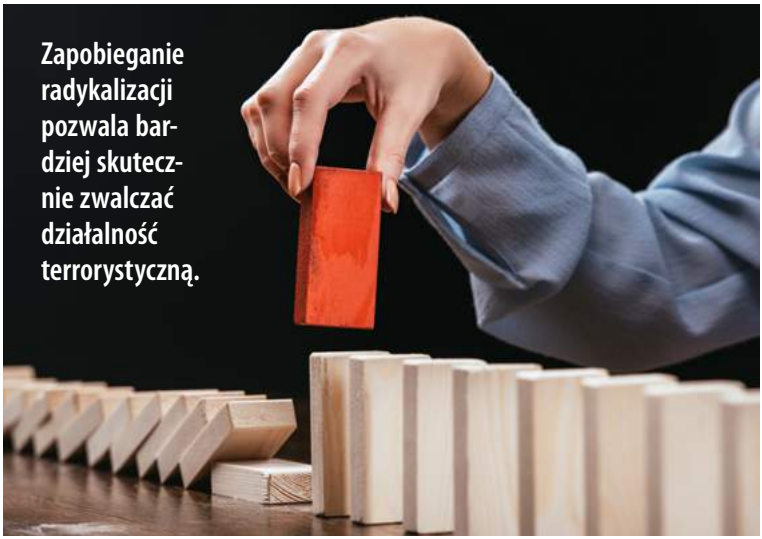
Alarmujące zachowanie

Ta kategoria obejmuje zachowania świadczące o niezwykle silnym przywiązaniu danej osoby do ideologii lub sprawy, które doprowadziło ją do przekonania, że przemoc jest jedynym możliwym i skutecznym środkiem działania.

- Bierze udział w działaniach grupy ekstremistycznej (materialnie, finansowo lub fizycznie).
- Rekrutuje lub namawia osoby do przyłączenia się do grupy ekstremistycznej lub ekstremistycznego przedsięwzięcia.

- Kontaktuje się z grupami lub osobami znanymi ze skrajnych poglądów (również przez Internet).
- Wzmacnia swoje przekonania przez odwiedzanie radykalnych stron i forów internetowych.
- Planuje lub popełnia akty przemocy inspirowane radykalnymi poglądami.
- Interesuje się bronią i (lub) materiałami wybuchowymi, bezprawnie stara się je nabyć lub uczy się nimi posługiwać.
- Planuje podróż do strefy konfliktu lub regionu, w którym aktywne są grupy ekstremistyczne lub terrorystyczne.

3.2. Jak przeciwdziałać radykalizacji?



Jeżeli osoba wykazuje zachowania opisane w trzech pierwszych kategoriach „Barometru Zachowań", to zarówno Twoje zachowanie, jak i jej najbliższego otoczenia odgrywa bardzo ważną rolę. Jeśli istnieje taka możliwość, spróbuj zniechęcić ją od popadania w skrajności przez perswazję, a także zaangażuj jej najbliższych do tego zadania. Podstawą jest zrozumienie osobistych problemów i punktu widzenia radykalizującej się osoby oraz przedstawienie jej alternatywnych sposobów rozwiązania sytuacji. Nie wdawaj się w spory i nie wyśmiewaj jej poglądów, gdyż może to tylko utwierdzić tę osobę w swoich przekonaniach i przyśpieszyć radykalizację.

Interakcja z osobą podatną na radykalizację:

- **okaż szacunek i empatię;**
- **słuchaj bez uprzedzeń;**
- **unikaj kwestionowania wartości i przekonań;**

- **wybierz właściwy czas i miejsce;**
- **zachowaj czujność;**
- **jeśli nie wiesz co zrobić - uzyskaj pomoc (np. psychologa).**

Skrajne poglądy wynikają często z niewiedzy i nieznajomości innych rozwiązań. Nie ma jednego sposobu na zatrzymanie lub odwrócenie procesu radykalizacji, jednak najgorsze co możemy zrobić, to zignorować problem i nie podjąć żadnych działań.

Jeśli jednak osoba przejawia zachowanie opisane w **kategorii zachowań alarmujących** - **poinformuj służby!** Świadczy ono o bardzo zaawansowanej radykalizacji, która może skłonić osobę do popełnienia aktu przemocy. **Twoja właściwa reakcja może uratować życie!**

Werbalizacja chęci dokonania ataku może pojawić się już na etapie radykalizacji, przygotowań do ataku lub tuż przed przeprowadzeniem samego ataku. Jeżeli zachowanie i inne czynniki wskazują na radykalizację danej osoby, a ta **sugeruje** chęć zabicia danej osoby (osób) lub dokonania innego czynu o charakterze terrorystycznym lub kryminalnym, bądź na ten temat **żartuje, nie lekceważ tego typu komunikatów – zadzwoń pod numer 112!**

Analiza zamachów terrorystycznych, które miały miejsce w ostatnich latach w Europie wykazała, że niektórzy ze sprawców informowali członków swojej najbliższej rodziny lub znajomych o chęci przeprowadzenia ataku lub wręcz namawiali ich do współpracy. Niestety, te zachowania były często bagatelizowane. Bliskie osoby nie chciały też przekazywać informacji o zagrożeniu ze strachu przed potencjalnymi konsekwencjami oraz dla ochrony swoich najbliższych.

Kwestią kluczową jest umiejętność rozpoznawania postępującego procesu radykalizacji i odpowiedniego reagowania w celu udaremnienia potencjalnego zagrożenia.

4 Mobilizacja

Gdy dana osoba lub grupa **podejmuje decyzję o przeprowadzeniu zamachu terrorystycznego** – następuje faza **mobilizacji.** Polega ona na przygotowywaniu się do popełnienia aktu przemocy. Zrozumienie tego procesu pozwala na lepszą identyfikację podejrzanych zachowań, a przez to daje możliwość udaremnienia ataku na etapie jego przygotowania.

Mobilizacja jest więc kolejną (po radykalizacji) fazą poprzedzającą zamach terrorystyczny. Najbardziej spektakularne i najniebez-

pieczniejsze ataki terrorystyczne wymagają długich przygotowań oraz – niekiedy – kontaktu z innymi osobami i ich wsparcia.

Wysoka świadomość społeczna pozwoli wykryć tego rodzaju przygotowania oraz wpłynie pośrednio na sprawców. Potencjalni terroryści mogą odstąpić od prób zdobycia broni palnej czy materiałów wybuchowych w obawie przed dekonspiracją planów.

Fazę mobilizacji cechują trzy podstawowe czynniki:

Intencje danej osoby do przeprowadzenia aktu przemocy. Na intencje mogą wpływać, np. wydarzenia polityczne, które motywują zradykalizowaną osobę do przeprowadzenia zamachu terrorystycznego.

Możliwości realizacyjne – dostęp do specjalnych narzędzi i przedmiotów, takich jak: broń palna, materiały wybuchowe oraz środki chemiczne lub biologiczne.

Sprawcy zamachu terrorystycznego, którego skutkiem ma być jak największa liczba ofiar, najczęściej będą się starali pozyskać broń palną lub materiały wybuchowe. Zamachy terrorystyczne z wykorzystaniem tych środków są bardzo dotkliwe w skutkach. Jednak pozyskanie odpowiednich narzędzi wymaga m.in. czasu, odpowiedniej wiedzy i znajomości. Przygotowania tego rodzaju ataku są trudne i znacznie zwiększają ryzyko wykrycia przez **służby** lub **obywateli**.

Zdolności – wykształcenie i specjalistyczna wiedza danej osoby. Zamach może być spontaniczny, czyli dokonany przy wykorzystaniu prostych narzędzi, bądź przeprowadzony np. z użyciem materiałów wybuchowych. W tego typu przypadku osoba musi opanować wiedzę z zakresu ich wytwarzania, co również może zostać zaobserwowane przez otoczenie.

Jak rozpoznać proces mobilizacji do ataku?

Poniżej prezentujemy przykłady zdarzeń mogących wskazywać na przygotowania do przeprowadzenia zamachu terrorystycznego. Jeżeli dany czyn lub aktywność **nie jest zagrożona karą**, to poniższy katalog jest jedynie **zbiorem wskazówek**, które należy odpowiednio zinterpretować w szerszym kontekście.

Samo posiadanie niektórych przedmiotów lub nietypowe zainteresowania nie muszą być powodem do obaw. Jeżeli jednak na podstawie poniższych informacji i **odpowiedniej interpretacji kontekstu całej sytuacji** uznasz, że dana osoba może przygotowywać się do aktu przemocy – poinformuj służby. Pamiętaj, że powiadomienie Policji nie będzie dla Ciebie źródłem problemów i nieprzyjemności. Jeśli sygnalizowane obawy będą zasadne, służby podejmą odpowiednie działania.

Gromadzenie materiałów wybuchowych

Jeżeli dana osoba gromadzi materiały wybuchowe przez:

- nielegalny zakup;
- wykopywanie niewybuchów;
- pozyskiwanie dużej ilości prochu z fajerwerków;
- kradzież,

… to nie zostawiaj takiej informacji dla siebie – **poinformuj służby!**

Wytwarzanie materiałów wybuchowych

Osoby niemające kontaktu z materiałami wybuchowymi oraz niedysponujące specjalistyczną wiedzą na ten temat będą musiały zdobyć niezbędne w tym zakresie informacje. Jeżeli dana osoba stara się pozyskać tego typu wiedzę i można to powiązać z innymi niepokojącymi informacjami – **należy poinformować służby!**

Prekursory materiałów wybuchowych to substancje, które mogą posłużyć do produkcji tych materiałów. Część prekursorów to substancje ogólnodostępne w naszym codziennym życiu, a ich posiadanie jest w pełni legalne.

Więcej informacji na temat prekursorów materiałów wybuchowych znajdziesz na stronie internetowej Komendy Głównej Policji w zakładce: „Krajowy Punkt Kontaktowy ds. prekursorów materiałów wybuchowych".

http://bip.kgp.policja.gov.pl/kgp/krajowy-punkt-kontaktow/23519,Krajowy-Punkt-Kontaktowy-ds-prekursorow-materialow-wybuchowych.html

Czy dana osoba kupuje substancje, które wydają się niepotrzebne w jej normalnym życiu i budzi to uzasadnione obawy?

Przykłady podejrzanych środków:

- **Urotropina**

- **Kwas siarkowy**

- **Aceton**

- **Azotan amonu (saletra amonowa)**

Czy dana osoba prowadzi testy z użyciem substancji chemicznych?

Czy posiada przedmioty rzadko używane w gospodarstwie domowym, np.: nietypowy sprzęt lub aparatura chemiczna, której obecności nie da się wytłumaczyć w racjonalny sposób? Jeżeli wydaje się to podejrzane – **poinformuj służby pod numerem alarmowym 112!**

Elementy wskazujące na tworzenie improwizowanych ładunków wybuchowych:

- **Detonatory**: wszystkie elementy wytwarzające łuk elektryczny, podłączone przewodami do baterii wraz z urządzeniami, takimi jak budzik czy telefon komórkowy.
- **Elementy korpusu urządzeń wybuchowych**, których zadaniem jest zwiększenie ciśnienia, takie jak: rury stalowe i szybkowary. Przy większych urządzeniach wybuchowych będą to np.: kanistry i beczki.
- **Elementy wzmacniające siłę oddziaływania bomby** w postaci: stożków miedzianych, gwoździ i śrub stalowych.

Jeżeli dana osoba posiada wymienione przedmioty oraz jeśli istnieje ryzyko, że ma dostęp do materiałów wybuchowych – poinformuj służby!

Rys. 4. Schemat bomby rurowej

Broń palna i sprzęt wojskowy

- Czy dana osoba posiada broń palną bez pozwolenia bądź stara się ją pozyskać?
- Czy posiada amunicję lub próbuje ją nielegalnie pozyskać?

Jeżeli wiesz o tego typu sytuacji – poinformuj służby!

- Czy dana osoba posiada kamizelki kuloodporne, wojskowy sprzęt taktyczny oraz inne przedmioty, które są stosowane w formacjach mundurowych o charakterze zbrojnym?
- Czy dana osoba posiada broń czarnoprochową, łuki, noże bojowe lub inne tego typu niebezpieczne przedmioty?

Nawet jeśli posiadanie tego rodzaju przedmiotów jest legalne, ale **nie pasują do stylu** życia danej osoby i wraz z innymi przesłankami budzą wątpliwości – **poinformuj służby!**

Substancje chemiczne i związki biologiczne

- Czy dana osoba posiada znaczne ilości substancji chemicznych lub biologicznych, ale nie jest to zgodne z jej stylem życia i wraz z innymi przesłankami budzi to uzasadnione wątpliwości?
- Czy dana osoba prowadzi działania zmierzające do pozyskania niebezpiecznych substancji chemicznych i związków biologicznych?
- Czy dana osoba kupuje substancje chemiczne, sprzęt laboratoryjny oraz inne przedmioty, co jednak nie odpowiada stylowi jej życia i wraz z innymi przesłankami budzi to wątpliwości?

Jeżeli wiesz o tego typu sytuacjach – poinformuj służby!

Ataki terrorystyczne mogą zostać przeprowadzone również przy użyciu ogólnodostępnych narzędzi, takich jak noże czy samochody. Tego rodzaju ataki nie wymagają szczegółowego planowania i przygotowań. Najważniejszą kwestią jest w tym przypadku wykrycie potencjalnego sprawcy **na etapie jego radykalizacji,** ponieważ od momentu podjęcia decyzji o ataku do jego przeprowadzenia może minąć bardzo mało czasu.

Indywidualne doświadczenie życiowe pozwala rozpoznać odstępstwo od normy w miejscu pracy, zamieszkania czy też wśród bliskich. Dlatego **każdy** może **rozpoznać fazę mobilizacji** do aktu przemocy i **zapobiec potencjalnej tragedii.**

5 Formy zdarzenia o charakterze terrorystycznym

Zgodnie z Ustawą z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych oraz Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 22 lipca 2016 r. w sprawie katalogu incydentów o charakterze terrorystycznym, wyróżniamy cztery podstawowe formy zdarzenia o charakterze terrorystycznym.

Rys. 5. Obszary zagrożeń różniące się nie tylko różnymi sposobami działania sprawców, lecz także metodami przeciwdziałania i reagowania na zdarzenia

Urządzenia i materiały wybuchowe

Sprawca dążąc do zabicia jak największej ilości osób lub zniszczenia wybranego obiektu, wykorzystuje materiały wybuchowe. Cel ataku może mieć również charakter symboliczny. Najbardziej narażone na tego typu ataki są ciągi komunikacyjne, wydarzenia publiczne (koncerty, manifestacje, uroczystości itp.) oraz miejsca i budynki użyteczności publicznej, w których może przebywać wiele osób.

Atak bombowy może zostać przeprowadzony przez zamachowca samobójcę lub przez pozostawienie ładunku w miejscu publicznym (np. ukrycie go w samochodzie, plecaku czy torbie). Możliwe jest również dostarczenie ładunku wybuchowego z wykorzystaniem bezzałogowych systemów latających (dronów). Co istotne, sprawca może dysponować więcej niż jednym ładunkiem wybuchowym, dlatego też **nigdy nie można wykluczyć kolejnych eksplozji** w tym samym czasie i miejscu.

Uzbrojony sprawca – „masowy zabójca” i sytuacja zakładnicza

Jedną z najniebezpieczniejszych form zdarzenia o charakterze terrorystycznym jest działanie uzbrojonego sprawcy. Najczęściej przybiera ono formę ataku tzw. masowego zabójcy lub sytuacji zakładniczej. Atak masowego zabójcy może przerodzić się w sytuację zakładniczą (i odwrotnie).

Atak „masowego zabójcy” (ang.: *active shooter*)

Mianem „masowego zabójcy” określa się osobę, która dokonuje ataku terrorystycznego przy użyciu niebezpiecznego narzędzia,

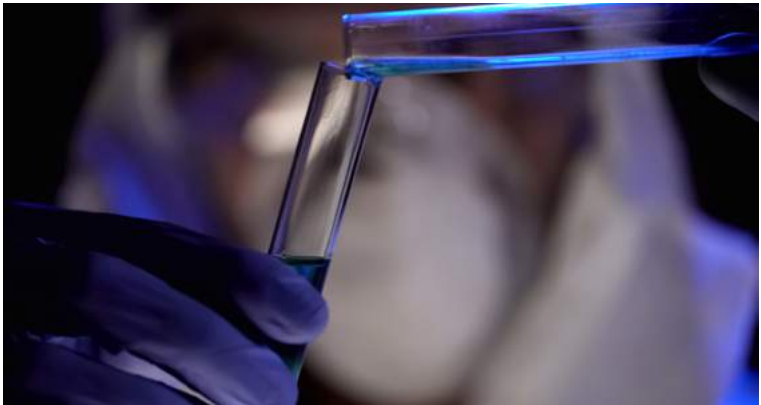
broni palnej lub pojazdu, a jej celem jest zabicie jak największej liczby osób. Masowy zabójca **nie bierze zakładników,** tylko zabija wszystkie napotkane osoby i **eliminuje rannych**. Zdarzenie tego typu jest bardzo dynamiczne i nieprzewidywalne w skutkach. Odpowiednia reakcja ofiar i osób postronnych oraz szybkie powiadomienie Policji są kluczowe w celu zminimalizowania liczby ofiar i jak najszybszego zneutralizowania napastnika.

Wzięcie zakładników

Konsekwencją działań masowego zabójcy może być sytuacja zakładnicza. Jest to zdarzenie, podczas którego napastnik przetrzymuje osoby z narażeniem ich życia i zdrowia w celu uzyskania korzyści, wymuszenia jakiejś decyzji lub zachowania. **Co do zasady** celem porywacza **nie jest zabijanie** zakładników, ponieważ są oni jego „argumentem" w negocjacjach z Policją.

Czynniki skażenia

Do katalogu zdarzeń o charakterze terrorystycznym zalicza się również wykorzystanie substancji (lub broni) chemicznych, biologicznych, radiacyjnych i nuklearnych (CBRN). Ich niekontrolowane rozprzestrzenianie grozi zaistnieniem zagrożenia dla zdrowia lub życia



osób oraz mienia i środowiska naturalnego na danym terenie. Najpopularniejszą formą ataku terrorystycznego przy wykorzystaniu czynników skażenia jest przesłanie ich za pomocą przesyłki pocztowej.

Cyberterroryzm

Sprawcy przestępstw o charakterze terrorystycznym wykorzystują do swoich celów również najnowsze technologie. Mianem „cyberterroryzmu" można określić takie działania, jak: ataki hakerskie, kradzież danych, infekowanie stron internetowych i systemów w celu uzyskania środków finansowych na działalność terrorystyczną, m.in. przeprowadzanie ataków, a także prowadzenie działań propagandowych i radykalizacyjnych.

6 Procedura 4U!

Zasada 4U!, czyli algorytm postępowania w przypadku wystąpienia zdarzenia o charakterze terrorystycznym.

Centrum Prewencji Terrorystycznej ABW opracowało procedurę rekomendowanego sposobu postępowania w przypadku wystąpienia ataku terrorystycznego – zamachu bombowego i ataku masowego zabójcy. Procedura jest sekwencją czterech kroków, które należy stosować w ściśle określonej kolejności.

po 1 UWAŻAJ

Pierwsze „U", czyli – uważaj! stosuj już na etapie radykalizacji i mobilizacji, które zostały opisane w poprzednich rozdziałach. Zwracaj uwagę na wszystkie nienaturalne (odbiegające od normy i kontekstu) zdarzenia i zachowania osób. Jeśli coś wzbudzi Twoje podejrzenie, nie bój się zadzwonić pod numer 112.

po 2 UCIEKAJ

Jeśli usłyszysz wybuch lub strzały albo dojdzie do innego aktu przemocy (np. ataku nożem) w pierwszej kolejności – jeśli masz taką możliwość – uciekaj! Najlepszą metodą reakcji na wszelkiego rodzaju niebezpieczeństwo jest oddalenie się w bezpieczne miejsce i powiadomienie służb pod numerem ratunkowym 112.

po 3 UKRYJ SIĘ

Jeśli ucieczka nie jest możliwa lub jest zbyt niebezpieczna, ukryj się! Jeżeli jesteś w budynku, postaraj się schować w pomieszczeniu, które można zamknąć.

po 4 UDAREMNIJ ATAK

Jeżeli ucieczka lub ukrycie się nie są możliwe, a konfrontacja z napastnikiem jest nieunikniona, masz prawo się bronić! Zgodnie z art. 25. Kodeksu karnego: Nie popełnia przestępstwa, kto w obronie koniecznej odpiera bezpośredni, bezprawny zamach na jakiekolwiek dobro chronione prawem.

Na bazie procedury powstała kampania społeczna 4U!

4U UWAŻAJ UCIEKAJ UKRYJ SIĘ UDAREMNIJ ATAK !

Zachęcamy do zapoznania się z kampanią pod adresem: www.4u.tpcoe.gov.pl lub wykorzystując kod QR

W następnych rozdziałach zaprezentowano wykorzystanie procedury 4U! w przypadku zagrożeń związanych z materiałami wybuchowymi, niebezpiecznymi przesyłkami oraz atakiem masowego zabójcy.

7 Urządzenia i materiały wybuchowe

7.1. Niebezpieczny przedmiot

Pozostawiony bez opieki bagaż lub torba to najprawdopodobniej skutek zapominalstwa właściciela przedmiotu. **Nie można** jednak **nigdy bagatelizować** tego rodzaju pozostawionych bez opieki rzeczy, szczególnie gdy znajdują się w nietypowym miejscu. Nie podchodź i nie dotykaj takiego pakunku. Najpierw zapytaj osoby w pobliżu, czy wiedzą do kogo należy pozostawiony przedmiot. Jeśli właściciel się nie znajdzie lub nie masz kogo zapytać – bezzwłocznie poinformuj ochronę (jeśli jest taka możliwość) i (lub) zadzwoń pod numer alarmowy **112.**

po 1 UWAŻAJ

- Nie pozostawiaj bagażu bez opieki!
- Każdy pozostawiony bez opieki nietypowy przedmiot uznaj za podejrzany
- Nie bagatelizuj zagrożenia bombowego

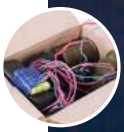
Gdy w pozostawionym bez kontroli plecaku lub torbie zauważysz:

Groźbę werbalną

Napis „bomba”, ikonę wybuchu, napisaną nazwę materiału wybuchowego.

Instalację z drutu

Instalację kablową, antenową umieszczoną na pojemnikach, pudełkach, rurach, wystającą z plecaka, torby, walizki.



Instalację elektroniczną

Instalację elektroniczną widoczną na zewnątrz lub wewnątrz opakowania.

Poczujesz intensywny zapach

Wydostający się z opakowania dym czy opar powiązany z intensywnym zapachem substancji chemicznej.

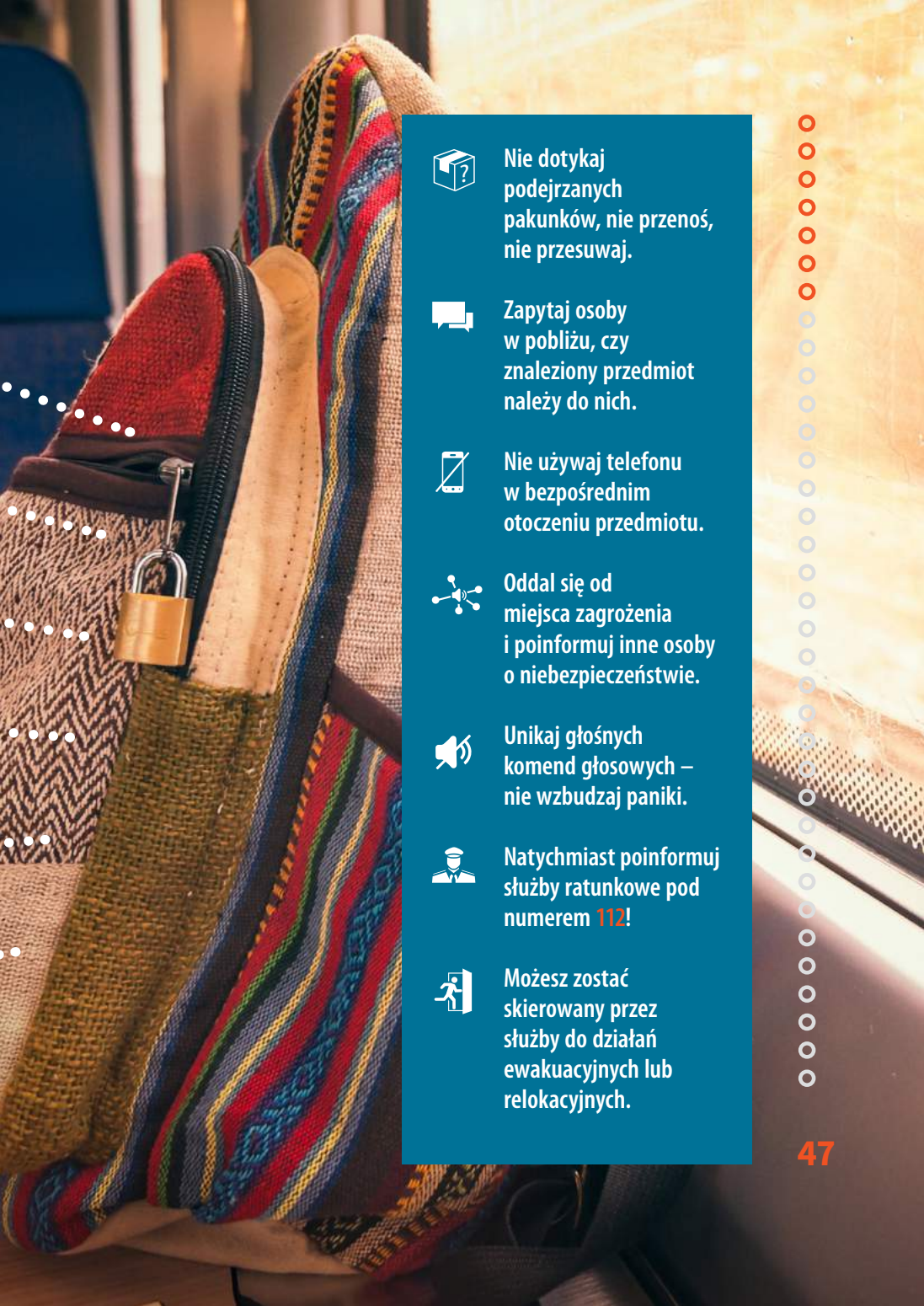
Kumulację przedmiotów

Przedmioty mogące stanowić odłamki – gwoździe, śruby, nakrętki, metalowe kulki, preparowany korpus metalowy.

Elementy lub całe egzemplarze

Elementy amunicji, granatu, pocisku, lub całe egzemplarze.

możesz mieć kontakt z urządzeniem wybuchowym!



Nie dotykaj podejrzanych pakunków, nie przenoś, nie przesuwaj.

Zapytaj osoby w pobliżu, czy znaleziony przedmiot należy do nich.

Nie używaj telefonu w bezpośrednim otoczeniu przedmiotu.

Oddal się od miejsca zagrożenia i poinformuj inne osoby o niebezpieczeństwie.

Unikaj głośnych komend głosowych – nie wzbudzaj paniki.

Natychmiast poinformuj służby ratunkowe pod numerem 112!

Możesz zostać skierowany przez służby do działań ewakuacyjnych lub relokacyjnych.

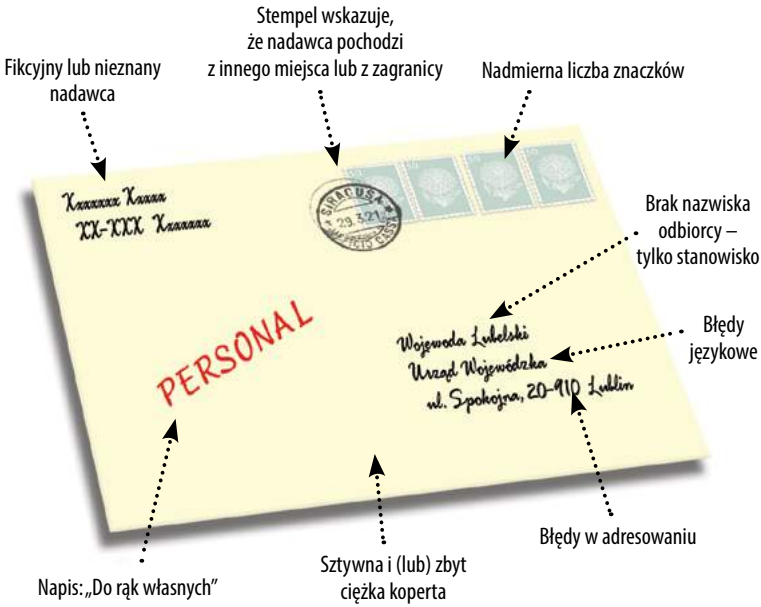
7.2. Podejrzana przesyłka

Pracownicy urzędów i innych instytucji państwowych mogą być narażeni na ataki terrorystyczne przy wykorzystaniu niebezpiecznych przesyłek zawierających materiały wybuchowe, środki chemiczne lub biologiczne. Sprawcy chcą w ten sposób (najczęściej zachowując anonimowość) uderzyć w organy władzy państwowej, zdestabilizować pracę danej instytucji lub bezpośrednio zaatakować konkretną osobę.

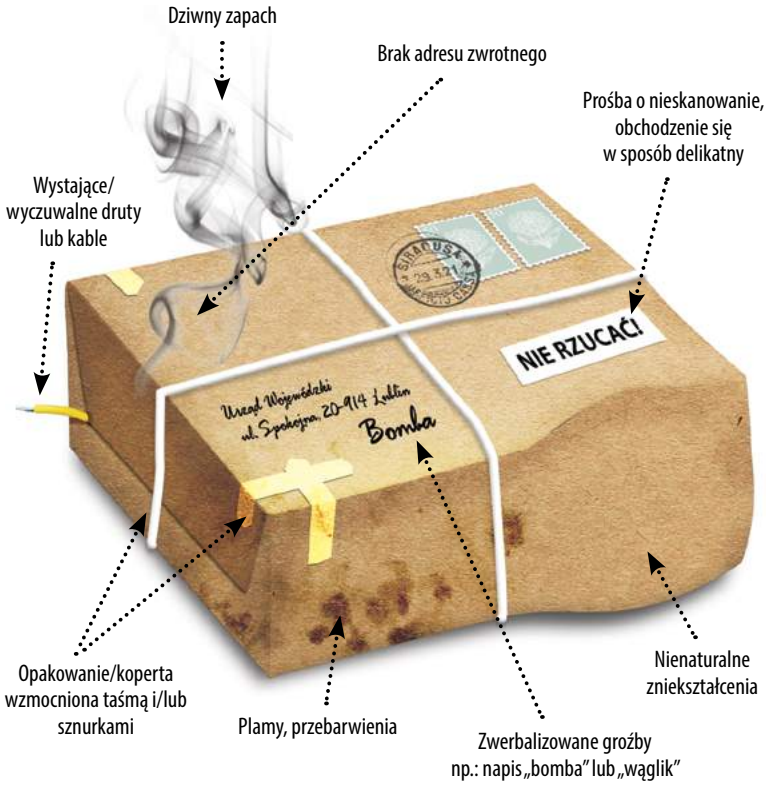
Najlepszym rozwiązaniem, które mogłoby znacznie zwiększyć możliwość wykrycia tego rodzaju niebezpieczeństwa, jest wdrożenie systemu kontroli wszystkich przesyłek trafiających do danej instytucji. Jednak nawet niewielkie nakłady finansowe i **właściwe przygotowanie personelu** pozwala znacznie ograniczyć podatność na tego rodzaju zagrożenia.

Pamiętaj, że po ogłoszeniu stopnia alarmowego BRAVO powstaje obowiązek kontroli wszystkich przesyłek wchodzących do urzędu lub instytucji.

Cechy świadczące o tym, że przesyłka może być niebezpieczna:



- **Nie otwieraj jej, nie dotykaj, nie przenoś!**
- **Bezzwłocznie zadzwoń pod numer alarmowy 112 i przekaż wszelkie szczegóły związane z przesyłką.**
- **Odizoluj pomieszczenie (w przypadku urządzenia wybuchowego – otwórz okna i drzwi, w przypadku – CBRN - zamknij okna i drzwi, wyłącz klimatyzację).**
- **Sporządź listę osób, które miały kontakt z przesyłką (odizoluj je).**
- **Współpracuj ze służbami, które przybędą na miejsce.**



Pozostaw przesyłkę delikatnie na płaskiej powierzchni.

Nie naruszaj jej zawartości – nie rozsypuj, nie przenoś, nie próbuj!

Jeżeli przesyłka może zawierać środki CBRN – delikatnie ją zakryj (np.: workiem na śmieci, marynarką).

W przypadku zagrożenia CBRN – staraj się nie przemieszczać po budynku, umyj ręce wodą np. z butelki lub czajnika.

8 Uzbrojony sprawca

po 1 UWAŻAJ

Masowy zabójca
(active shooter)

- Zabicie jak największej ilości osób
- Dobija rannych
- Zdesperowany

Sytuacja zakładnicza

- Korzyść majątkowa, polityczna lub społeczna
- Głównym celem nie jest zabijanie
- Nie atakuje osób bez powodu

Najbardziej „popularne” typy broni palnej

Uzbrojony w broń palną sprawca będzie najprawdopodobniej posługiwał się jednym z zaprezentowanych typów broni. Ich znajomość pozwoli na lepszą reakcję na dane zdarzenie i dokładniejsze poinformowanie Policji.

Pistolet

- Najczęściej 14-17 kul w magazynku
- Skuteczny zasięg – do 25 m.
- Możliwość zacięcia

Ogień pojedynczy

Rewolwer

- Najczęściej 6 kul w magazynku
- Skuteczny zasięg – do 25 m.
- Niemal niezawodny

Ogień pojedynczy

Strzelba

- Najczęściej kilka kul w magazynku
- Skuteczny zasięg – kilka metrów
- Duża siła i rozrzut pocisków

Ogień pojedynczy

Karabin i karabinek

- Najczęściej 30 kul w magazynku
- Skuteczny zasięg – nawet 400 m.
- Duża szybkostrzelność
- Amunicja karabinowa – duży kaliber

Ogień ciągły - serie

Pistolet maszynowy

- Najczęściej 30 kul w magazynku
- Skuteczny zasięg – ok 150 m.
- Duża szybkostrzelność
- Amunicja pistoletowa

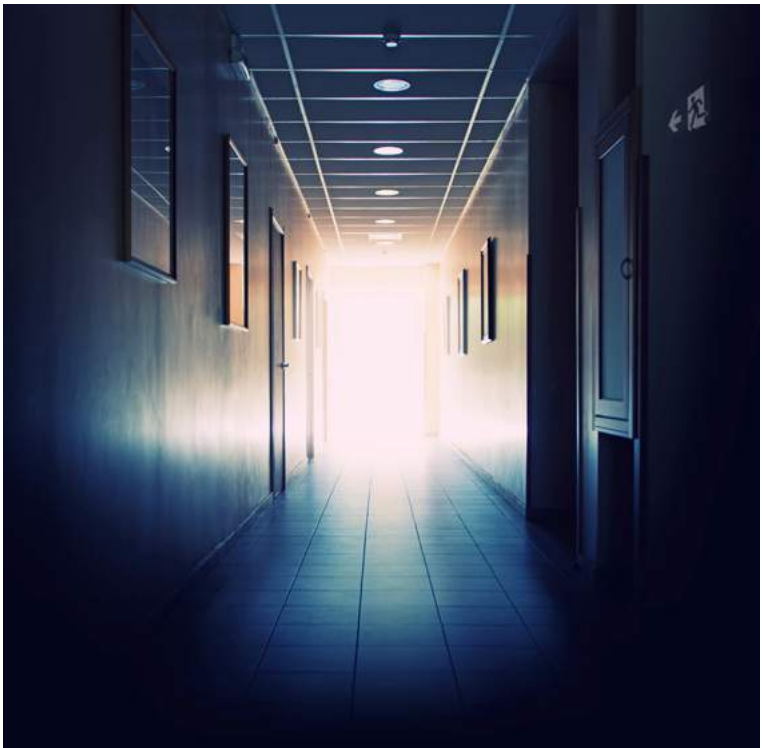
Ogień ciągły - serie

8.1. Atak masowego zabójcy

po 2 UCIEKAJ

Jeśli usłyszysz wybuch lub strzały albo dojdzie do innego aktu przemocy (np. ataku nożem), **w pierwszej kolejności** – jeśli masz taką możliwość – **uciekaj!** Najlepszą metodą reakcji na **wszelkiego rodzaju niebezpieczeństwo** jest oddalenie się w bezpieczne miejsce i powiadomienie służb **pod numerem ratunkowym 112**.

Staraj się uciec jak najszybciej i jak najdalej od miejsca zagrożenia. Pozostaw zbędne rzeczy, które opóźniłyby ucieczkę i nie wracaj na miejsce zdarzenia. Informuj mijane osoby o zagrożeniu, ale nie trać czasu na ich przekonywanie o konieczności ucieczki. Ewakuuj się niezależnie od decyzji innych. Gdy tylko będziesz bezpieczny, zadzwoń pod numer alarmowy.



Jeśli jesteś w bezpośrednim niebezpieczeństwie – przyjmij pozycję leżącą.

Oceń sytuację - opracuj opcję działania.

Uciekaj! - zagrożenie jest realne, napastnik cię nie widzi, istnieje bezpieczna trasa ucieczki.

Uciekaj na odległość pozwalającą na spokojną ocenę i podjęcie dalszych decyzji.

Informuj o zagrożeniu wewnątrz, wyciągaj ludzi na zewnątrz.

Uciekaj szybko, nie zabieraj żadnych rzeczy osobistych.

Jeśli są ranni – pomóż im WYJŚĆ ALBO SCHOWAĆ SIĘ.

Jeśli bardzo opóźni to ewakuację – pozostaw rannych na miejscu.

Jak tylko będziesz bezpieczny – zadzwoń pod numer 112.

Telefon służy do wzywania pomocy, a nie do rejestracji zdarzeń!

po 3 UKRYJ SIĘ

Jeśli ucieczka nie jest możliwa lub jest zbyt niebezpieczna, **ukryj się!** Jeżeli jesteś w budynku, postaraj się ukryć w pomieszczeniu, które można zamknąć.

Kiedy powinieneś zamknąć i zabarykadować drzwi do pomieszczenia, w którym się znajdujesz:

- jeżeli otrzymałeś taki komunikat i tak wskazują procedury w obiekcie,
- jeżeli w Twojej ocenie ucieczka prowadziłaby do konfrontacji z napastnikiem,
- jeżeli nie jesteś w stanie z innych przyczyn wydostać się w sposób bezpieczny z budynku.

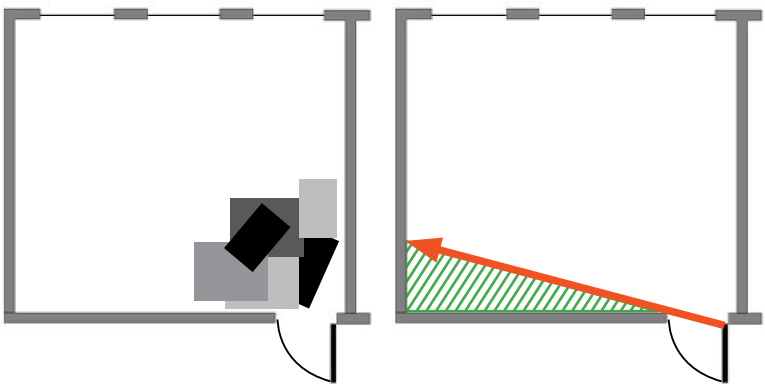
Zamknij drzwi na klucz. Zabarykaduj drzwi meblami lub ciężkimi przedmiotami. Odsuń się od drzwi i okien, tak aby nie było Cię widać z zewnątrz oraz aby ewentualny strzał przez drzwi stanowił dla Ciebie jak najmniejsze zagrożenie. Wycisz dzwonek w telefonie i wygaś jego wyświetlacz. Wyłącz światło w pomieszczeniu, unikaj przemieszczania się oraz staraj się zachować bezwzględną ciszę.

Jeśli:

- nie wiesz, gdzie jest napastnik albo nie jesteś tego pewien,
- napastnik jest w pobliżu, a ucieczka byłaby zbyt niebezpieczna

po 3 UKRYJ SIĘ

- Zamknij pomieszczenie, w którym przebywasz.
- Zabarykaduj drzwi, schowaj się w pomieszczeniu dodatkowym.
- Zgaś światło i zasłoń okna.



Rys. 6. Barykadowanie pomieszczenia

- Jeżeli to możliwe - wyłącz gaz, urządzenia elektryczne.
- Znajdź osłonę, nie wyglądaj przez okna i drzwi.
- Wycisz telefon, nie kontaktuj się z rodziną.
- Nie krzycz, nie panikuj, nie poruszaj się – zachowaj ciszę.
- Jeżeli kryjówka to umożliwia - powiadom służby ratunkowe.

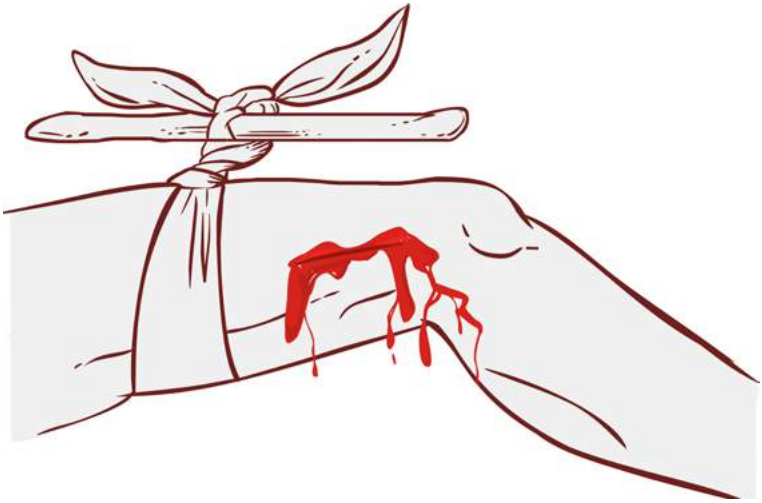
W miarę potrzeby staraj się uspokoić i uciszyć panikujące osoby. Napastnik najprawdopodobniej nie będzie chciał forsować zamkniętych drzwi, jeśli uzna, że pomieszczenie jest puste.

Jeśli jest to możliwe i jesteś bezpieczny, zadzwoń po pomoc lub wyślij SMS. Jeżeli jesteś w budynku dokładnie określ swoją lokalizację, podaj piętro, skrzydło budynku a nawet numer pokoju. Pozwoli to na szybsze udzielenie pomocy przez służby. Nie kontaktuj się z bliskimi osobami, aby nie potęgować paniki. Opanowanie emocji i zachowanie ciszy są kluczowe w tego typu sytuacji.

Jeżeli w pomieszczeniu znajdują się ranne osoby:

1. Priorytetem jest zawsze zabarykadowanie drzwi i obserwowanie, czy nikt nie próbuje dostać się do pomieszczenia (również w inny sposób np. przez inne drzwi lub okna).
2. W przypadku, gdy brakuje osób do udzielenia pomocy, bądź nie jest to możliwe z innego powodu – pilnuj wejścia do pomieszczenia i nie udzielaj pomocy.

3. Dopiero gdy wszystkie wejścia do pomieszczenia są odpowiednio zabezpieczone i obserwowane, pozostałe osoby (jeśli takie są) mogą przystąpić do udzielania pomocy poszkodowanym.
4. Jeżeli w pomieszczeniu znajdują się osoby, które nie wiedzą, co mają robić, nakaż im pilnować wejścia lub udzielić pomocy poszkodowanym.
5. Jeśli osoba poszkodowana ma rany postrzałowe, kłute lub innego rodzaju obrażenia, które powodują masywny krwotok – **w pierwszej kolejności zatamuj krwawienie,** nawet jeśli osoba jest nieprzytomna i nie oddycha! Z powodu szybkiego upływu krwi może ona umrzeć znacznie szybciej niż w wyniku zatrzymania krążenia.
6. Jeśli nie dysponujesz sprzętem medycznym, użyj przedmiotów, które masz pod ręką w celu zatamowania krwawienia. Użyj improwizowanej opaski uciskowej.



Rys. 7. Przykład wykonania improwizowanej opaski uciskowej. Więcej informacji na temat tamowania krwawień znajdziesz w rozdziale pt.: „Ratownictwo w warunkach zagrożenia"

7. Jeżeli udało Ci się opanować krwotoki, a osoba nie oddycha – możesz rozpocząć resuscytację krążeniowo-oddechową.

8. Jeśli poszkodowany jest przytomny, postaraj się go uspokoić i monitoruj jego stan. Jeżeli jest taka możliwość, poleć mu, aby razem z Tobą obserwował wejścia i okna do pomieszczenia.
9. Pamiętaj! W sytuacji zagrożenia nie masz obowiązku udzielania pomocy. Jeśli sytuacja jest zbyt niebezpieczna – nie ryzykuj własnym życiem.

po 4 UDAREMNIJ ATAK

Tylko i wyłącznie kiedy:

- nie możesz uciec ani się ukryć,
- konfrontacja z napastnikiem jest nieunikniona,
- istnieje bezpośrednie zagrożenie dla życia lub zdrowia.

Jeżeli ucieczka lub ukrycie się nie są możliwe, a konfrontacja z napastnikiem jest nieunikniona, masz prawo się bronić!

Zgodnie z art. 25. Kodeksu karnego: *Nie popełnia przestępstwa, kto w obronie koniecznej odpiera bezpośredni, bezprawny zamach na jakiekolwiek dobro chronione prawem.*

- Zaatakuj przez zaskoczenie i przy współpracy z innymi osobami.
- Użyj wszelkich dostępnych przedmiotów w celu obezwładnienia napastnika (np. krzesła, gaśnicy).
- Walkę powinny podjąć wszystkie zdolne do tego osoby (również te, które udzielały pomocy poszkodowanym) w celu uzyskania przewagi nad atakującym.
- Pamiętaj, że walka z napastnikiem to ostateczność i należy ją podjąć tylko wtedy, gdy nie ma innego wyjścia.

Wykorzystaj element zaskoczenia!

Wykorzystaj przewagę liczebną!

Improwizuj – wykorzystaj np. taboret, gaśnicę!

Obezwładniłeś sprawcę – odbierz mu broń!

Udawanie osoby martwej **nie jest rekomendowane,** ponieważ sprawcy ataków terrorystycznych często **eliminują rannych**. Jedynie w sytuacji, gdy nie masz żadnej możliwości na ucieczkę, ukrycie się lub udaremnienie ataku napastnika, możesz spróbować położyć się na ziemi i udawać osobę martwą. Agresor przeprowadzający zamach terrorystyczny przeżywa silny stres i może znajdować się pod wpływem środków odurzających. Jego pole widzenia jest zawężone, a uwaga skupiona na pojedynczych rzeczach i wydarzeniach. Istnieje więc szansa, że może nie zwrócić na Ciebie uwagi.

Jeśli jednak nie możesz lub nie jesteś w stanie walczyć:

- udawaj martwego,
- przyjmij pozycję bezpieczną i nie ruszaj się,
- błagaj o litość.

Pamiętaj! Staraj się nie wyjeżdżać do krajów tzw. podwyższonego ryzyka (ostrzeżenia znajdziesz na stronie MSZ) i nie bierz udziału w wydarzeniach, w których zachodzi wysokie prawdopodobieństwa przeprowadzenia zamachu terrorystycznego.

8.2. Sytuacja zakładnicza

Rekomendowane zachowanie w przypadku znalezienia się w sytuacji zakładniczej

Jeżeli uzbrojony napastnik po przejęciu kontroli nad sytuacją (np. wejściu do pomieszczenia, w którym się znajdujesz) nie atakuje Ciebie ani innych osób, to Twoim najważniejszym zadaniem jest **odpowiednie zinterpretowanie jego zamiarów oraz właściwa ocena sytuacji**.

Staraj się wykonywać wszystkie polecenia. Nie prowokuj, nie dyskutuj, nie staraj się uciec ani zaatakować napastnika.

Jeżeli po kilku minutach zaobserwujesz, że:

- napastnik nie ma zamiaru oddalić się z miejsca zdarzenia,
- barykaduje drzwi,
- wydaje polecenia zakładnikom,
- informuje o swoich zamiarach,

to masz do czynienia z sytuacją zakładniczą.

Jak się zachować?

1. Staraj się opanować swoje emocje – nie wykonuj gwałtownych ruchów, ponieważ może to wywołać agresję w napastniku.
2. Zadbaj o swój stan zdrowia – wykorzystuj każdą okazję do przyjmowania posiłków i napoi.
3. Nawiązuj kontakt z napastnikami, tylko jeżeli jest to niezbędne, np.: potrzeba zażycia niezbędnych lekarstw, udzielenie pomocy rannym lub skorzystanie z toalety.
4. Jeżeli w trakcie długotrwałego przetrzymywania przez napastników zauważysz, że masz realną szanse na ucieczkę – wykorzystaj ją.

- Bądź spokojny, naturalny, wykonuj polecenia napastników.
- Unikaj jakichkolwiek przejawów buntu, agresji czy silnych reakcji emocjonalnych.
- Nie zadawaj pytań, nie patrz w oczy, bądź posłuszny, pozostań spokojnie na miejscu.
- Nie komentuj zachowań ani poleceń napastników.
- Zawsze pytaj o pozwolenie, nie rób niczego bez zgody.
- Na żądanie oddaj przedmioty osobiste, usuń (wyrzuć) wszelkie oznaki zajmowania ważnego stanowiska.
- Nie kłam, nie oszukuj.
- Nie przebywaj w pobliżu okien i drzwi pomieszczeń.
- Spożywaj posiłki wyłącznie za zgodą napastnika.
- Pytaj o możliwość skorzystania z toalety.
- Obserwuj przebieg zdarzenia, postaraj się zapamiętać szczegóły.
- Wśród innych zakładników mogą być osoby współpracujące z terrorystami.
- Nie blokuj drogi ucieczki terrorystów.

9 Powiadamianie służb

Telefonując na numer **alarmowy 112**

- Przekaż dokładną **lokalizację zdarzenia** (miasto, ulica, numer budynku, kondygnacja, numer pomieszczenia).
- Podaj **liczbę** napastników.
- Opisz wygląd napastników.
- Podaj liczbę i typ broni posiadanej przez sprawców (jeżeli nie znasz się na broni, wystarczy informacja: **krótka lub długa**.
- Podaj liczbę potencjalnych **ofiar** lub **zakładników** w miejscu zdarzenia.
- Podaj opis najdogodniejszego dojazdu do obiektu zdarzenia.
- Jeżeli skończyłeś **nie rozłączaj się** – posłuchaj instrukcji Policji.
- **Nie konfabuluj, nie zmyślaj** – to wiedza na wagę cudzego życia.

10 Przybycie służb (działania kontrterrorystyczne)

Jeżeli w pomieszczeniu, w którym się znajdujesz:

- dojdzie do eksplozji;
- napastnicy zaczynają się bronić albo podejmować próbę ucieczki;
- zaobserwujesz bądź usłyszysz, że zbliżają się służby mundurowe

– najprawdopodobniej masz do czynienia ze szturmem ratunkowym, czyli operacją, która ma na celu uwolnienie zakładników.

W tej sytuacji:

- połóż się na ziemi i nie wykonuj gwałtownych ruchów;
- nie trzymaj nic w rękach – **puste dłonie** trzymaj na wysokości głowy;
- wykonuj **wszystkie polecenia** wydawane przez funkcjonariuszy;
- w przypadku strzelaniny nie uciekaj ani nie atakuj napastników;
- daj się swobodnie przeszukać przez funkcjonariuszy i odpowiadaj na ich pytania;
- w momencie ewakuacji nie zabieraj rzeczy osobistych.

11 Ratownictwo w warunkach zagrożenia

Jeżeli kiedykolwiek znajdziesz się w sytuacji zagrożenia o charakterze terrorystycznym czy też kryminalnym, w pierwszych sekundach i minutach będziesz zdany tylko na siebie. Zgodnie z procedurą **4U!**, w pierwszej kolejności należy uciekać, a jeśli nie jest to możliwe – ukryć się. Może jednak dojść do sytuacji, w której napotkasz osoby potrzebujące pomocy medycznej lub będziesz zmuszony

do udzielenia pomocy sobie. Pamiętaj, że w sytuacji **bezpośredniego zagrożenia Twojego życia** (np. podczas strzelaniny czy ataku z użyciem noża) **nie jesteś zobowiązany** do udzielania pomocy poszkodowanym, a Twoim podstawowym celem powinno być ratowanie własnego zdrowia i życia. Jeżeli jednak sytuacja na to pozwala i zdecydujesz się na jej udzielenie, musisz pamiętać, że będzie ona różnić się od „cywilnej" wersji pierwszej pomocy. Skuteczne szkolenie w tym zakresie wymaga wielu godzin ćwiczeń praktycznych, jednak na potrzeby tej publikacji nakreślono najważniejsze zasady i algorytmy postępowania.

W przypadku wystąpienia zdarzenia o charakterze terrorystycznym lub kryminalnym, możesz spotkać się z następującymi obrażeniami:

- rany postrzałowe,
- rany cięte i kłute (np. od noża),
- rozległe obrażenia spowodowane detonacją materiału wybuchowego.

Najważniejsza jest świadomość, które urazy są najniebezpieczniejsze i powinny być opatrzone w pierwszej kolejności. Istotny jest rodzaj urazu, a nie narzędzie, które go spowodowało.

11.1. Apteczka ratunkowa

Aby móc skutecznie ratować cudze i własne życie podczas zdarzenia o charakterze terrorystycznym, trzeba posiadać nie tylko przygotowanie teoretyczne, ale także dysponować umiejętnościami praktycznymi. Wiedzę taką zdobywa się na powtarzanych regularnie szkoleniach, które pozwalają wyrobić odpowiednie nawyki. Ćwiczenia praktyczne nie mogą jednak odbywać się bez odpowiedniego sprzętu.

Współczesne apteczki pierwszej pomocy nie są wyposażone w środki pomocy na wypadek ran spowodowanych w sytuacji o charakterze terrorystycznym (np. rany postrzałowe, obrażenia spowodowane wybuchem). Dlatego też Centrum Prewencji Terrorystycznej ABW rekomenduje wprowadzenie do apteczek znajdujących się w obiektach administracji państwowej następujących środków:

◄ Staza (opaska uciskowa)

Opatrunek indywidualny ►

◄ Rękawice nitrylowe

◄ Nożyce

Gaza skompresowana ►

◄ Karta poszkodowanego

Marker permanentny ►

◄ Opatrunek wentylowy

Statystyka zgonów powodowanych poszczególnymi rodzajami urazów:

Na podstawie badania Komitetu TCCC

- masywne krwawienia z kończyn i ich połączeń z korpusem – 60%
- odma prężna – 33%
- niedrożność dróg oddechowych – 6%
- hipotermia – 1%

Jak wynika z powyższej statystyki, najgroźniejszymi urazami powypadkowymi, które powodują największą liczbę zgonów, są masywne krwawienia. Dlatego też sposób udzielania pierwszej pomocy będzie różnił się od tej udzielanej w warunkach „cywilnych". W pierwszej kolejności najważniejsze będzie właśnie zatamowanie masywnych krwawień, a nie prowadzenie resuscytacji krążeniowo-oddechowej.

11.2. Zasady udzielania pomocy w sytuacji zagrożenia

1. Zadbaj o własne bezpieczeństwo.

- Zanim zaczniesz udzielać pomocy, zadbaj o własne bezpieczeństwo.
- Jeżeli sam odniesiesz obrażenia, to nie będziesz w stanie udzielić pomocy innym.
- Jeśli Twoje bezpieczeństwo zostanie zagrożone, spróbuj przedostać się (i jeśli to możliwe – przenieść poszkodowanego) w bezpieczne miejsce.

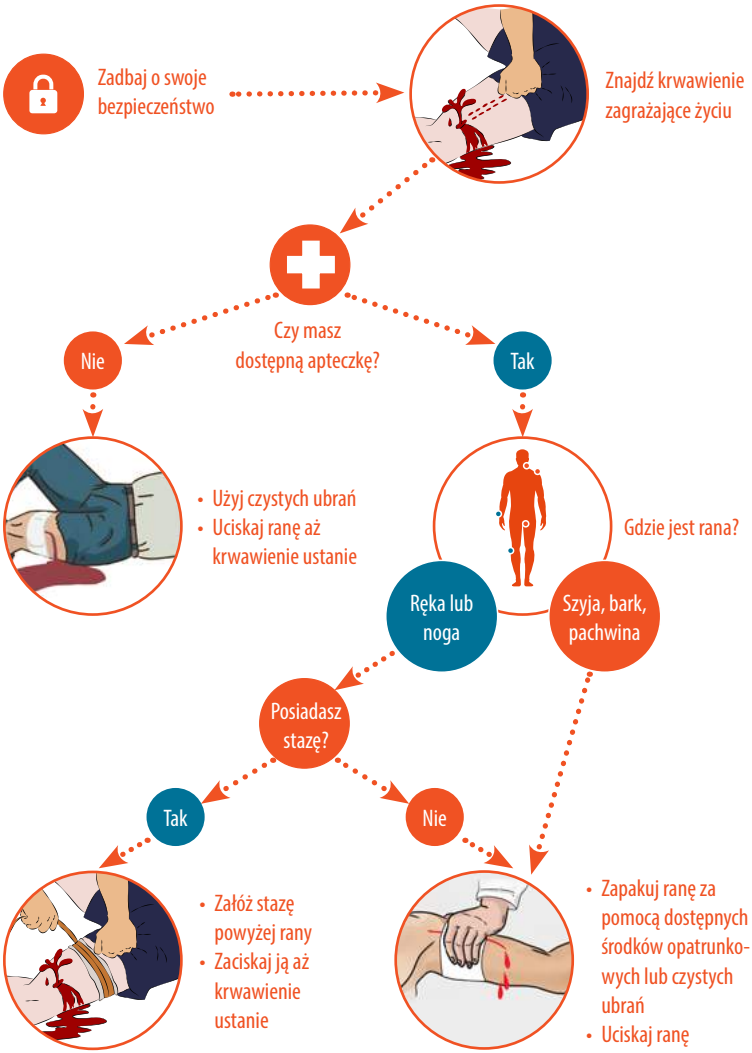
2. Poinformuj służby o zaistniałym zdarzeniu lub wyznacz inną osobę do tego zadania.

3. Udziel pomocy poszkodowanemu.

- Sprawdź, czy poszkodowany krwawi.
- Znajdź źródło krwawienia i oceń, czy jest to krwawienie zagrażające życiu.
- Zatamuj krwawienie.
- Jeśli potrafisz, zaopatrz obrażenia klatki piersiowej (zastosuj opatrunek uszczelniający; jeśli nie masz odpowiedniego opatrunku, zostaw ranę otwartą).
- Udrożnij drogi oddechowe.
- Zapobiegaj hipotermii – chroń poszkodowanego przed wyziębieniem.
- Monitoruj stan poszkodowanego.

11.3. Tamowanie krwawień

Istnieje wiele metod, które można skutecznie wykorzystać, aby zatamować krwawienie. Wszystkie mają jeden wspólny mianownik – uciskanie rany i (lub) naczyń krwionośnych.



Minimalnie krwawiące rany nie zagrażają życiu i nie wymagają natychmiastowego opatrunku.

Użyj **opaski uciskowej lub opatrunku uciskowego**, aby zatrzymać masywne krwawienie z kończyny.

- Jeśli używasz opaski uciskowej, załóż ją jak najwyżej na krwawiącej kończynie, bezpośrednio na skórę. Jeśli nie jesteś w stanie w pełni odsłonić rany, załóż ją na ubranej kończynie powyżej rany (nie zakładaj opaski uciskowej na staw lub otwarte złamanie).
- W przypadku amputacji (całkowitej lub częściowej) opaskę uciskową należy stosować niezależnie od rodzaju występującego krwawienia. Opaski uciskowej nie należy zdejmować ani poluzowywać z powodu bólu.

Zakładanie opaski uciskowej

- Jeśli opaska uciskowa jest prawidłowo nałożona, ale krwawienie nie ustaje, zastosuj drugą opaskę uciskową. Postaraj się ją założyć nad pierwszą opaską (bliżej tułowia).

- Jeśli jest to możliwe, opatrz głęboką ranę gazą lub środkiem hemostatycznym, przed zastosowaniem opatrunku uciskowego. Następnie nałóż opatrunek uciskowy bezpośrednio na opatrunek z gazy.

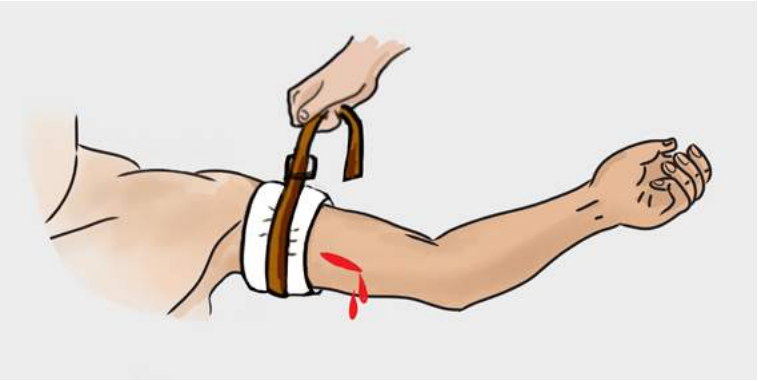
Opaski uciskowe

Najlepszym sposobem tamowania masywnych krwawień jest wykorzystanie opasek uciskowych (staz taktycznych). Koszt zakupu profesjonalnej opaski nie jest wysoki, a wożąc ją ze sobą, np. w samochodzie, będziesz znacznie lepiej przygotowany na sytuacje kryzysowe. Jeśli nie dysponujesz stazą w trakcie zdarzenia, spróbuj wykonać improwizowaną opaskę uciskową. Opaska musi składać się z wytrzymałego i odpowiednio szerokiego materiału (co najmniej 3 cm szerokości) oraz krępulca, czyli przedmiotu, który pozwoli na skręcenie materiału w celu zaciśnięcia go na kończynie. Improwizowaną opaskę możesz wykonać np. z pasów samochodowych i plastikowej butelki z wodą.

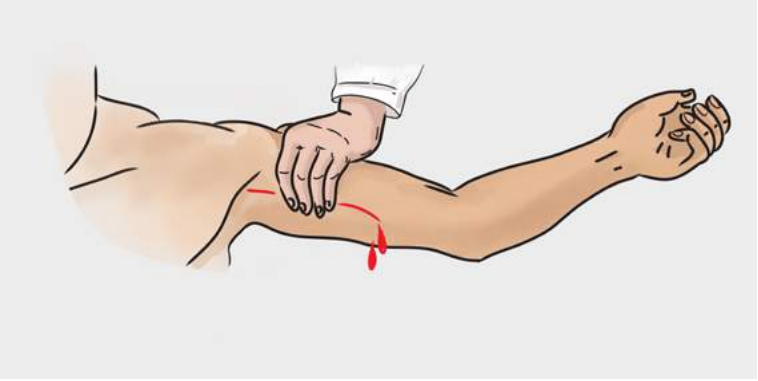
Pamiętaj! Mimo kontrowersji związanych z bezpieczeństwem wykorzystywania opasek uciskowych, Polska i Europejska Rada Resuscytacji w najnowszych wytycznych z 2015 roku zalecają stosowanie opasek uciskowych do zaopatrywania masywnych krwawień zewnętrznych. Ryzyko związane z powikłaniami na skutek niedokrwienia kończyny, na której znajduje się opaska, jest bardzo niskie. Skuteczne zastosowanie opaski może uratować życie!

W przypadku silnego krwawienia w miejscach połączeń (np. pachwinach), w których nie można użyć opaski uciskowej:

- jeśli to możliwe, opatrz ranę środkiem hemostatycznym i zastosuj bezpośredni nacisk zgodnie ze wskazówkami producenta;
- jeśli nie jest dostępny żaden środek hemostatyczny, opatrz ranę gazą i zastosuj bezpośredni nacisk, aby kontrolować krwawienie, następnie załóż odpowiedni opatrunek;



- w przypadku silnego krwawienia, gdy nie ma dostępu do opaski uciskowej ani opatrunku uciskowego, naciskaj bezpośrednio ranę.



12 Cyberbezpieczeństwo

Dynamiczny rozwój Internetu i nowych technologii stworzył wiele możliwości i udogodnień, ale i wynikających z tego zagrożeń. Internet stał się groźnym narzędziem w rękach terrorystów i przestępców (hakerów), którzy wykorzystują go do swoich celów. Odpowiedzialne korzystanie z usług internetowych oraz nowoczesnych urządzeń pozwala uniknąć większości zagrożeń w cyberprzestrzeni.

12.1. Zagrożenia bezpośrednio związane z terroryzmem

Propaganda terrorystyczna w Internecie

Nawet jeżeli robisz to w celach informacyjnych, nie udostępniaj i nie przekazuj dalej treści terrorystycznych w Internecie, gdyż leży

to w interesie terrorystów. Jest to „promocja" przesłania, jakie ma za sobą nieść dany zamach. Taka promocja może przyczynić się do podejmowania prób naśladowania poczynań terrorystów przez osoby podatne na radykalizację lub niestabilne psychicznie. Relacja z zamachu terrorystycznego w Christchurch, którą nagrał sprawca, została udostępniona przez internautów **kilka milionów razy**.

Próby werbunku

Upewnij się, że Twoje dzieci w bezpieczny sposób korzystają z Internetu, ponieważ są one najłatwiejszym celem dla terrorystów. Osoby młode, podatne na radykalizację lub przejawiające skłonność do agresji, mogą być zachęcane do wstąpienia do różnego rodzaju organizacji terrorystycznych.

Wykradanie danych

Pamiętaj o tym, że wszystkie dane, które znajdują się w Internecie, są również widoczne dla terrorystów. Dane o Twoich kontaktach i miejscu pracy mogą zostać użyte na etapie planowania zamachu

terrorystycznego. Nie udostępniaj na portalach społecznościowych informacji, które mogłyby zostać wykorzystane przez terrorystów lub przestępców.

12.2. Bezpieczeństwo danych osobowych użytkownika i informacji wrażliwych w miejscu pracy

Udostępnianie informacji w Internecie

Nie udostępniaj w Internecie żadnych informacji o swoim miejscu pracy i osobach, z którymi pracujesz. Każda informacja, która znalazła się w Internecie, może być niemożliwa do usunięcia. Pamiętaj, że informacje wrażliwe na Twój temat mogą zostać udostępnione również przez Twoich bliskich.

Próby wyłudzenia danych

Nie odpowiadaj na wiadomości, w których pojawia się żądanie przekazania osobistych danych, loginów, haseł itp. Nawet jeśli kontaktujące się z Tobą osoby podają się za pracowników banku albo służb.

Ochrona danych osobowych

Nie twórz wersji elektronicznej dokumentów tożsamości (paszportu, dowodu osobistego, prawa jazdy itp.) przez ich skanowanie lub fotografowanie. Nie udostępniaj ich w sieci i nie przesyłaj drogą elektroniczną.

12.3. Higiena pracy w Internecie

Programy antywirusowe

Upewnij się, że masz zainstalowany na komputerze oraz telefonie program antywirusowy i podlega on cyklicznej aktualizacji.

Tworzenie haseł

Twórz silne hasła – powinny się one składać z małych i wielkich liter, cyfr i znaków specjalnych. Nie używaj jednego hasła do wszystkich usług (np. skrzynka pocztowa, bank, portal społecznościowy). Co jakiś czas staraj się zmieniać hasła na nowe (np. co kilka miesięcy). Nie zapisuj haseł w ogólnodostępnym miejscu, np. na kartce leżącej obok komputera czy w pliku komputerowym.

Bezpieczne pobieranie plików z Internetu

Nie pobieraj żadnych plików z Internetu, co do których pochodzenia nie masz absolutnej pewności.

Otwieranie załączników e-maili

Nie otwieraj żadnych załączników e-maili, chyba że są one oczekiwane i pochodzą od znanych odbiorców. Wszystkie załączniki przeskanuj aktualnym programem antywirusowym.

Otwieranie nieznanych i podejrzanych linków. Oszustwa bankowe

Nie otwieraj linków przesłanych drogą elektroniczną od nieznanych osób. Częstym sposobem oszustwa jest podmiana adresu strony (np. banku) na adres bardzo podobny w celu uzyskania Twoich danych logowania. Przy logowaniu do banku upewnij się, że adres strony jest właściwy.

Niezabezpieczone i niebezpieczne strony Internetowe

Nie lekceważ komunikatów przeglądarki internetowej lub Google, że dana strona Internetowa może być niebezpieczna. Nie wchodź na tego typu strony.

Pobieranie aplikacji na telefony komórkowe

Upewnij się, że aplikacje, które pobierasz z Google Play lub Apple Store, są oficjalne i pochodzą od zaufanych producentów. Aplikacja

banku może się okazać programem, który wygląda bardzo podobnie, jednak jest stworzony w celu wykradnięcia Twoich danych logowania.

Bezpieczeństwo publicznych sieci Wi-Fi

Staraj się nie korzystać z publicznych sieci Wi-Fi, które nie są zabezpieczone hasłem. Istnieje możliwość przechwycenia danych z Twojego komputera lub telefonu przez innego użytkownika takiej sieci, który dysponuje odpowiednim oprogramowaniem. Domową i służbową sieć Wi-Fi zawsze zabezpieczaj hasłem.

Zgłaszanie incydentów bezpieczeństwa

Wszystkie podejrzane wiadomości zgłaszaj niezwłocznie osobie odpowiedzialnej w Twoim miejscu pracy za bezpieczeństwo teleinformatyczne, swojemu bankowi, gdy próba ataku skierowana jest na konto bankowe, lub platformie społecznościowej, jeżeli jesteś jej użytkownikiem. W przypadku braku możliwości zgłoszenia do ww. podmiotów, pamiętaj, że wszystkie incydenty teleinformatyczne **w urzędzie lub instytucji państwowej** możesz zgłosić również na stronie:

www.csirt.gov.pl.

13 Przygotowanie obiektu na wypadek zagrożeń terrorystycznych

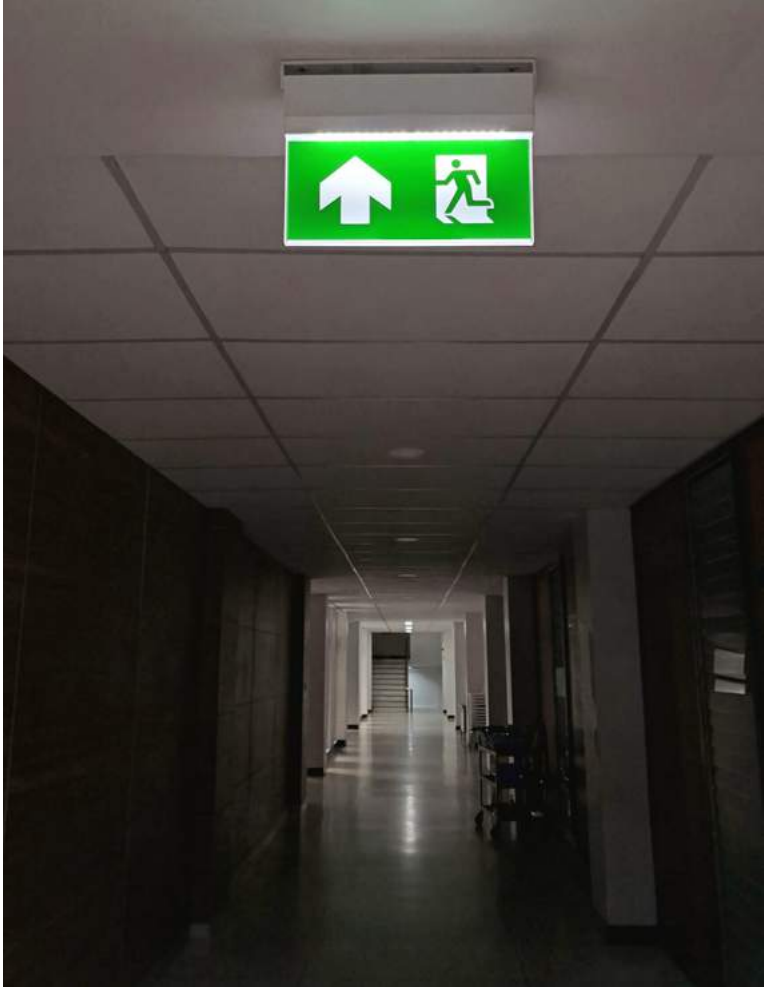
Poniżej prezentujemy zbiór wybranych zaleceń mających na celu podniesienie poziomu bezpieczeństwa w obiektach administracji publicznej.

- Posiadanie **innego niż w przypadku alarmu pożarowego** sygnału alarmowego i komunikatu słownego do sygnalizo-

wania zagrożenia zamachem z wykorzystaniem materiałów wybuchowych.

- Posiadanie komunikatu słownego lub **sygnału do sprawdzenia pomieszczeń** przez personel oraz piony techniczne czy bezpieczeństwa, wraz z procedurą przekazania informacji zwrotnej o wynikach takich sprawdzeń.
- Kształt sygnału lub treść komunikatu powinny być przyjęte wraz z określeniem **technicznych sposobów ich przekazywania** (np.: dźwiękowe systemy ostrzegawcze, łączność internetowa, aplikacje na telefonach komórkowych).

Podczas planowania ewakuacji należy rozważyć wyznaczenie miejsc **zbiórek do ewakuacji** oraz miejsc **docelowej ewakuacji** (oddalonych od obiektu, w strefie bezpiecznej od potencjalnego zagrożenia wybuchem). Te informacje powinny znaleźć się w Instrukcji Bezpieczeństwa Pożarowego oraz w planach ochrony. Do planowania takich miejsc można wykorzystać inne budynki



użyteczności publicznej na podstawie wcześniej przygotowanych umów realizacji takich usług.

- Miejsca **zbiórek do ewakuacji** oraz **docelowej ewakuacji** powinny być odpowiednio oznakowane (zgodnie z polskimi normami) oraz powinny zapewniać bezpieczeństwo ludziom ewakuującym się przed atakami z użyciem broni, materiałów wybuchowych czy pojazdów.
- Należy przewidzieć możliwość przeprowadzania **ewakuacji częściowej** (w przypadku niewielkiego punktowego rozpoznanego zagrożenia), **całkowitej** (pozostawienie obiektu bez żadnych osób

w nim pozostającym) oraz **ewakuacji do obiektu** – w przypadku zagrożenia punktowego występującego na zewnątrz obiektu.
- Do wykonywania zadań w zakresie ostrzegania, alarmowania oraz ewakuacji można wykorzystywać tzw. **liderów bezpieczeństwa** (odpowiednio wyposażonych, oznakowanych i przeszkolonych), których zadania należy szczegółowo określić w instrukcjach i zasadach postępowania na wypadek zagrożeń w obiekcie.

Proponowane rozwiązania

Koperta bezpieczeństwa

Opracowanie bazy danych o obiekcie na potrzeby służb (Policja, Straż Pożarna). W przypadku zagrożenia tego rodzaju informacje mogą w znacznym stopniu ułatwić pracę służb. Są nimi:
- dokumentacja opisowa,
- rzuty kondygnacji,
- widoki elewacji,
- przekroje obiektu,

- dokumentacja fotograficzna,
- przyłącza mediów.

Liderzy bezpieczeństwa

Wybrani pracownicy lub funkcjonariusze przygotowani do reagowania w przypadku wystąpienia zagrożenia o charakterze terrorystycznym.

- Przeszkoleni pod kątem zagrożeń terrorystycznych.
- Widoczni – koncentrują uwagę.
- Wydają polecenia, koordynują ewakuację.
- Przeciwdziałają panice.
- Współpracują z przybyłymi służbami.

Zabezpieczenia techniczne

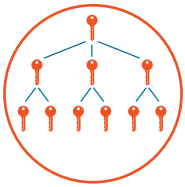
Sieć głośników (radiowęzeł)

Monitoring, czujniki ruchu podłączone do centrum nadzoru lub ochrony

Piloty i przyciski napadowe (stacjonarne i przenośne)

Możliwość zamknięcia drzwi od środka

Wizjery w drzwiach



System klucza „master key”

14 Zarządzanie ryzykiem w obiektach

Czy można zminimalizować ryzyko?

Wysoki poziom świadomości, odpowiednie przeszkolenie, zabezpieczenie obiektów i uaktualnianie procedur, pozwalają zminimalizować ryzyko wystąpienia zdarzeń o charakterze terrorystycznym. Właściwe przygotowanie na niebezpieczeństwa pozwala podjąć prawidłową reakcję w przypadku ewentualnego incydentu, a także może odwieźć sprawcę od popełnienia aktu przemocy w danym miejscu.

Atrakcyjność obiektu z perspektywy sprawcy

Obiekty i miejsca użyteczności publicznej są częstym celem ataków terrorystycznych. Są one szczególnie atrakcyjne z perspektywy sprawców, zwłaszcza wtedy, gdy dysponują niewielkim poziomem zabezpieczeń. Potencjalny napastnik może liczyć na następujące korzyści:

- Spowodowanie znacznej liczby ofiar.
- Możliwość wykorzystania symboliki konkretnego budynku (kościoły, siedziby określonych firm lub władz państwowych, w tym służb i instytucji, banki, ambasady).
- Zapewnienie odpowiedniego zainteresowania medialnego.
- Niski stopień ochrony niektórych obiektów użyteczności publicznej (galerie handlowe, kina, teatry, dworce kolejowe).
- Niekontrolowany i zapewniający anonimowość dostęp do obiektu, a także możliwość ucieczki po zdarzeniu (galerie handlowe, kina, teatry, dworce kolejowe, ogólnodostępne części portów lotniczych).

- Możliwość wykorzystania materiałów wybuchowych i każdego rodzaju broni – szczególnie w budynkach niechronionych.

- Możliwość wykorzystania w zamachach bombowych stref parkingowych w celu kumulacji zniszczeń (rozprzestrzenianie się pożaru dzięki kolejnym wybuchom paliwa samochodowego lub dążenie do zagrożenia integralności oraz stabilności konstrukcji budynku).

- Możliwość potęgowania skutków zamachów z wykorzystaniem broni chemicznej, biologicznej lub oparów powybuchowych za pomocą systemów wentylacyjnych.

- Spotęgowanie liczby ofiar z powodu możliwości wystąpienia paniki i niekontrolowanej ucieczki z budynku.

- Ograniczone możliwości działania służb ratowniczych ze względu na możliwości przepustowe dróg ewakuacyjnych oraz najczęściej zwartą infrastrukturę wokół budynków (szczególnie w ścisłych centrach miast).

- Wpływ zamachu na kolejne obiekty znajdujące się w pobliżu i zwiększenie w ten sposób liczby ofiar i zniszczeń.

- Poprzez atak na obiekty powszechnie używane przez obywateli (dworce kolejowe, stacje metro, galerie handlowe, kina, teatry), wywołanie strachu przed dalszym korzystaniem z takich obiektów.

- Możliwość spowodowania znacznych strat materialnych dla określonych sektorów gospodarki lub wywołania paraliżu komunikacyjnego w przypadku zaatakowania węzłów komunikacyjnych.

- Możliwość obecności w budynkach osób znanych i atrakcyjnych medialnie.

14.1. Przyjęcie informacji o zagrożeniu

Informowanie o zagrożeniach dotyczących obiektów użyteczności publicznej nie jest niczym nowym. Jednak zdecydowana większość ataków na obiekty użyteczności publicznej odbywa się bez zapowiedzi. Natura współczesnego terroryzmu powoduje, że

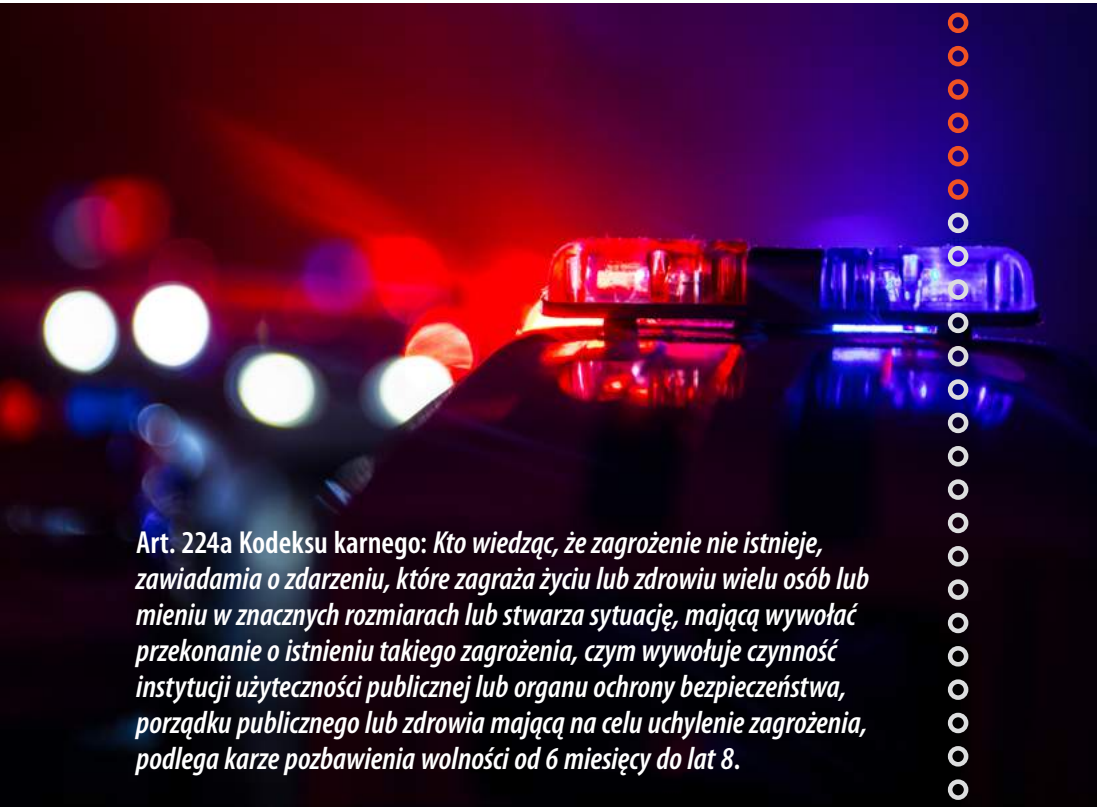
sprawcom zależy przede wszystkim na jak największej liczbie ofiar. Zatem informowanie o zagrożeniu personelu obiektu nie jest w ich interesie i taki sposób działania nie znajduje potwierdzenia w *modus operandi* poszczególnych sprawców zamachów z ostatnich lat.

Mimo to nigdy nie można wykluczyć, że sprawca będzie chciał poinformować o swoich zamiarach. Warto zaznaczyć, że poza terrorystami o zagrożeniach mogą również informować osoby niepoczytalne (np. zaburzone psychicznie, pod wpływem alkoholu czy środków odurzających) lub osoby celowo informujące o fałszywym zagrożeniu, które chcą zakłócić prawidłowe funkcjonowanie obiektu (w celu spowodowania ewakuacji, obniżenia wizerunku marki czy instytucji).

Rodzaje informacji o zagrożeniu

- **Informacje prawdziwe** – o realnym zagrożeniu.
- **Informacje fałszywe** – o zagrożeniu, które nie istnieje – w celu spowodowania ewakuacji obiektu albo przeprowadzenia zamachu w innym miejscu.

- **Informacje fałszywe** – o zagrożeniu, które nie istnieje – w celu destabilizacji funkcjonowania obiektu lub obniżenia wizerunku instytucji.
- **Informacje fałszywe** – o zagrożeniu, które nie istnieje – przeprowadzone przez osobę bez wyraźnego celu (sprawcy niepoczytalni, z zaburzeniami osobowości, żarty).



Art. 224a Kodeksu karnego: ***Kto wiedząc, że zagrożenie nie istnieje, zawiadamia o zdarzeniu, które zagraża życiu lub zdrowiu wielu osób lub mieniu w znacznych rozmiarach lub stwarza sytuację, mającą wywołać przekonanie o istnieniu takiego zagrożenia, czym wywołuje czynność instytucji użyteczności publicznej lub organu ochrony bezpieczeństwa, porządku publicznego lub zdrowia mającą na celu uchylenie zagrożenia, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.***

Szczególną formą zgłoszeń są **alarmy kaskadowe**. Dotyczą one informowania przez jednego sprawcę o zagrożeniu dla **większej liczby obiektów**, w tym samym lub **zbliżonym czasie,** przy wykorzystaniu tego samego środka łączności.

Sposoby informowania o zagrożeniu:

- **telefonicznie**,
- **listownie**,
- **drogą elektroniczną** (e-mailem, za pomocą portali społecznościowych, komunikatorów),
- **osobiście**,
- **za pośrednictwem innych osób niż sprawca** (z wykorzystaniem każdej z wyżej wymienionych metod).

Informacja przekazana telefonicznie

1. Bądź przygotowany na przyjęcie informacji w każdej chwili – pamiętaj, gdzie jest **formularz przyjęcia informacji o zagrożeniu.**
2. Prowadź rozmowę w sposób opanowany, **nie oceniaj, nie krytykuj i nie pouczaj** osoby informującej.
3. Nie rozpoczynaj rozmowy od pytania o tożsamość.
4. Używaj **pytań otwartych** (jaka, jakie, dlaczego), zadawaj pytania o charakter zagrożenia, czas, skutki, metodę, powód, możliwości odstąpienia od czynu itp.

5. Nie rozłączaj się w żadnym wypadku – staraj się **podtrzymać rozmowę.**
6. Zasygnalizuj innym osobom, aby byli świadkami rozmowy, jeśli to możliwe – **nagraj tę rozmowę.**
7. Poproś kogoś w pobliżu o **powiadomienie o tej sytuacji przełożonego** i (lub) pracownika pionu bezpieczeństwa.
8. Jeżeli aparat telefoniczny identyfikuje numer dzwoniącego – **zanotuj go.**
9. Zapisz dokładnie przekazaną informację w sposób najbardziej szczegółowy.
10. Użyj formularza przyjęcia informacji o zagrożeniu, który pomoże Ci zebrać **jak najwięcej informacji**.
11. Po przyjęciu informacji bądź przygotowany do przekazania wszystkich uzyskanych szczegółów przełożonym lub osobom odpowiedzialnym za bezpieczeństwo w obiekcie.

Informacja przekazana osobiście

1. Zwróć uwagę na **wygląd zewnętrzny** osoby zawiadamiającej, zapamiętaj znaki szczególne.

2. Rozmowę **prowadź w sposób spokojny**, nie oceniaj, nie krytykuj i nie pouczaj osoby informującej, która może być sprawcą. Zadawaj pytania dotyczące szczegółów zagrożenia.
3. Jeśli to możliwe, nagraj rozmowę z informującym.
4. Zadbaj o **swoje bezpieczeństwo**. Jeśli masz możliwość, powiadom inną osobę, że przyjmujesz taką informację, utrzymuj dystans od osoby, z którą rozmawiasz, bądź przygotowany na możliwe wybuchy agresji czy inne niekontrolowane reakcje.
5. Jeśli osoba przekazująca informację odejdzie, **zanotuj, w którym kierunku się udała**.
6. Powiadom przełożonego lub osobę odpowiedzialną za bezpieczeństwo w obiekcie.
7. Zapisz przekazaną informację dokładnie w ten sam sposób, w jaki została wyartykułowana.
8. Zanotuj **dane oraz rysopis osoby**, która przekazała informację.

Informacja przekazana drogą elektroniczną

1. Zostaw wiadomość **otwartą na komputerze.**
2. Nie odpisuj i **nie wykonuj poleceń** zawartych w korespondencji.
3. Powiadom przełożonego lub osobę odpowiedzialną za bezpieczeństwo w obiekcie.
4. Utrwal informację, np. **wydrukuj, sfotografuj albo skopiuj** wiadomość i jej temat.
5. Zanotuj datę i czas odebrania wiadomości.

Informacja przekazana listownie

1. Jeżeli to możliwe, ogranicz dostęp do dokumentu niepowołanym do tego osobom.
2. Nie dotykaj i **nie przemieszczaj dokumentu.**
3. Powiadom przełożonego lub osobę odpowiedzialną za bezpieczeństwo w obiekcie.
4. Zapamiętaj, kto widział i dotykał dokument, kto go przekazał i w jakiej formie.
5. Jeżeli to możliwe, **sfotografuj treść dokumentu.**

Formularz przyjęcia informacji o zagrożeniu

Formularz przyjęcia informacji o zagrożeniu jest dostępny w wersji elektronicznej – do pobrania – na stronie: https://tpcoe.gov.pl/cpt/materialy

Formularz przyjęcia informacji o zagrożeniu jest zbiorem wskazówek, które pomogą zebrać jak najwięcej informacji w przypadku otrzymania informacji o zagrożeniu.

Będzie to wiedza niezwykle cenna dla służb, których zadaniem będzie identyfikacja sprawcy i jego zatrzymanie. Formularz powinien

zawsze znajdować się w dostępnym miejscu dla każdego pracownika instytucji państwowej. Należy go wypełnić bezpośrednio po otrzymaniu informacji o zagrożeniu.

14.2. Algorytm postępowania zarządzającego budynkiem w przypadku podłożenia materiałów wybuchowych

Alarmowanie

1. Przyjęcie informacji o zagrożeniu lub rozpoznanie zagrożenia. Osobie przyjmującej zgłoszenie o podłożeniu urządzenia wybuchowego oraz administratorowi obiektu nie wolno lekceważyć żadnej informacji na ten temat.
2. Przekazanie informacji o zagrożeniu administratorowi obiektu oraz Policji, która dokonuje weryfikacji wiarygodności informacji.
3. W zależności od rodzaju zdarzenia, zawiadamiając Policję, należy podać:
    - treść rozmowy ze zgłaszającym podłożenie urządzenia wybuchowego, którą należy prowadzić korzystając z formularza przyjęcia informacji o zagrożeniu,

- treść przesłanej wiadomości o podłożeniu urządzenia wybuchowego,
- miejsce i opis zlokalizowanego przedmiotu, który może zawierać materiał wybuchowy,
- numer telefonu, z którego prowadzona jest rozmowa, oraz swoje nazwisko.

Czynności podejmowane przez administratora obiektu po uzyskaniu informacji o podłożeniu urządzenia wybuchowego lub w przypadku jego zlokalizowania

1. Do czasu przybycia Policji czynnościami zarządza administrator obiektu, a w czasie jego nieobecności – osoba przez niego upoważniona.
2. Zarządzający czynnościami, w sytuacji gdy urządzenie wybuchowe nie zostało jeszcze zlokalizowane, poleca użytkownikom pomieszczeń, aby dokonali sprawdzenia, czy znajdują się w nich:
   - przedmioty, których wcześniej nie było i nie wnieśli ich użytkownicy pomieszczeń (a mogły być wniesione i pozostawione przez inne osoby, np. interesantów),
   - ślady przemieszczenia elementów wyposażenia pomieszczeń,
   - zmiany we właściwościach zewnętrznych przedmiotów znajdujących się w pomieszczeniu oraz emitowane z nich sygnały (np. dźwięki mechanizmów zegarowych, świecące elementy elektroniczne).
3. Pomieszczenia ogólnodostępne, takie jak: korytarze, klatki schodowe, hole, windy, toalety, piwnice, strychy itp. oraz najbliższe otoczenie zewnętrzne obiektu, powinny być sprawdzone przez pracowników obsługi administracyjnej lub ochrony.
4. W przypadku stwierdzenia przez użytkowników pomieszczeń obecności przedmiotów, których wcześniej nie było, lub zmiany w wyglądzie i usytuowaniu przedmiotów stale znajdujących się w tych pomieszczeniach, można przypuszczać, że mogą to być urządzenia wybuchowe. W takiej sytuacji nie wolno dotykać zlokalizowanych przedmiotów, a o ich umiejscowieniu należy natychmiast powiadomić administratora obiektu.

Administrator obiektu może wydać decyzję o ewakuacji osób z zagrożonego obiektu przed przybyciem Policji!

5. W przypadku ogłoszenia ewakuacji administrator obiektu poleca użytkownikom pomieszczeń zabrać rzeczy osobiste, z którymi przybyli do obiektu, i mieć je stale przy sobie np.: torebki, nesesery, plecaki oraz nakrycia wierzchnie. Nie może to jednak opóźnić ewakuacji.
6. Administrator obiektu, ogłaszając ewakuację, powinien zachować spokój i opanowanie, aby nie dopuścić do przejawów paniki.

Akcja rozpoznawczo-neutralizacyjna zlokalizowanych urządzeń wybuchowych

1. Po przybyciu do obiektu policjanta lub policyjnej grupy interwencyjnej administrator obiektu powinien przekazać im wszelkie informacje dotyczące zdarzenia oraz wskazać miejsca zlokalizowanych przedmiotów obcego pochodzenia i punkty newralgiczne w obiekcie.
2. Policjant lub dowódca grupy policjantów przejmuje zarządzanie czynnościami, a administrator obiektu powinien udzielić mu wszechstronnej pomocy.
3. Przy uwzględnieniu oceny wiarygodności informacji o podłożeniu urządzenia wybuchowego przygotowanej przez Policję, administrator obiektu podejmuje decyzję o ewakuacji osób z obiektu lub z jego części – o ile wcześniej to nie nastąpiło – albo o braku zasadności ewakuacji.
4. Uprawnione komórki organizacyjne Policji, przy wykorzystaniu specjalistycznych środków technicznych, zajmują się identyfikacją i rozpoznawaniem zlokalizowanych przedmiotów obcego pochodzenia oraz neutralizowaniem ewentualnie podłożonych urządzeń wybuchowych.
5. Po zakończeniu czynności policjant przekazuje protokolarnie obiekt administratorowi.

14.3. Algorytm postępowania zarządzającego budynkiem w przypadku ataku masowego zabójcy

1. Identyfikacja zagrożenia.
2. Przekazanie informacji o zagrożeniu Policji oraz (jeśli jest) grupie interwencyjnej.
3. Podanie sygnału alarmowego zastrzeżonego na wypadek **ataku masowego zabójcy**.
4. Wykorzystanie do ewakuacji tzw. **liderów bezpieczeństwa** (koordynowanie ewakuacji i zapewnienie bezpieczeństwa w miejscach ewakuacji).
5. Współpraca z Policją i innymi służbami przybywającymi na miejsce zdarzenia.
6. Powrót do obiektu na podstawie decyzji Policji dopuszczającej obiekt do dalszej eksploatacji.

15 Komunikacja strategiczna

Komunikację strategiczną możemy zdefiniować jako przekazywanie informacji w celu osiągnięcia wcześniej założonego rezultatu strategicznego. Prowadzą ją zarówno podmioty państwowe – urzędy, służby i instytucje oraz przedsiębiorstwa, jak i sami terroryści i organizacje terrorystyczne.

Terroryzm poza samym aktem przemocy jest formą przekazania wiadomości lub manifestu. Sprawcom zamachów zależy bardzo często na wzbudzeniu strachu, demonstracji siły, promocji swoich przekonań oraz pozyskaniu zwolenników. Swoimi czynami chcą zwrócić na siebie uwagę i wywołać pożądany efekt. Rolą instytucji

państwowych, a także samych obywateli, jest umiejętne rozpoznawanie i przeciwdziałanie propagandzie terrorystycznej – zarówno przed, w trakcie, jak i po wystąpieniu zdarzenia o charakterze terrorystycznym.

W niniejszym rozdziale prezentujemy zagadnienia związane z wykorzystaniem komunikacji strategicznej w przeciwdziałaniu terroryzmowi i propagandzie terrorystycznej. Jest on skierowany przede wszystkim do kadry zarządzającej, rzeczników prasowych oraz osób odpowiedzialnych za komunikację w urzędach i instytucjach w naszym kraju.

Siła przekazu

Zamachy terrorystyczne od wielu lat wzbudzają zainteresowanie mediów na całym świecie. Wraz z rozwojem Internetu i mediów społecznościowych informacje o atakach rozchodzą się jeszcze szybciej i na jeszcze większą skalę. Terroryści uzyskali nowe narzędzia do promowania swoich postulatów i aktów przemocy, a także do prowadzenia radykalizacji.

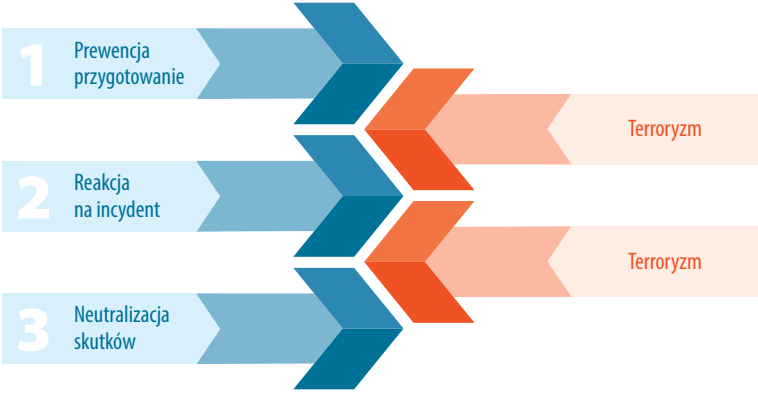
Niektórzy sprawcy przed dokonaniem ataku zamieszczają w Internecie manifesty, w których zachęcają odbiorców do naśladowania ich czynów. Znamy również przypadki, w których zamachowcy nagrywali, a nawet transmitowali na żywo dokonywany przez siebie atak. Tego rodzaju treści budzą duże zainteresowanie wielu osób – nawet tych, które nie są zradykalizowane czy skłonne do agresji. Takie materiały są również szybko i na masową skalę rozpowszechniane dalej przez internautów, co powoduje, że docierają do milionów odbiorców na całym świecie. Firmy technologiczne oraz służby bezpieczeństwa dokładają wszelkich starań aby jak najszybciej usunąć takie treści z Internetu, jednak jest to zadanie bardzo trudne. Obecnie nie jest możliwe wyeliminowanie wszystkich treści o charakterze terrorystycznym z Internetu.

Ugrupowania terrorystyczne i ich zwolennicy tworzą również specjalnie przygotowane materiały radykalizujące, które są kierowane do konkretnych państw i grup społecznych. Doprowadzają w ten sposób do radykalizacji osób oddalonych o tysiące kilometrów, które w konsekwencji dokonują zamachów lub wyjeżdżają do stref konfliktów zbrojnych.

Istotne jest więc współdziałanie instytucji państwowych, organizacji pozarządowych, mediów i innych podmiotów na rzecz skutecznego przeciwdziałania narracji terrorystów i ugrupowań terrorystycznych.

Trzystopniowe podejście w zarządzaniu kryzysowym

Wyróżniamy trzy podstawowe fazy komunikacji strategicznej związanej z zapobieganiem, przeciwdziałaniem i neutralizacją skutków terroryzmu. Stosowanie ich przez urzędy i instytucje państwowe może być odpowiedzią na komunikację prowadzoną przez organizacje terrorystyczne i zminimalizować jej skutki.



Prewencja i przygotowanie

Pierwsza faza polega na prowadzeniu działań prewencyjnych mających na celu niedopuszczenie do zdarzeń o charakterze terrorystycznym. Przez **działania uświadamiające**, takie jak kampanie społeczne i informacyjne, można podnosić świadomość społeczeństwa w zakresie zagrożeń, a także uczyć właściwych sposobów reagowania w przypadku ich wystąpienia. Wysoka świadomość społeczna będzie wpływała również pośrednio na potencjalnych sprawców, których podejrzane zachowania będą mogły być łatwiej dostrzegane przez obywateli.

Przykładem działań uświadamiających jest zrealizowana przez Centrum Prewencji Terrorystycznej ABW kampania społeczna 4U!

www.4u.tpcoe.gov.pl

4U UWAŻAJ UCIEKAJ UKRYJ SIĘ UDAREMNIJ ATAK!

Równie istotne jest **budowanie gotowości** na wypadek ewentualnego zdarzenia. Polega ono na wprowadzaniu procedur, planów i zabezpieczeń technicznych, a także regularnych szkoleń dla pracowników. W przypadku wystąpienia zdarzenia o charakterze terrorystycznym, odpowiednie procedury oraz przeszkolony personel będą w stanie zminimalizować straty lub całkowicie zapobiec niebezpiecznej sytuacji.

Świadomość społeczna
- Podniesienie zdolności publicznej do identyfikacji zagrożeń

Budowanie gotowości
- Planowanie
- Szkolenia i treningi

Alternatywna narracja
- Przeciwdziałanie radykalizacji online

Odporność

Wysoki poziom zabezpieczeń odgrywa również **rolę odstraszającą**. Potencjalny sprawca może odstąpić od przeprowadzenia ataku, jeśli zauważy, że dany obiekt posiada wysoki poziom zabezpieczeń. Nawet tabliczka z informacją o zakazie wnoszenia niebezpiecznych przedmiotów, który będzie egzekwowany przez ochronę, może wzbudzić wątpliwości napastnika.

Prewencja ogólna
w komunikacji strategicznej (odstraszanie)
pomaga udaremniać ataki na wybraną instytucję
lub organizację i (lub) jej stronę internetową

•

Jeśli potencjalny sprawca wierzy,
że dana instytucja i jej strona internetowa
mają dobre zabezpieczenia,
może odstąpić od ataku fizycznego lub hakerskiego

Ważnym elementem jest też budowanie alternatywnej narracji (**kontrnarracji**), która polega na promowaniu i przekazywaniu treści przeciwstawnych do propagandy terrorystycznej. Jest to w głównej mierze zadanie instytucji odpowiedzialnych za przeciwdziałanie terroryzmowi, jednak może być podejmowane również przez inne podmioty, np. placówki edukacyjne. Istotną rolę odgrywa również odpowiednio szybkie zgłaszanie i usuwanie przez wszystkie urzędy i instytucje wszelkich treści o charakterze terrorystycznym w przestrzeni cyfrowej (np. wpis na stronie internetowej czy forum prowadzonym przez dany urząd lub instytucję). Rolą służb odpowiedzialnych za bezpieczeństwo jest też publikowanie sprostowań i wyjaśnień treści o charakterze terrorystycznym, które pojawią się w opinii publicznej.

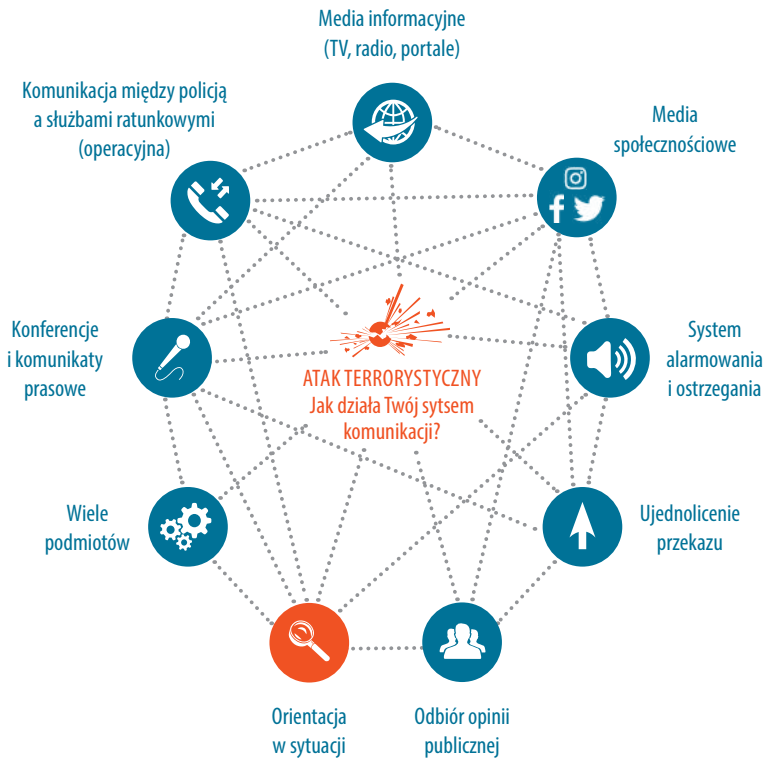
Reakcja na incydent

Prowadzenie skutecznej i zorganizowanej polityki informacyjnej w przypadku wystąpienia zdarzenia o charakterze terrorystycznym może być dużym wyzwaniem, jednak jest konieczne w celu **minimalizowania skutków zdarzenia**. W tym momencie najważniejsze mogą okazać się przygotowane wcześniej procedury.

Podczas sytuacji kryzysowej już w pierwszych minutach zdarzenia jego świadkowie mogą za pośrednictwem telefonów i mediów społecznościowych informować o wydarzeniach. Niekontrolowana ilość często sprzecznych informacji może doprowadzić do powstania paniki oraz plotek i dezinformacji. Niektórzy obywatele, nie mając świadomości o stanie zagrożenia, mogą udać się w miejsce zdarzenia i sami znaleźć się w niebezpieczeństwie lub utrudniać działania służb. Dlatego też najważniejsze jest odpowiednio **szybkie i rzetelne poinformowanie** opinii publicznej o zaistniałej sytuacji. Jeżeli incydent miał miejsce w urzędzie lub instytucji państwowej, komunikat powinien zostać opracowany w porozumieniu z przedstawicielem instytucji oraz właściwą służbą (np. Policją i Państwową Strażą Pożarną).

Zasady komunikacji w sytuacjach kryzysowych

- Szybka reakcja.
- Rzetelność.
- Konsekwentny przekaz.
- Zachowanie spokoju i zapobieganie panice.
- Dostarczanie sprawdzonych informacji.
- Przeciwdziałanie plotkom i dezinformacji.
- Ostrzeganie o ewentualnych zagrożeniach.



Dużym wyzwaniem w przypadku ataku terrorystycznego jest uzyskanie odpowiedniej wiedzy o wydarzeniu przez wszystkie podmioty. Potrzeby i wymagania dotyczące informacji i komunikacji dla każdego odbiorcy są różne (treść, objętość, czas, priorytet).

Neutralizacja skutków

Komunikacja prowadzona po wystąpieniu incydentu ma za zadanie łagodzić jego skutki oraz przeciwdziałać intencjom jego sprawców. **Centrum Prewencji Terrorystycznej ABW rekomenduje, aby nie eksponować danych osobowych sprawców zamachu, szczególnie ich nazwisk**, gdyż bardzo często leży to w interesie terrorystów. Komunikację należy skupić przede wszystkim na świadczeniu wsparcia dla ofiar zdarzenia. Należy również uświadomić opinię publiczną co do tego, że zamach nie wpłynie na działalność danej instytucji lub bardzo szybko zostanie przywrócone jej funkcjonowanie w pełnym zakresie, a więc cel sprawców nie zostanie osiągnięty.

Prowadząc komunikację po wystąpieniu incydentu

- Ustal dokładną wersję wydarzeń.
- Rozwiewaj obawy, skup się na ofiarach, a nie na sprawcach.
- Jeśli możesz – zapewnij realne wsparcie ofiarom.
- Postaraj się jak najszybciej zlikwidować szkody i przywrócić prawidłowe działanie instytucji.
- Usuwaj lub zgłaszaj wszelkie treści o charakterze terrorystycznym, zwłaszcza związane z aktem przemocy.
- Przeciwdziałaj radykalizacji w społeczeństwie (próbie odwetu) i debacie publicznej (mowie nienawiści).

Schemat blokowy trzech etapów komunikacji

Rekomendacje skutecznej komunikacji

1. Ustal system komunikacji i procedur reagowania.
2. Załóż, utrzymuj i promuj konto w mediach społecznościowych do wykorzystania w sytuacjach kryzysowych – informacje przekażesz szybciej niż przez media tradycyjne.
3. W sytuacji zagrożenia reaguj i przejmij inicjatywę.
4. Współpracuj z innymi instytucjami podczas sytuacji kryzysowej.

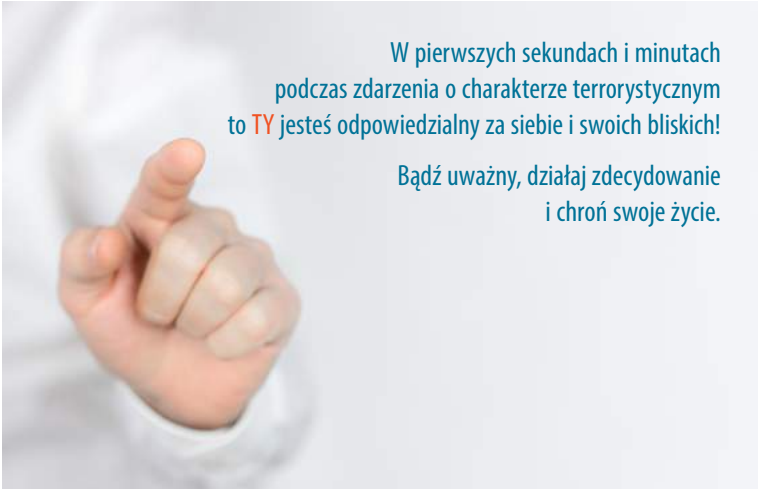
Zachęcamy do zapoznania się z Księgą Komunikacji Kryzysowej przygotowaną przez Rządowe Centrum Bezpieczeństwa dostępnej na stronie: https://rcb.gov.pl/ksiega-komunikacji-kryzysowej-2017/

16 Podsumowanie

- Radykalizacja może prowadzić do przemocy, a nawet terroryzmu. Nie bądź obojętny. Poproś inne osoby o wsparcie i skontaktuj się z odpowiednią instytucją (szkołą lub miejscem zatrudnienia danej osoby).
- Jeśli podejrzewasz, że dana osoba przygotowuje się lub wyraża chęć dokonania aktu przemocy – powiadom służby pod numerem alarmowym 112. **Możesz zapobiec tragedii!**
- Zwracaj uwagę na pozostawione bez opieki bagaże i pakunki. Jeżeli ich właściciel się nie znajdzie – powiadom ochronę i (lub) Policję.
- Jeśli odbierasz w swoim miejscu pracy przesyłki pocztowe, uważaj na cechy mogące świadczyć o tym, że przesyłka jest niebezpieczna.
- W przypadku wystąpienia zagrożenia o charakterze terrorystycznym postępuj zgodnie z procedurą **4U!** – Uważaj -> Uciekaj -> Ukryj się -> Udaremnij atak!
- Jeżeli udzielasz pomocy w sytuacji zagrożenia – w pierwszej kolejności zadbaj o własne bezpieczeństwo. Pamiętaj, że najważniejsze jest zatamowanie masywnych krwawień. Zaopatrz swoją apteczkę w dodatkowe środki pomocy medycznej.
- Jeżeli jesteś osobą odpowiedzialną za bezpieczeństwo w Twoim miejscu pracy, wprowadź dodatkowe procedury i zabezpieczenia na wypadek zagrożeń o charakterze terrorystycznym. Możesz zacząć od tych najłatwiejszych do wdrożenia, które zostały zawarte w Rekomendacjach przedstawionych przez CPT ABW.

Pełną treść Rekomendacji Szefa ABW w zakresie profilaktyki antyterrorystycznej w budynkach użyteczności publicznej administracji państwowej znajdziesz na stronie: https://tpcoe.gov.pl/cpt/materialy/1649,Rekomendacje-w-zakresie-profilaktyki-antyterrorystycznej.html

- Jeśli masz możliwość – bierz udział w szkoleniach z zakresu prewencji terrorystycznej i udzielania pierwszej pomocy lub deleguj podległych pracowników na takie szkolenia. Wysoki poziom świadomości antyterrorystycznej i przeszkolenia zwiększa szansę na identyfikację potencjalnych zagrożeń i właściwy sposób reakcji.
- Pamiętaj o bezpiecznym korzystaniu z Internetu i nowych technologii. Nie wchodź na podejrzane strony internetowe, nie pobieraj załączników z wiadomości e-mail od nieznanych osób, stosuj silne i zróżnicowane hasła oraz nie udostępniaj prywatnych i wrażliwych informacji w Internecie.
- Nie powielaj informacji związanych z terroryzmem w Internecie. Pamiętaj, że ugrupowania terrorystyczne rozpowszechniają w sieci radykalne treści i starają się pozyskiwać nowych zwolenników – szczególnie osoby młode.



17 Materiały

Stopnie alarmowe i stopnie alarmowe CRP

Podstawa prawna: Zarządzenie Nr 18 Prezesa Rady Ministrów z dnia 2 marca 2016 r. w sprawie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego.

1 stopień zagrożenia — **Poziom niski**

ALFA
ALFA – CRP
(w przypadku zagrożeń w cyberprzestrzeni)
Brak informacji wskazujących bezpośrednio na zagrożenie o charakterze terrorystycznym

2 stopień zagrożenia — **Poziom umiarkowany**

BRAVO
BRAVO – CRP
(w przypadku zagrożeń w cyberprzestrzeni)
Zdarzenie o charakterze terrorystycznym jest mało prawdopodobne, ale występują informacje wskazujące możliwość wystąpienia

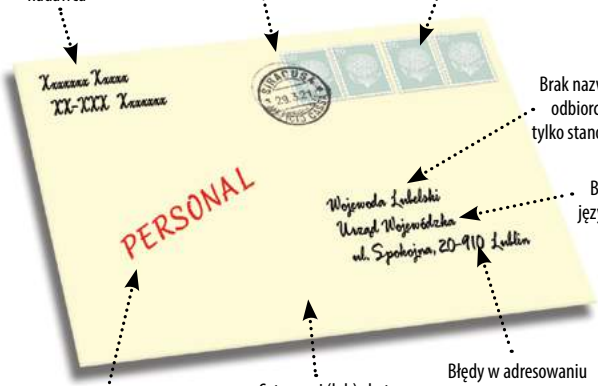
3 stopień zagrożenia — **Poziom wysoki**

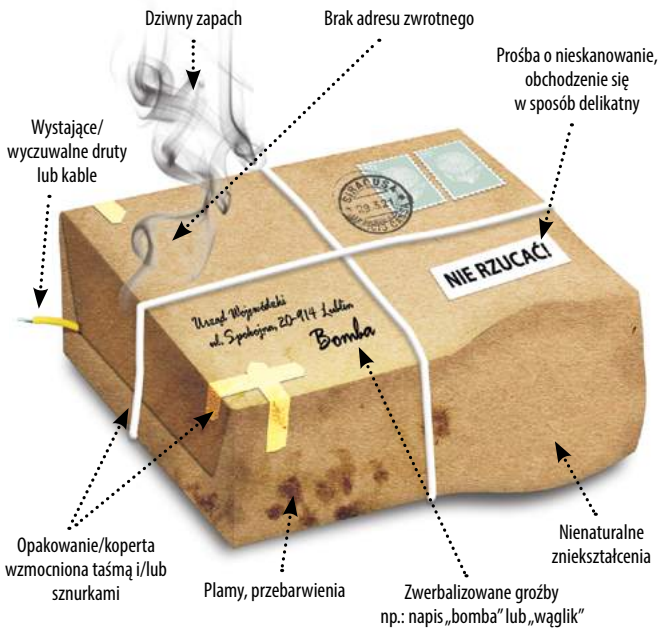
CHARLIE
CHARLIE – CRP
(w przypadku zagrożeń w cyberprzestrzeni)
Zdarzenie o charakterze terrorystycznym jest prawdopodobne oraz występują potwierdzone informacje o możliwości jego wystąpienia

4 stopień zagrożenia — **Poziom bardzo wysoki**

DELTA
DELTA – CRP
(w przypadku zagrożeń w cyberprzestrzeni)
Wystąpiło zdarzenie o charakterze terrorystycznym lub uzyskane informacje wskazują na końcową fazę jego przygotowania

Cechy podejrzanej przesyłki





Formularz przyjęcia informacji o zagrożeniu

Uwaga: dokument powinien być przechowywany w miejscu dostępnym dla pracownika, na stanowisku pracy, w pobliżu aparatu telefonicznego

Treść słów wypowiadanych przez zawiadamiającego:

Jakiego rodzaju jest zagrożenie?

Urządzenie wybuchowe	Inne zagrożenie
Kiedy urządzenie wybuchowe eksploduje?	Kiedy zagrożenie zaistniało?
Gdzie jest w tej chwili urządzenie wybuchowe?	Jakiego miejsca dotyczy?
Jakiego rodzaju jest to urządzenie i co zawiera?	Kto jest zagrożony?
Jak wygląda urządzenie wybuchowe?	Jak mogę się do Pana/Pani zwracać?
W którym miejscu zostało podłożone?	Kto jest sprawcą zagrożenia i dlaczego?
Dlaczego podłożono urządzenie wybuchowe?	Jak można uniknąć zagrożenia?
Jak mogę się do Pana/Pani zwracać?	Czy można Panu/Pani pomóc?
Czy Pan/Pani jest konstruktorem urządzenia wybuchowego?	Skąd Pan/Pani telefonuje?
Skąd Pan/Pani telefonuje?	

CZĘŚĆ FORMULARZA WYPEŁNIANA PO PRZEPROWADZENIU ROZMOWY Podstawowe informacje dotyczące zawiadamiającego			
Forma kontaktu	Data i godzina przekazania informacji		Płeć
Nr telefonu Adres e-mail	Długość kontaktu		Wiek
Opis głosu zawiadamiającego:	Opis języka zawiadamiającego:	Opis zachowania się zawiadamiającego:	Dźwięk tła:
Akcent	Wykształcony	Spokojny	Biuro
Głośny/Cichy	Wulgarny	Rozsądny	Fabryka, zakład
Szybki/Wolny	Obcojęzyczny	Rozgniewany	Ulica
Niski/Wysoki	Nagrany	Desperacki	Dworzec
Ciepły/Chrapliwy	Nieracjonalny	Arogancki	Głos ludzki
Jąkający się	Niezrozumiały	Nieracjonalny	Zwierzęta
Zniekształcony		Wesoły	Muzyka
Bełkotliwy			Klimatyzator
Sepleniący			Inne
Inne uwagi dotyczące zawiadamiającego:			
Inne uwagi przyjmującego zgłoszenie:			
Zgłoszenie przyjął (imię, nazwisko, miejsce przyjęcia zgłoszenia – nr telefonu, adres e-mail, miejsce przyjęcia informacji)			
Zgłoszenie zostało przekazane do: Imię, nazwisko oraz stanowisko: Data, godzina przekazania informacji: Podpis:		Polecenia i uwagi osoby, do której przekazano zgłoszenie:	

TERRORISM
PREVENTION
Centre of Excellence

Centrum Prewencji Terrorystycznej ABW

00-993 Warszawa
ul. Rakowiecka 2A
e-mail: kontakt.cpt@abw.gov.pl
www.tpcoe.gov.pl