Zagrożenia czasu pokoju – terroryzm cyberzagrożenia

Tomasz A. Winiarczyk

zagrożenie

- **zdarzenie powstające losowo lub wywołane celowo**,
  które wywiera negatywny wpływ na funkcjonowanie politycznych i gospodarczych struktur państwa, na warunki bytowania ludności oraz stan środowiska naturalnego

zagrożenie

- zjawisko wywołane działaniem sił natury bądź człowieka,
  które powoduje, że poczucie bezpieczeństwa maleje bądź zupełnie zanika

https://pl.wikipedia.org/wiki/Zagro%C5%BCenie

zagrożenie a ryzyko

- ryzyko to wskaźnik stanu lub zdarzenia, które może prowadzić do strat
  - jest proporcjonalne do prawdopodobieństwa wystąpienia zdarzenia i do wielkości strat, które może spowodować
- ryzyko następuje jako skutek zagrożenia
- ryzyko mierzy się jako własność zdarzenia i miary wartości szkody spowodowanej przez to zdarzenie dla społeczeństwa

klasyfikacja zagrożeń ze względu na rozmiar

- globalne
- regionalne
- lokalne

klęska żywiołowa

- **katastrofa naturalna** lub **awaria techniczna**, których skutki zagrażają życiu lub zdrowiu dużej liczby osób, mieniu w wielkich rozmiarach albo środowisku na znacznych obszarach,
  a pomoc i ochrona mogą być skutecznie podjęte tylko przy zastosowaniu nadzwyczajnych środków,
  we współdziałaniu różnych organów i instytucji oraz specjalistycznych służb i formacji działających pod jednolitym kierownictwem

klęska żywiołowa – **katastrofa naturalna**

- zdarzenie związane z działaniem sił natury, w szczególności wyładowania atmosferyczne, wstrząsy sejsmiczne, silne wiatry, intensywne opady atmosferyczne, długotrwałe występowanie ekstremalnych temperatur, osuwiska ziemi, pożary, susze, powodzie, zjawiska lodowe na rzekach i morzu oraz jeziorach i zbiornikach wodnych, masowe występowanie szkodników, chorób roślin lub zwierząt albo chorób zakaźnych ludzi albo też działanie innego żywiołu

klęska żywiołowa – **awaria techniczna**

- gwałtowne, nieprzewidziane uszkodzenie lub zniszczenie obiektu budowlanego, urządzenia technicznego lub systemu urządzeń technicznych powodujące przerwę w ich używaniu lub utratę ich właściwości

szczególny przypadek katastrofy/awarii

- **Katastrofą naturalną lub awarią techniczną może być również zdarzenie wywołane działaniem terrorystycznym**

art. 4 ustawy o stanie klęski żywiołowej

1. Stan klęski żywiołowej może być wprowadzony na obszarze, na którym wystąpiła klęska żywiołowa, a także na obszarze, na którym wystąpiły lub mogą wystąpić skutki tej klęski.
2. Stan klęski żywiołowej wprowadza się na czas oznaczony, niezbędny dla zapobieżenia skutkom klęski żywiołowej lub ich usunięcia, nie dłuższy niż 30 dni.

rozporządzenie

- Rada Ministrów, w drodze rozporządzenia, może wprowadzić stan klęski żywiołowej z własnej inicjatywy lub na wniosek właściwego wojewody.
- W rozporządzeniu określa się przyczyny, datę wprowadzenia oraz obszar i czas trwania stanu klęski żywiołowej, a także, w zakresie dopuszczonym niniejszą ustawą, rodzaje niezbędnych ograniczeń wolności i praw człowieka i obywatela.

inne miejscowe zagrożenie

- zdarzenie wynikające z rozwoju cywilizacyjnego i naturalnych praw przyrody niebędące pożarem ani klęską żywiołową,
  stanowiące zagrożenie dla życia, zdrowia, mienia lub środowiska,
  któremu zapobieżenie lub którego usunięcie skutków nie wymaga zastosowania nadzwyczajnych środków

Zagrożenie terroryzmem

- definicja terroryzmu
- wyróżniki współczesnego terroryzmu
- podejrzana/niebezpieczna osoba
- atak uzbrojonego napastnika w budynku
- zamach bombowy
- podejrzana rzecz/przesyłka
- podejrzany pojazd
- zachowanie w razie informacji o podłożeniu ładunku wybuchowego
- żywe bomby
- zachowanie w razie wybuchu
- wzięcie zakładnika
- szturm jednostki antyterrorystycznej

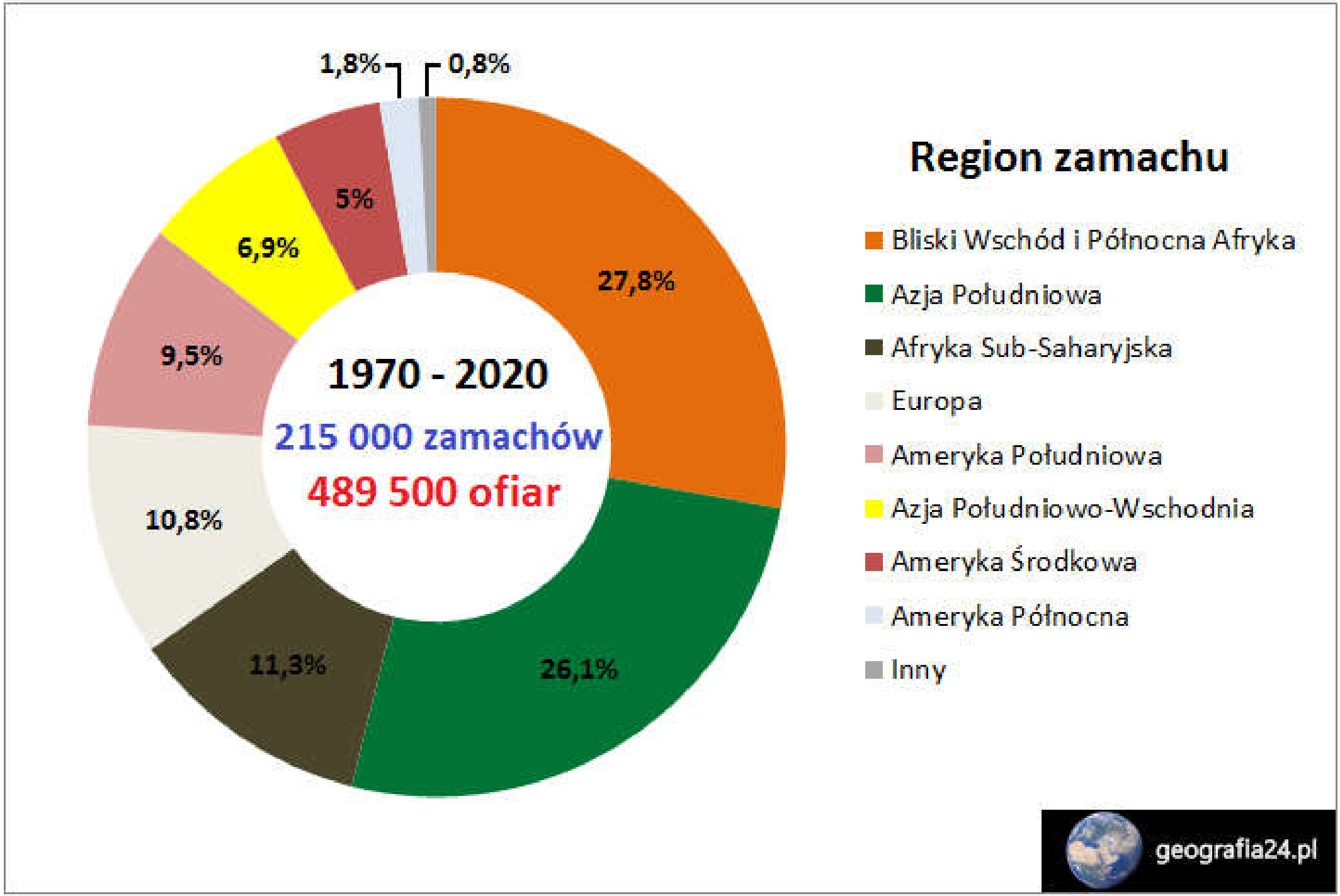
zagrożenie terroryzmem

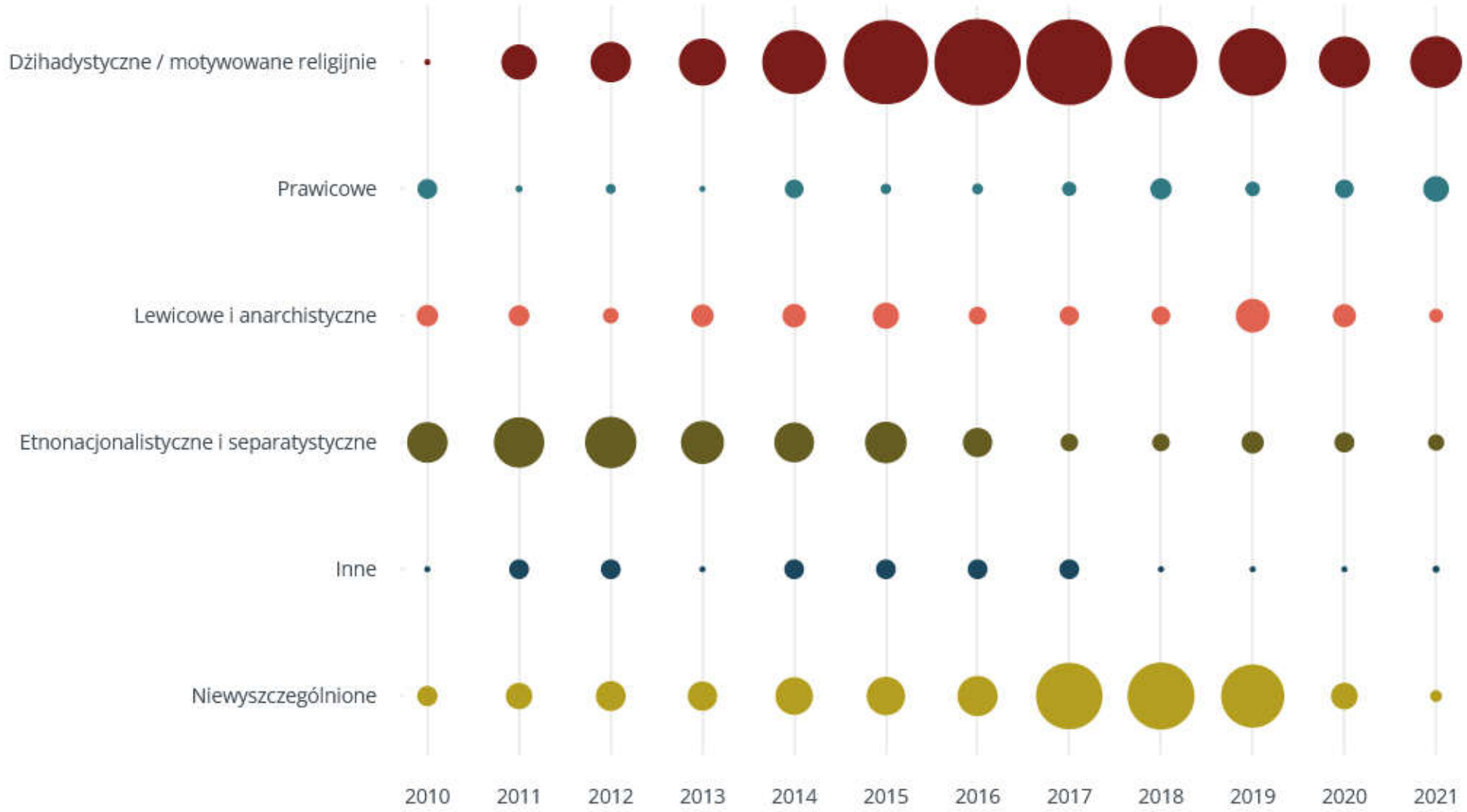
- **terroryzm** – użycie siły lub przemocy psychicznej przeciwko osobom lub własności z pogwałceniem prawa, mające na celu zastraszenie i wymuszenie na danej grupie ludności lub państwie ustępstw w drodze do realizacji określonych celów

996 – numer alarmowy do Centrum Antyterrorystycznego

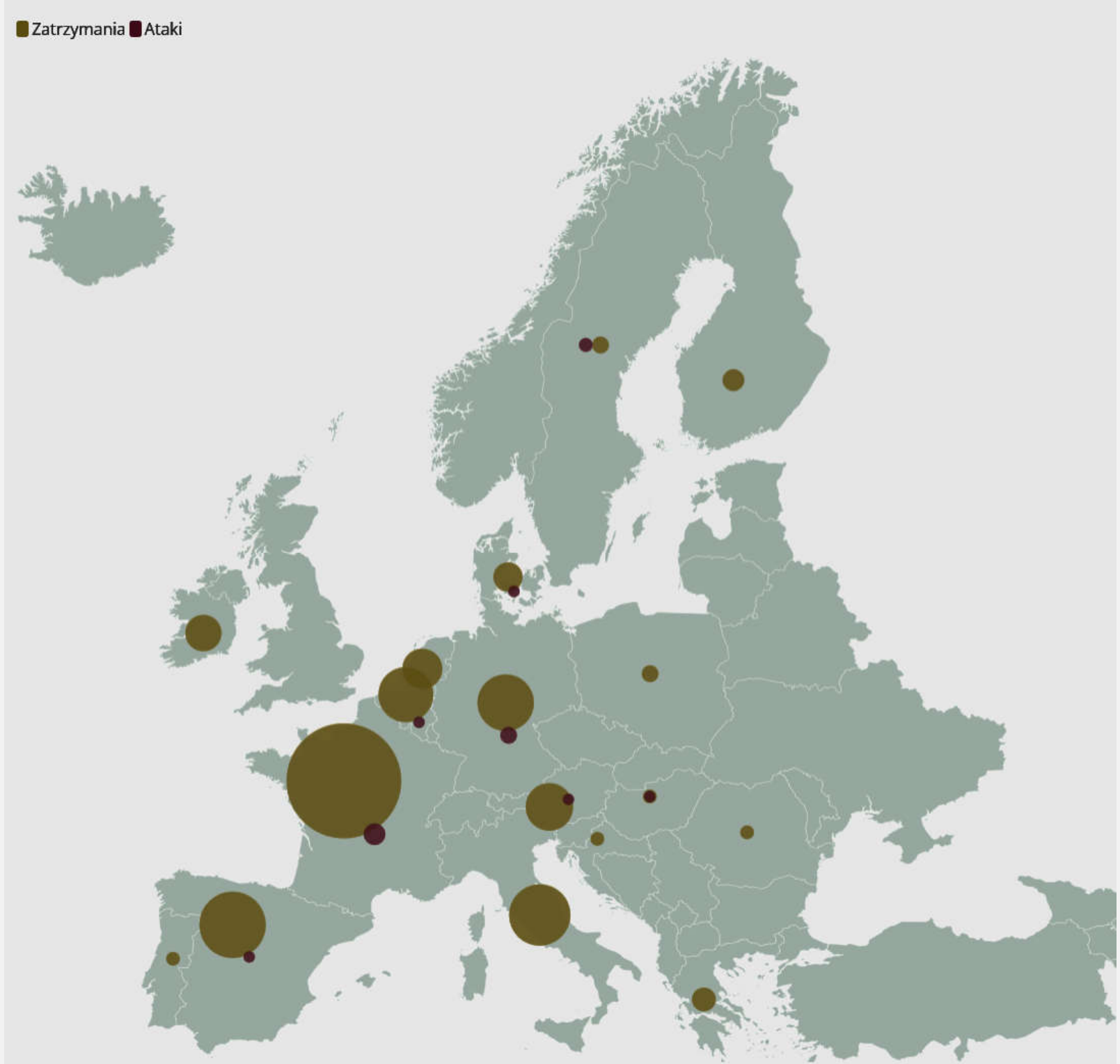
terroryzm współczesny – wyróżniki

- gloryfikacja siły jako metody walki politycznej
- okrucieństwo i brak skrupułów moralnych
- wzbudzenie silnego i powszechnego poczucia zagrożenia
- uzyskanie rozgłosu
- polityczny szantaż i wymuszenie określonych zmian politycznych
- duża możliwość uniknięcia kary
- przygotowanie sytuacji rewolucyjnej


1,8%
0,8%
5%
6,9%
27,8%
9,5%
1970 - 2020
215 000 zamachów
489 500 ofiar
10,8%
11,3%
26,1%
Region zamachu
Bliski Wschód i Północna Afryka
Azja Południowa
Afryka Sub-Saharyjska
Europa
Ameryka Południowa
Azja Południowo-Wschodnia
Ameryka Środkowa
Ameryka Północna
Inny
geografia24.pl



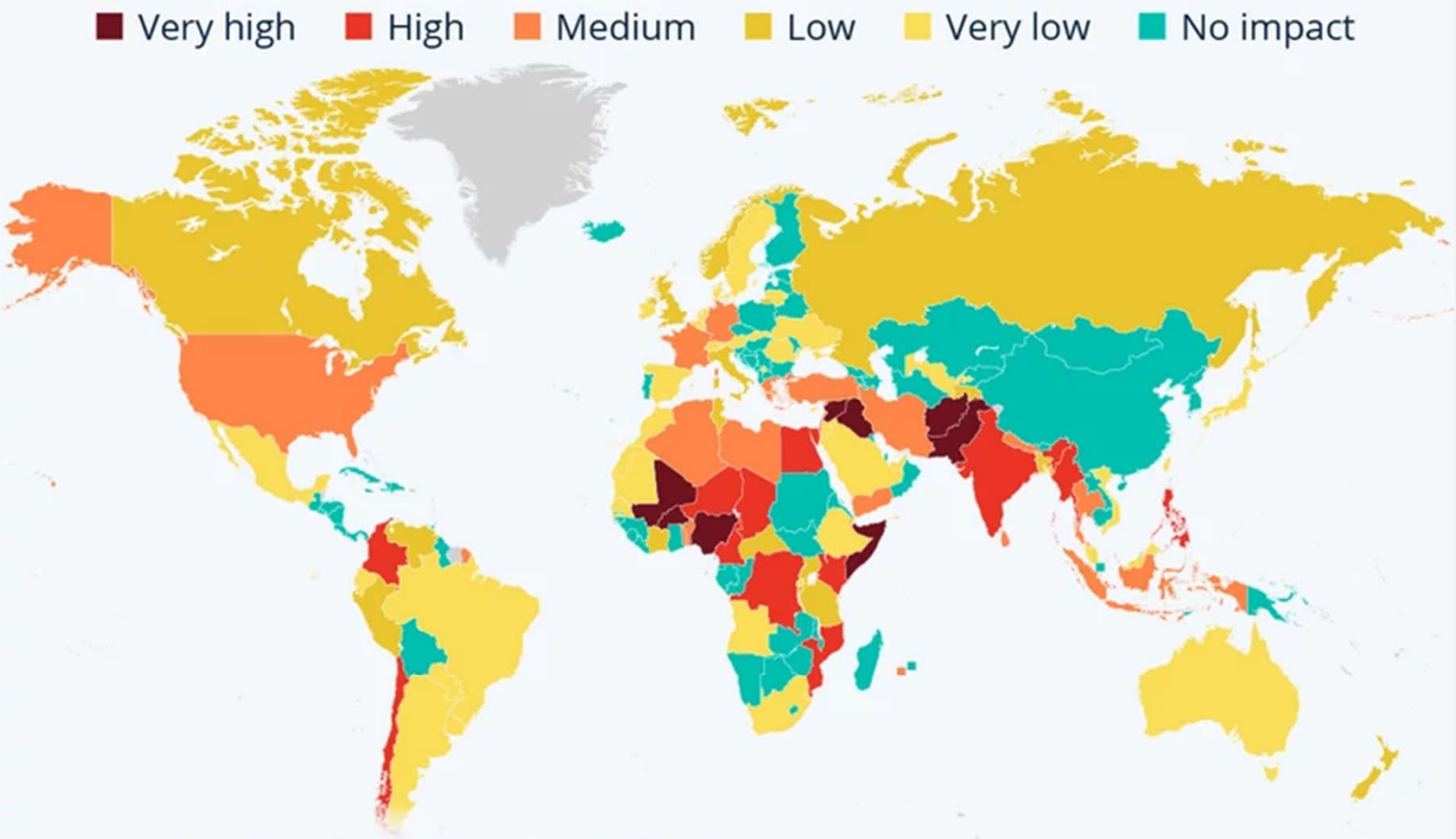
Źródło: Roczne sprawozdanie Europolu dotyczące sytuacji i tendencji w dziedzinie terroryzmu w UE (2011–2022)
*Dane za lata 2010–2019 obejmują Wielką Brytanię



Źródło: Roczne sprawozdanie Europolu dotyczące sytuacji i tendencji w dziedzinie terroryzmu w UE (2021)

The Impact of Terrorism Around the World

Impact of terrorism in countries according to the Global Terrorism Index (2023)

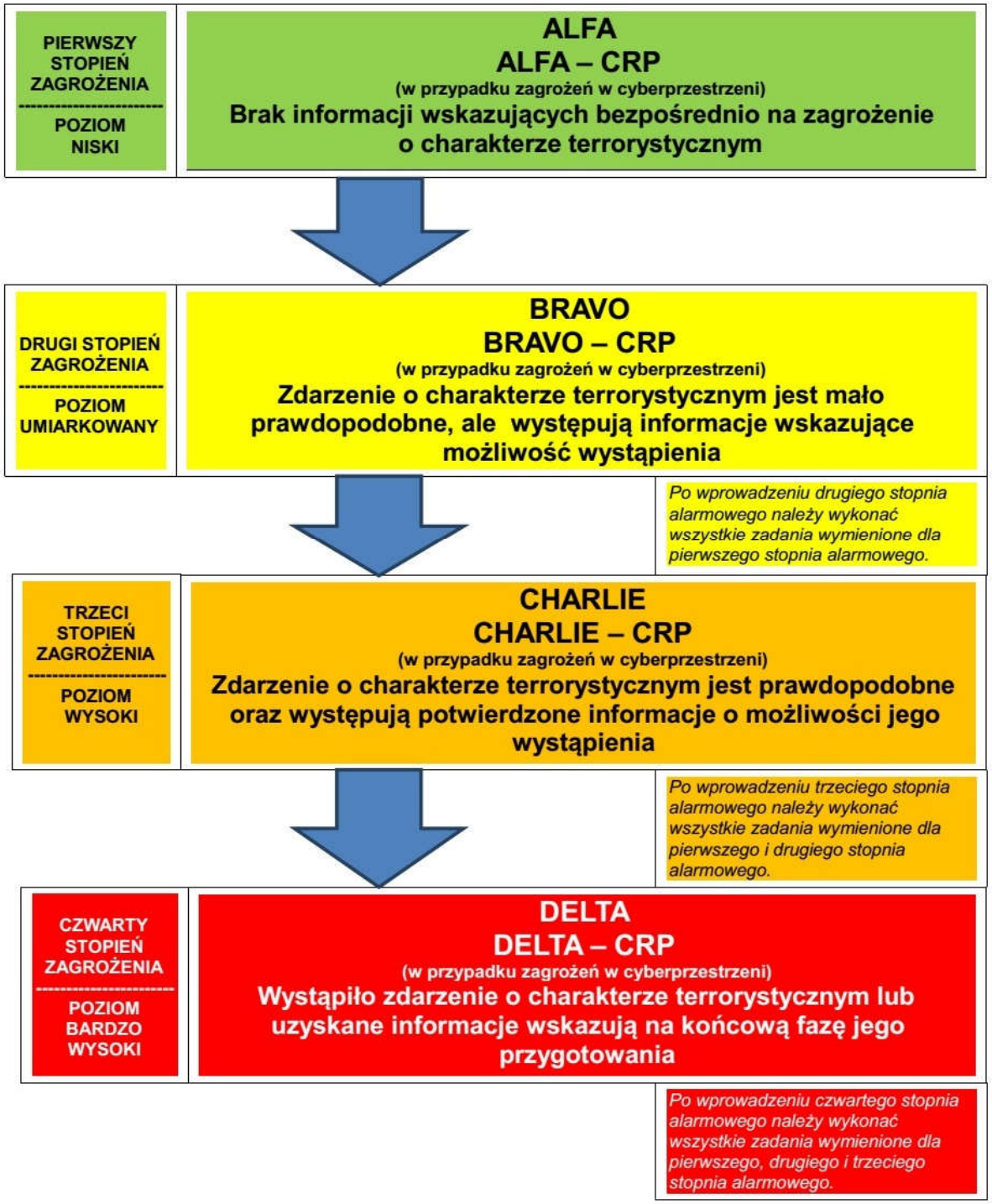


Source: Institute for Economics and Peace

statista

STOPNIE ALARMOWE I STOPNIE ALARMOWE CRP

Podstawa prawna: Zarządzenie Nr 163 Prezesa Rady Ministrów z dnia 1 grudnia 2016 r. w sprawie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego.



podejrzana/niebezpieczna osoba

- dyskretnie poinformuj o swoich podejrzeniach osobę odpowiedzialną
- pozostań z osobą w kontakcie wzrokowym
- w miarę możliwość krzyknij do osoby, by ją zdekoncentrować
- w razie możliwości skróć dystans, odciągając uwagę tej osoby
- przejmij kontrolę fizyczną nad nią – zwłaszcza nad rękami i ramionami

atak uzbrojonego napastnika w budynku

- Uciekaj z miejsca zagrożenia, jeśli jest to możliwe (cicho i zostawiwszy rzeczy)
- Jeżeli bezpieczna ewakuacja nie jest możliwa:
  - zamknij drzwi od pomieszczenia i zabarykaduj się
  - wyłącz telefon komórkowy i inne źródła dźwięków
  - połóż się na ziemi z dala od drzwi i okien
  - bądź absolutnie cicho
  - oczekuj przybycie służb

najtrudniejsze jest pierwsze 45 minut – potem sytuacja się stabilizuje

atak uzbrojonego napastnika w budynku – kontakt bezpośredni

- nie odzywaj się niepotrzebnie
- próbuj zachować spokój, skup się na przyjemnych myślach
- co do zasady nie groź ani nie walcz
- stosuj się do poleceń napastnika (-ów)
- nie odwracaj się tyłem, bądź człowiekiem z konkretną twarzą
- nie próbuj uciekać
- nie patrz napastnikom prosto w oczy
- nie żartuj ani nie rozmawiaj na tematy kontrowersyjne
- jeśli dają jeść i pić, korzystaj
- w sytuacjach ostatecznych walcz albo błagaj o litość

wzięcie ciebie jako zakładnika

- to nie ty kontrolujesz sytuację – podporządkuj się poleceniom napastnika/porywacza
- staraj się zapamiętywać jak najwięcej szczegółów dot. napastnika i otoczenia
- nie prowokuj, nie wyróżniaj się
- jedz i pij, ale staraj się nie chodzić do toalety
- nie odzywaj się bez potrzeby
- w razie strzałów czy wybuchów – kładź się na podłodze

JAK POSTĘPOWAĆ W PRZYPADKU ZAGROŻENIA TERRORYSTYCZNEGO

bezpiecznej

WYBUCH

uciekaj

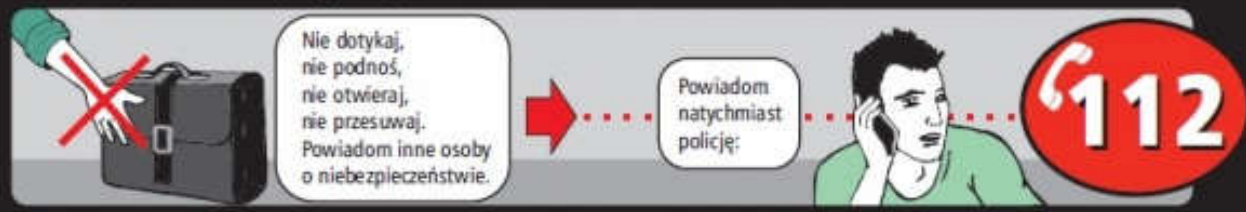
STRZELANINA

ukryj się

WZIĘCIE ZAKŁADNIKÓW

nie stawiaj oporu

PODEJRZANY BAGAŻ/PAKUNEK



MIASTO STOŁECZNE WARSZAWA

zamach bombowy

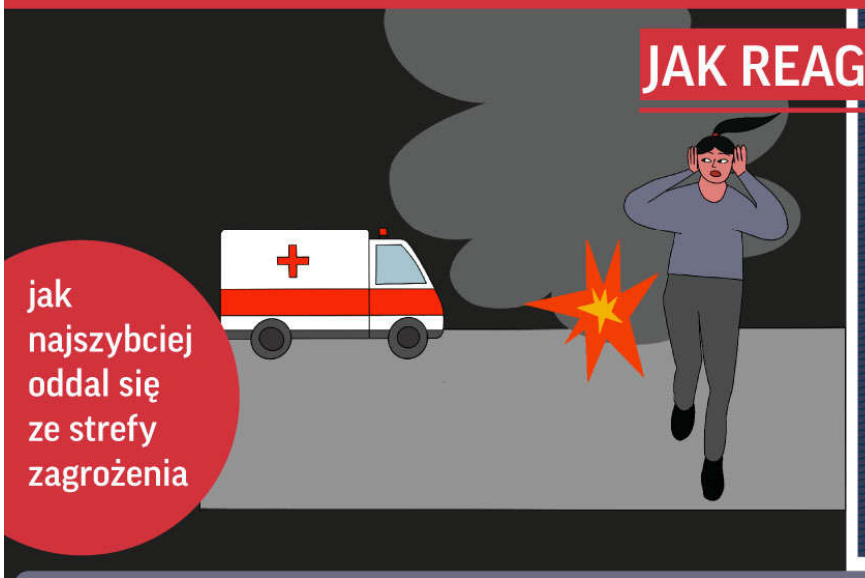
- często stosowana metoda ataku terrorystycznego
- może być przeprowadzony zdalnie bądź w postaci ataku samobójczego
- powoduje duże szkody osobowe i rzeczowe
- nie rozróżnia swoich i obcych

ZAGROŻENIE TERRORYSTYCZNE - ALARM BOMBOWY

nie dotykaj przedmiotów pozostawionych bez opieki

NA CO ZWRÓCIĆ UWAGĘ

- nietypowe zachowania osób
- pojazdy zaparkowane w nietypowych miejscach
- anonimowe przesyłki



jak najszybciej oddal się ze strefy zagrożenia

JAK REAGOWAĆ

- o swoich podejrzeniach powiadom służby
- stosuj się do poleceń służb
- zachowaj spokój

112

rcb.gov.pl @RCB_RP @rzadowecentrumbezpieczenstwa @rcbgovpl

RCB | Rządowe Centrum Bezpieczeństwa

podejrzana rzecz/przesyłka

- pozostawione przedmioty jak teczki, paczki, pakunki itp. powinny zaniepokoić
- uwaga na przesyłki, których się nie spodziewamy, noszące ślady rozpakowywania, nie posiadające oznaczeń pocztowych
- przesyłki, których doręczyciel nie oczekuje pokwitowania, warto traktować jako podejrzane

nie dotykaj ani nie przenoś takiej rzeczy/przesyłki

zabezpiecz miejsce, w którym pozostawiono rzecz

oddal się od tego miejsca

powiadom odpowiednie służby

podejrzany pojazd

- zaparkowany w nietypowym miejscu
- zaparkowany przez dłuższy czas w miejscu, gdzie jest zakaz parkowania
- może wyglądać na przeładowany
- kierowca pojazdu zdradza oznaki niepokoju

nie dotykaj ani nie otwieraj drzwi takiego pojazdu

oddal się od tego miejsca

powiadom odpowiednie służby

próbuj rozproszyć gapiów

żywe bomby – czy można rozpoznać

- osoba podenerwowana albo wykazująca całkowite panowanie nad emocjami
- wygląda nietypowo
- ubrana nieodpowiednio do sytuacji pogodowej
- nosi luźny ubiór
- niesie ciężki bagaż
- ukrywa ręce i bladą twarz
- ma skupiony wzrok
- wygląda, jakby porozumiewała się z innymi dziwnymi znakami
- to nie musi być osoba wyglądająca na cudzoziemca

zachowanie w razie informacji o podłożeniu ładunku wybuchowego

- w razie zgłoszenia telefonicznego postaraj się opanować i przedłużając rozmowę, uzyskać jak najwięcej informacji
- w miarę możliwości rozmowę nagrywaj
- próbuj wyłapać informacje pozawerbalne: cechy głosu osoby, tło dźwiękowe rozmowy
- pytaj, kto i dlaczego podkłada ładunek
- pytaj, co należy zrobić, by do wybuchu nie doszło

nigdy nie wolno traktować takiej informacji jako żartu

konieczne zarządzenie ewakuacji i powiadomienie stosownych służb

w trakcie ewakuacji z powodu bomby należy koniecznie zabrać swoje rzeczy

podręcznik wyd. Operon

Postępowanie po otrzymaniu telefonu z informacją o podłożeniu ładunku wybuchowego	
Rozmowę prowadź spokojnie i uprzejmie.	W większości przypadków możesz się spodziewać krótkiej informacji ze wskazaniem miejsca, w którym jest podłożona bomba. Opanuj emocje, nie ogłaszaj tego gwałtownie, ponieważ możesz wywołać panikę, nie podnoś głosu na rozmówcę w trakcie rozmowy.
Poinformuj przełożonego, policję.	Im wcześniej powiadomisz odpowiednie służby, tym szybciej zostaną podjęte odpowiednie działania.
Okazuj zainteresowanie rozmówcy, zadawaj pytania.	Pytaj o wygląd i rodzaj ładunku, czas detonacji oraz to, co skłoniło rozmówcę do czynu, zapisuj podawane informacje – będą one bardzo pomocne dla policji.
Zapamiętaj godzinę zgłoszenia, płeć rozmówcy i wygłoszone żądania.	
Staraj się uświadomić sprawcy skutki jego czynu.	Informuj zwłaszcza o potencjalnej liczbie ofiar oraz stratach, istnieje możliwość wpłynięcia na zachowanie rozmówcy, który odstąpi od swoich zamiarów. Pamiętaj, że każdy sposób jest dobry na to, aby uniknąć tragicznego w skutkach zamachu terrorystycznego.
Skup się na odgłosach w tle.	Podczas przyjmowania informacji o podłożonym ładunku staraj się skupić, jakie odgłosy są słyszalne w tle rozmowy (np. odgłosy ulicy, domowe, megafon itp.).

Źródło: *Edukacja antyterrorystyczna. Konieczność i obowiązek naszych czasów*, red. K. Jałoszyński, A. Letkiewicz, Szczytno 2010.

zachowanie w razie wybuchu

- połóż się na ziemi – najlepiej na miękkim podłożu
- nie wstawaj zbyt szybko
- nie kieruj się w stronę źródła eksplozji
- niczego nie dotykaj
- staraj się nie zatrzeć żadnych śladów
- jeśli możesz, pomóż poszkodowanym
- kieruj się do stref bezpiecznych
- w razie konieczności wspomóż służby ratownicze i porządkowe

szturm jednostki antyterrorystycznej

- połóż się na podłodze
- zabezpiecz drogi oddechowe
- nie podnoś się bez wyraźnego polecenia
- nie podnoś żadnych rzeczy
- **pamiętaj**: wszyscy są najpierw traktowani jak ewentualni pomocnicy terrorystów
- nie stawiaj oporu i wykonuj wszystkie polecenia funkcjonariuszy

Zagrożenia cyberbezpieczeństwa
Cyberprzemoc

Tomasz A. Winiarczyk

cyberbezpieczeństwo
= bezpieczeństwo teleinformatyczne

- ogół technik, procesów i praktyk stosowanych w celu ochrony sieci informatycznych, urządzeń, programów i danych przed atakami, uszkodzeniami lub nieautoryzowanym dostępem

podręcznik wyd. Operon

Wypadki – zagrożenie losowe o zewnętrznym pochodzeniu, zależnym w różnym stopniu od czynników technicznych; nie muszą sugerować celowego działania o negatywnych przesłankach.

Awarie – zdarzenia o charakterze losowym, wywołane działaniem wewnętrznym, zależnym w różnym stopniu od czynników technicznych; nie muszą sugerować celowego działania o negatywnych przesłankach.

Ataki – wydarzenia umyślne, sprowokowane ingerencją człowieka.

Obraźliwe i nielegalne treści:

spam
dyskredytacja, obrażanie
pornografia dziecięca
przemoc

Złośliwe oprogramowanie:

wirus
robak sieciowy
koń trojański
oprogramowanie szpiegowskie
dialer
rootkit

ZAGROŻENIA CYBERBEZPIECZEŃSTWA

Gromadzenie informacji:

skanowanie
podsłuch
inżynieria społeczna

Próby włamań i włamania:

wykorzystanie znanych luk systemowych
próby nieuprawnionego logowania
wykorzystanie nieznanych luk systemowych
włamanie na konto uprzywilejowane
włamanie na konto zwykłe
włamanie do aplikacji
bot

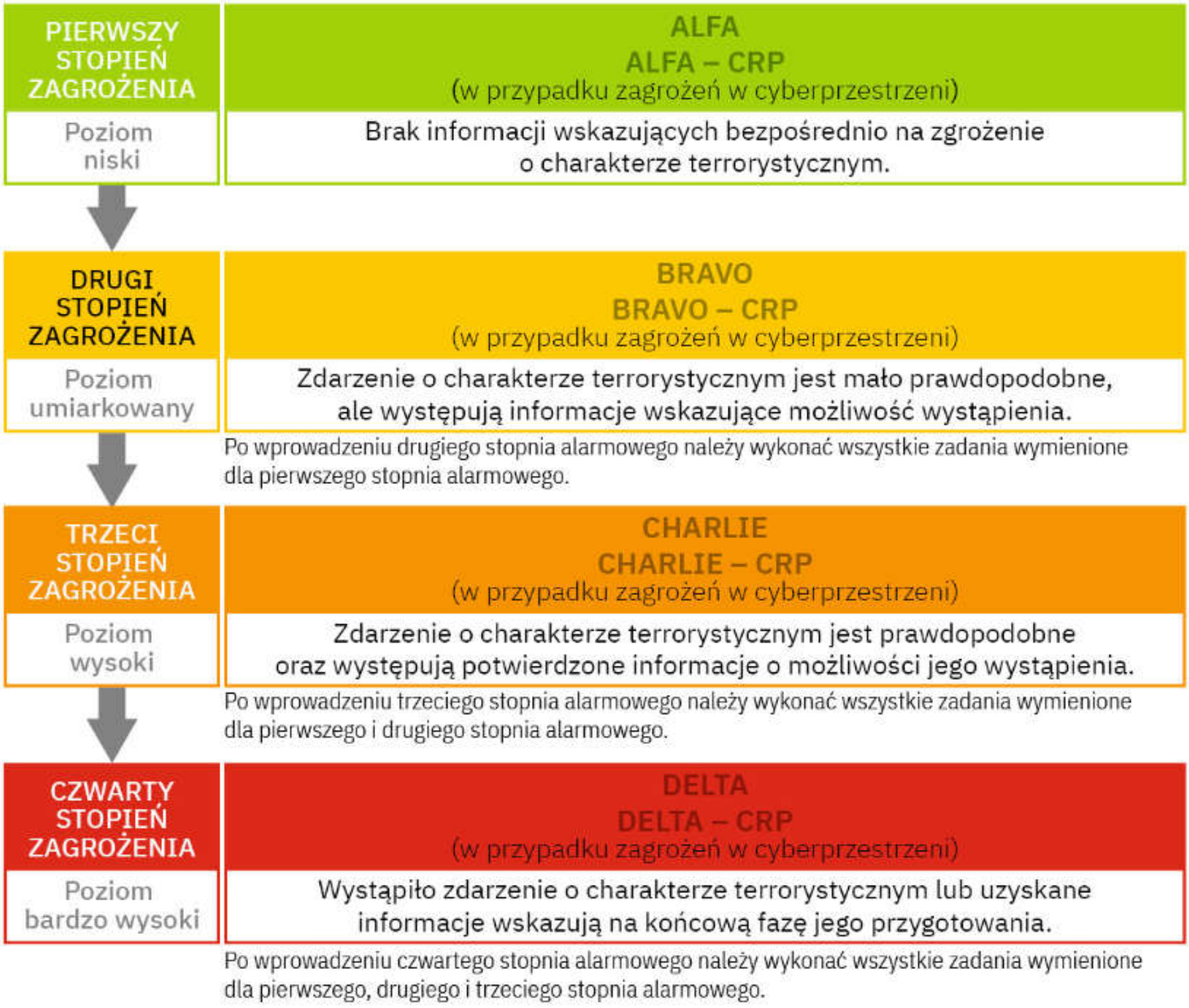
Zagrożenia bezpieczeństwa informacji i dostępu do zasobów cyfrowych:

atak odmowy usługi (DoS)
rozproszony atak odmowy usługi (DDoS)
sabotaż komputerowy
przerwa w działaniu usług
nieuprawniony dostęp do informacji
nieuprawnione przetwarzanie informacji
nieuprawnione wykorzystanie zasobów
naruszenie praw autorskich
kradzież tożsamości, podszycie się
phishing

Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT)

- Ustawa o krajowym systemie cyberbezpieczeństwa ustanowiła trzy Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego: CSIRT NASK, CSIRT GOV oraz CSIRT MON. Każdy z CSIRT odpowiedzialny jest za koordynację incydentów zgłaszanych przez przyporządkowane zgodnie z ustawą podmioty.
  - CSIRT GOV – prowadzony jest przez Agencję Bezpieczeństwa Wewnętrznego
    - główne zadania CSIRT GOV to:

      rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej
  - CSIRT MON – prowadzony przez Ministerstwo Obrony Narodowej
    - CSIRT MON koordynuje incydenty zgłaszane przez podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane oraz przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym
  - CSIRT NASK – prowadzony jest przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy
    - *CSIRT NASK zobowiązany jest do koordynacji incydentów zgłaszanych przez pozostałe podmioty, w tym obywateli*


PIERWSZY STOPIEŃ ZAGROŻENIA
Poziom niski
ALFA
ALFA – CRP
(w przypadku zagrożeń w cyberprzestrzeni)
Brak informacji wskazujących bezpośrednio na zgrożenie o charakterze terrorystycznym.
DRUGI 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.
Po wprowadzeniu drugiego stopnia alarmowego należy wykonać wszystkie zadania wymienione dla pierwszego stopnia alarmowego.
TRZECI 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.
Po wprowadzeniu trzeciego stopnia alarmowego należy wykonać wszystkie zadania wymienione dla pierwszego i drugiego stopnia alarmowego.
CZWARTY 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.
Po wprowadzeniu czwartego stopnia alarmowego należy wykonać wszystkie zadania wymienione dla pierwszego, drugiego i trzeciego stopnia alarmowego.

Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy

- państwowy instytut badawczy, którego misją jest poszukiwanie i wdrażanie rozwiązań, służących rozwojowi sieci teleinformatycznych w Polsce oraz poprawie ich efektywności i bezpieczeństwa
- https://cyberprofilaktyka.pl/baza-wiedzy/publikacje.html

CSIRT = Computer Security Incident Response Team
CERT = Computer Emergency Response Team

CERT Polska

- zespół powołany do reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet
- działa w strukturach Naukowej i Akademickiej Sieci Komputerowej
- od dnia 28 sierpnia 2018 r. zespołowi CERT Polska zostały powierzone obowiązki CSIRT NASK wynikające z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa

Prześlij je nam na nr:

8080

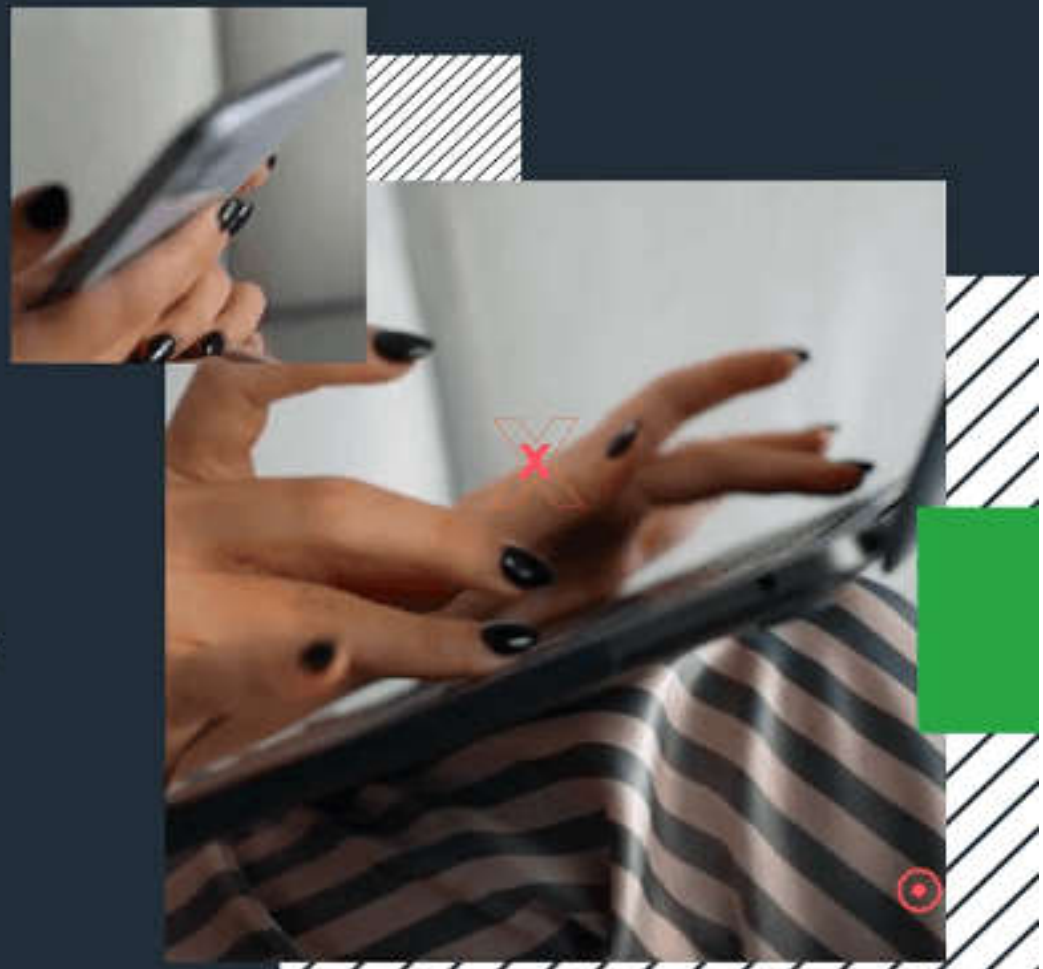
lub zgłoś przez formularz na stronie

incydent.cert.pl

albo mailowo na

cert@cert.pl

SMS bezpłatny. Koszt wysyłki w roamingu zgodny z cennikiem operatora.



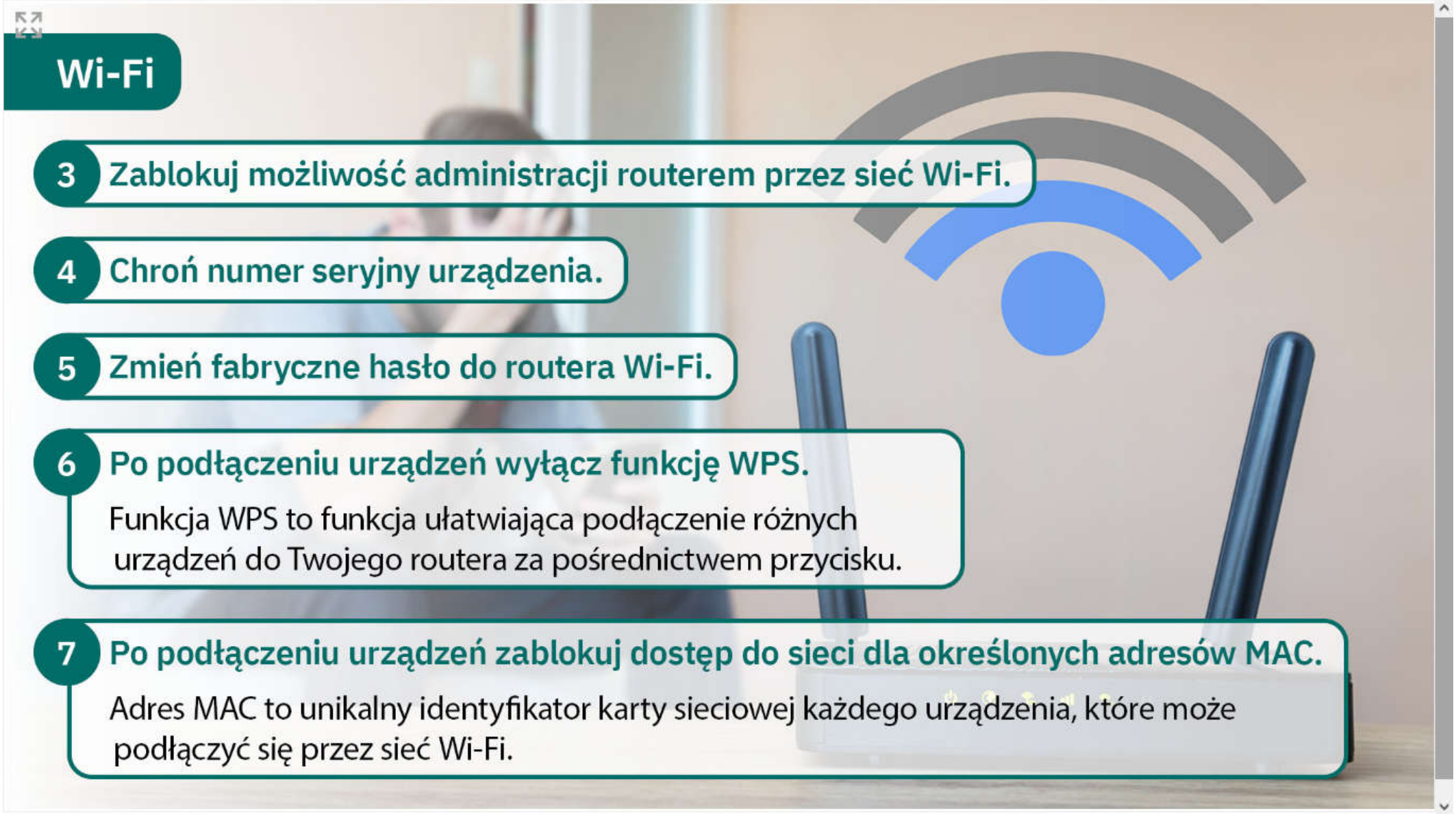
Wi-Fi

Sieć Wi-Fi to jeden z elementów infrastruktury sieciowej najbardziej podatnych na włamania przez hakerów. Sposoby zwiększające ochronę:

1 **Ustaw długie, trudne hasło do swojej sieci Wi-Fi.**

2 **Stosuj szyfrowanie WPA2 lub WPA3.**

W 2018 r. wprowadzono najnowszy i najbezpieczniejszy protokół szyfrowania połączeń – WPA3. Stosuj ten protokół, jeżeli wszystkie Twoje urządzenia mają możliwość jego wykorzystania. Obecnie starsze urządzenia są w stanie maksymalnie korzystać z protokołu WPA2. Jest to dość dobre szyfrowanie, więc jeżeli nie możesz skorzystać z WPA3, wybierz WPA2.


Wi-Fi
3 Zablokuj możliwość administracji routerem przez sieć Wi-Fi.
4 Chroń numer seryjny urządzenia.
5 Zmień fabryczne hasło do routera Wi-Fi.
6 Po podłączeniu urządzeń wyłącz funkcję WPS.
Funkcja WPS to funkcja ułatwiająca podłączenie różnych urządzeń do Twojego routera za pośrednictwem przycisku.
7 Po podłączeniu urządzeń zablokuj dostęp do sieci dla określonych adresów MAC.
Adres MAC to unikalny identyfikator karty sieciowej każdego urządzenia, które może podłączyć się przez sieć Wi-Fi.


Wi-Fi
8 Ukryj pokazywanie SSID sieci Wi-Fi.
9 Jeżeli to możliwe stosuj pasmo 5 GHz.
2,4 Ghz jest wolniejsza, ale ma większy zasięg, 5 GHz jest za to szybsza, ale ma mniejszy zasięg. Ta ostatnia właściwość (mniejszy zasięg) może okazać się także praktyczna z punktu widzenia bezpieczeństwa.
10 Zaktualizuj firmware (oprogramowanie) routera Wi-Fi.
Pamiętaj, by regularnie (raz na 1–3 miesiące) sprawdzać, czy nie wyszła aktualizacja do oprogramowania routera. Utrzymanie firmware'u w aktualnej wersji jest kluczowe do zapewnienia bezpieczeństwa.

>Poczta e-mail. Zagrożenia_

94% wszystkich złośliwych ataków jest przeprowadzana za pomocą poczty e-mail.

Phishing. Elementy procesu

Oszust

Ofiara pod którą podszywa się oszust np. sklep internetowy, firma kurierska czy bank

Phishingowa wiadomość e-mail

Ofiara, której dane są wyłudzane np. klient sklepu internetowego czy banku

jak się bronić

- Dokładnie sprawdzaj od kogo otrzymałeś wiadomość oraz czy link nie zawiera jakichś literówek:
  - fałszywy nadawca poczty może mieć przeinaczoną nazwę np. contact@netfflix.com.
- Adres strony internetowej również może nieznacznie różnić się od oryginalnego:
  - będą w nim dodane lub usunięte pojedyncze litery np. faceebok.ru. albo cybefoks.pl, które na pierwszy rzut oka wyglądają normalnie.

https://cyberfolks.pl/blog/5-zasad-bezpiecznej-poczty-znasz-je-wszystkie/

Szukaj... CTRL + K

Plik Edycja Widok Przejdź Wiadomość Wydarzenia i zadania Narzędzia Pomoc

Niechciane - [redacted] [SPAM] Taw:Potrzebujemy.twojego

Od Poczta Polska <untl@richards.xsxweb.com>

Do Taw only! <[redacted]>

Odp. do Poczta Polska <Taw@gmail.com>

Temat **[SPAM] Taw:Potrzebujemy.twojego.potwierdzenia.do.wysłania.twojego.zamówienia.N.2473812**

Odpowiedz Przekaż

Poczta Polska

Masz (1) paczkę czekającą na dostawę.

Potwierdź swoje dane dostawy

POTWIERDŹ TERAZ

>5 zasad bezpiecznego korzystania z poczty e-mail_

1. Silne hasło
2. Szyfrowanie
3. Konfiguracja zabezpieczeń
4. Uwierzytelnianie dwuskładnikowe
5. Weryfikacja nadawcy

https://cyberprofilaktyka.pl/blog/cyberprzemoc--czym-jest-i-jak-rozmawiac-o-niej-z-dzieckiem_i27.html

CYBERPRZEMOC

- przemoc z użyciem urządzeń elektronicznych, najczęściej telefonu bądź komputera
- jej celem zawsze jest wyrządzenie krzywdy drugiej osobie
- podobnie jak przemoc tradycyjna – regularne, podejmowane z premedytacją działanie wobec słabszego, który nie może się bronić.

- określana jako cyberbullying, nękanie, dręczenie, prześladowanie w internecie

najczęstsze formy cyberprzemocy

- agresja słowna, np. wyzywanie na czatach internetowych, zamieszczanie komentarzy na forach internetowych w celu ośmieszenia, sprawienia przykrości lub wystraszenia innej osoby
- upublicznianie upokarzających, przerobionych zdjęć i filmów
- zamieszczanie przykrych komentarzy na profilach innych osób w portalach społecznościowych
- włamanie na konto i podszywanie się pod kogoś
- szantażowanie
- ujawnianie sekretów
- wykluczanie z grona „znajomych” w Internecie
- celowe ignorowanie czyjejś działalności w sieci

niebezpieczne zachowania

- **Flood** – wielokrotne wysyłanie tej samej bądź wielu różnych wiadomości do ofiary celem zapychania jej skrzynki odbiorczej.
- **Maskarada** – tworzenie nieprawdziwych kont na portalach internetowych w celu krzywdzenia ofiary.
- **Flaming** – wymiana pełnych agresji wiadomości za pośrednictwem komunikatora.
- **Trolling** – zamieszczanie dużej liczby nieprzyjemnych komentarzy na temat ofiary; może przejawiać się też w zmienianiu zdjęć i informacji umieszczanych na profilach ofiary czy też umieszczanie w jej imieniu obraźliwych statusów.
- **Cyberstalking** – nękanie ofiary w sposób ciągły i regularny przez wysyłanie jej ubliżających wiadomości SMS, e-maili lub za pomocą innych komunikatorów; można tu zaliczyć też wysyłanie gróźb czy też rozsyłanie wiadomości otrzymanych od ofiary, aby ją poniżyć.
- **Patostream** – internetowa transmisja prowadzona na żywo, w serwisach internetowych typu YouTube, której celem jest prezentowanie zachowań dewiacyjnych.
- **Sexting** – wysyłanie oraz wymienianie się zdjęciami, filmami i innymi treściami o charakterze seksualnym w celu poniżenia ofiary.
- **Sextortion** – wyłudzanie od innej osoby materiałów o treści seksualnej z jej udziałem, a następnie grożeniu, że treści te zostaną udostępnione, jeśli ofiara nie wpłaci określonej sumy pieniędzy bądź nie przyśle kolejnych materiałów.
- **Sharenting** – bezmyślne udostępnianie przez rodziców zdjęć swoich dzieci na portalach społecznościowych; może być źródłem takich sytuacji jak używanie fotografii przez dewiantów czy choćby wywoływanie w dziecku poczucia zażenowania.
- **Szkodliwe i niebezpieczne challenge** – wyzwania, których podjęcie uczestnicy dokumentują poprzez portale społecznościowe lub komunikatory.

Cyberprzemoc:
Młodzi respondenci obrażani są ze względu na:

- Sytuację materialną: 3,3%
- Wygląd fizyczny: 13,7%
- Religię, wyznanie: 4,3%
- Upodobania, zainteresowania, hobby: 9,7%
- Kolor skóry: 2,3%
- Ubiór (styl, typ ubrań): 8,5%
- Narodowość: 2,8%
- Preferencje seksualne: 4,9%
- Poglądy polityczne: 7,1%
- Inne, jakie?: 3,4%
- Płeć: 4,5%

@kademia NASK

co robić, by minimalizować cyberprzemoc

- **Dodawaj do znajomych lub obserwujących tylko konta, o których wiesz, że są utworzone przez znane ci osoby –** dodawanie profili społecznościowych nieznanych właścicieli, daje takim kontom dostęp do informacji o osobie, a te mogą być wykorzystane do anonimowego dręczenia; trudno wtedy o namierzenie sprawcy nękania, odpowiedzialność za nękanie może się rozmyć.
- **Nie podawaj nikomu swoich haseł –** niektórzy podają swoje hasła przyjaciołom i traktują to jako oznakę zaufania; daje to możliwość podszywania się pod kogoś w sieci.
- **Sprawdź swoje ustawienia prywatności** – warto korzystać z narzędzi pozwalających na ograniczanie widoczności wpisów na mediach społecznościowych; ustawiajmy je tak, aby nasze wpisy, zdjęcia czy filmiki mogły oglądać tylko osoby dodane do grona znajomych; konta można zablokować także tak, aby nie było możliwości udostępniania postów dalej.
- **Pomyśl, zanim cokolwiek opublikujesz –** jeśli publikuje się prywatne przemyślenia, zdjęcia oraz nagrania, można tym samym zachęcać internetowych trolli do dodawania negatywnych komentarzy; nic w sieci nie ginie, może zostać zachowane jako zrzut ekranu, może zostać pobrane na dysk komputera i powielane bez wiedzy autora.
- **Powiedz rodzicowi, nauczycielowi lub innemu zaufanemu dorosłemu, gdy czujesz się zaniepokojony daną sytuacją w Internecie –** osoba pokrzywdzona powinna móc o nieprzyjemnych doświadczeniach w sieci mieć z kimś porozmawiać, kto może doradzić właściwe zachowanie i okazać wsparcie.

możliwe kategorie prawne

- art. 190 k.k. – groźba karalna; grożenie komuś popełnieniem przestępstwa (np. pozbawieniem życia) przez Internet;
- art. 190a k.k. – stalking: uporczywe nękanie, podszywanie się pod inną osobę oraz wykorzystywanie jej wizerunku;
- art. 191 k.k. – zmuszenie do określonego działania wbrew jego woli;
- art. 191a k.k. – naruszenie intymności seksualnej, utrwalenie i rozpowszechnienie wizerunku nagiej osoby bez jej zgody;
- art. 212 i art. 216 k.k. – zniesławienie i zniewaga; wszelkie zachowania uwłaczające czyjejś godności, stanowiące przejaw lekceważenia oraz pogardy; pomówienie (oszczerstwo) o takie postępowanie lub właściwości, które mogą daną osobę poniżyć w opinii publicznej; użycie wizerunku osoby w celu jej ośmieszania, upokorzenia, wypowiadanie pod adresem pokrzywdzonego znieważających go wulgaryzmów lub epitetów;
- art. 267 k.k. – bezprawne uzyskanie informacji, np. włamanie się na pocztę email lub profil społecznościowy, które są zabezpieczone hasłem;
- art. 268 k.k. – niszczenie, usuwanie lub zmienianie informacji albo utrudnianie zapoznania się z informacją.
- art. 23 k.c. i art. 24 k.c. – naruszenie wizerunku, który jest dobrem osobistym człowieka. Zamieszczenie zdjęcia lub filmu przedstawiającego daną osobę na stronach internetowych lub w mediach społecznościowych, a także ich rozsyłanie za pomocą urządzeń z dostępem do Internetu, bez zgody tej osoby.

800 100 100 – TELEFON DLA RODZICÓW I NAUCZYCIELI

Bezpłatna i anonimowa pomoc telefoniczna i online dla rodziców/opiekunów i nauczycieli, którzy potrzebują wsparcia i informacji w zakresie przeciwdziałania przemocy, a także pomocy psychologicznej dzieciom przeżywającym kłopoty i trudności, takie jak: agresja i przemoc w szkole, cybeprzemoc i zagrożenia związane z nowymi technologiami, wykorzystanie seksualne, kontakt z substancjami psychoaktywnymi, depresja i obniżony nastrój, myśli samobójcze, zaburzenia odżywiania. Linia czynna jest od poniedziałku do piątku w godzinach 12.00–15.00. Więcej informacji na stronie https://800100100.pl/

116 111 – TELEFON ZAUFANIA DLA DZIECI I MŁODZIEŻY

Bezpłatny i anonimowy telefon dla dzieci i młodzieży prowadzony przez Fundację Dajemy Dzieciom Siłę. Telefon działa codziennie – 7 dni w tygodniu, 24 godziny na dobę. Dzieci i młodzież mogą także zarejestrować się na stronie internetowej i napisać wiadomość do konsultantów pełniących dyżur online. Więcej informacji na stronie https://116111.pl/

800 12 12 12 – DZIECIĘCY TELEFON ZAUFANIA RZECZNIKA PRAW DZIECKA

Bezpłatna działająca całodobowo telefoniczna linia interwencyjna dla dzieci i młodzieży. Osoby dorosłe mogą zgłaszać problemy dzieci lub rażące zaniedbania względem nich. Telefon działa codziennie – 7 dni w tygodniu, 24 godziny na dobę. Więcej informacji na stronie https://brpd.gov. pl/telefon-zaufania

DYŻURNET.PL

Zespół ekspertów NASK, działający jako punkt kontaktowy do zgłaszania nielegalnych treści w internecie, szczególnie związanych z seksualnym wykorzystywaniem dzieci. Zgłoszenia o potencjalnie nielegalnych treściach można przekazywać za pomocą formularza, na adres e-mailowy lub za pomocą infolinii 0 801 615 005. Szczegółowe informacje można znaleźć na stronie https://dyzurnet.pl/

Jak i gdzie

zgłosić przestępstwo popełnione w internecie

Wystarczy podejrzenie!

Zgłaszając sprawę na Policję lub do Prokuratury nie trzeba mieć stuprocentowej pewności, że doszło do popełnienia przestępstwa. Wystarczy podejrzenie lub poczucie zagrożenia. Warto mieć na uwadze, że każde zgłoszenie może skutkować zatrzymaniem i ukaraniem sprawcy.

Kto może zgłosić sprawę?

Każda osoba, bez względu na wiek, uprawniona jest do dokonania zgłoszenia o podejrzeniu popełnienia przestępstwa!

W trosce o bezpieczeństwo psychiczne dziecka należy zredukować do minimum liczbę jego przesłuchań oraz czynników stresowych. Gdy problem dotyczy osoby małoletniej (np. oszustwo na jej szkodę, kradzież konta na portalu społecznościowym) zgłoszenia można dokonać, bez udziału dziecka, w najbliższej jednostce Policji lub Prokuratury.

WAŻNE!

W przypadku zgłoszenia przestępstwa na szkodę małoletniego dotyczącego użycia przemocy lub groźby, a także naruszenia wolności seksualnej oraz obyczajności, przesłuchanie przeprowadza Sąd na posiedzeniu z udziałem biegłego psychologa w tzw. przyjaznym pokoju przesłuchań.

Jak dokonać zgłoszenia?

1 Ustnie:

W każdej jednostce Policji i Prokuratury w Polsce. Funkcjonariusz ma obowiązek przyjąć takie zgłoszenie. Zgodnie z polskim prawem zgłoszenie musi zakończyć się spisaniem protokołu, który powinien zostać podpisany przez zgłaszającego. Jest to istotne, ponieważ jedynie protokół z przesłuchania podpisany przez osobę składającą zeznania stanowi podstawę prawną do wszczęcia postępowania.

UWAGA!

Przed dokonaniem zgłoszenia warto:

- zanotować wszystkie ważne informacje dotyczące zdarzenia (na przykład: co, kiedy i gdzie się wydarzyło, kto uczestniczył w zdarzeniu w roli sprawcy i ofiary, jak doszło do popełnienia potencjalnego przestępstwa),
- zabrać ze sobą dowody przestępstwa (na przykład: print screeny rozmów, nazwy i adresy profili, dane kontaktowe do przelewu, itp.),
- zabrać ze sobą dokument potwierdzający tożsamość.

dyżurnet.pl NASK NASK saferinternet.pl

2 Pisemnie:

W każdej jednostce Policji i Prokuratury w Polsce. Zgłoszenie można także wysłać mailem, pocztą lub faksem. Pismo powinno zawierać:

- dane Zgłaszającego (imię, nazwisko, adres do korespondencji, adres e-mail, nr telefonu),
- dane adresata (jednostki Policji), możliwie wyczerpujący opis sprawy, z uwzględnieniem posiadanych informacji o sprawcy oraz dat i godzin zdarzeń,
- własnoręczny podpis.

Do pisma należy dołączyć kopię posiadanego materiału dowodowego (np. print screeny rozmów, nazwy i adresy profili, dane kontaktowe do przelewu, itp.)
W przypadku pisemnego zgłoszenia, funkcjonariusz prowadzący postępowanie może wezwać zgłaszającego do złożenia zeznań.

3 Anonimowo:

Forma zgłoszenia pisemnego (bez podawania swoich danych osobowych). Zainicjuje ona czynności Policji, jednak w takim przypadku nie będą udzielane informacje o dalszym toku postępowania.

Przydatne linki

dyzurnet.pl
Zespół Reagujący na Nielegalne Treści w Internecie

cbzc.policja.gov.pl
Centralne Biuro Zwalczania Cyberprzestępczości

incydent.cert.pl
Zespół Reagowania na Incydenty Bezpieczeństwa w Sieci

takeitdown.ncmec.org
Pomoc w usunięciu materiałów intymnych z internetu dla osób małoletnich

stopncii.org
Pomoc w usunięciu materiałów intymnych z internetu dla osób dorosłych

reportcontent.google.com/forms/eu_removal
Usunięcie danych osobowych zgodnie z przepisami UE

dyżurnet.pl NASK NASK saferinternet.pl

art. 14 ustawy z 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną

1. Nie ponosi odpowiedzialności za przechowywane dane ten, kto udostępniając zasoby systemu teleinformatycznego w celu przechowywania danych przez usługobiorcę, nie wie o bezprawnym charakterze danych lub związanej z nimi działalności, a w razie otrzymania urzędowego zawiadomienia lub uzyskania wiarygodnej wiadomości o bezprawnym charakterze danych lub związanej z nimi działalności niezwłocznie uniemożliwi dostęp do tych danych.
2. Usługodawca, który otrzymał urzędowe zawiadomienie o bezprawnym charakterze przechowywanych danych dostarczonych przez usługobiorcę i uniemożliwił dostęp do tych danych, nie ponosi odpowiedzialności względem tego usługobiorcy za szkodę powstałą w wyniku uniemożliwienia dostępu do tych danych.
3. Usługodawca, który uzyskał wiarygodną wiadomość o bezprawnym charakterze przechowywanych danych dostarczonych przez usługobiorcę i uniemożliwił dostęp do tych danych, nie odpowiada względem tego usługobiorcy za szkodę powstałą w wyniku uniemożliwienia dostępu do tych danych, jeżeli niezwłocznie zawiadomił usługobiorcę o zamiarze uniemożliwienia do nich dostępu.
4. Przepisów ust. 1 - 3 nie stosuje się, jeżeli usługodawca przejął kontrolę nad usługobiorcą w rozumieniu przepisów o ochronie konkurencji i konsumentów

WZÓR ZAWIADOMIENIA WYDAWCY SERWISU INTERNETOWEGO O WPISIE NARUSZAJĄCYM DOBRA OSOBISTE

miejscowość, data

imię i nazwisko
adres osoby zawiadamiającej

nazwa i adres
wydawcy serwisu internetowego

Niniejszym zawiadamiam, że na portalu internetowym XYZ – www.xyz.pl, na łamach forum, pod artykułem pt: „abc", zostały zamieszczone wpisy, naruszające moje dobra osobiste.

Wpisy te zostały zamieszczone przez użytkownika posługującego się identyfikatorem „xx" *(w tym miejscu możemy podać link do komentarzy, które nas obrażają).*

Emocjonalna treść w/w komentarza narusza wprost moje dobre imię, wypełniając jednocześnie znamiona przestępstwa zniesławienia (art. 212 kk)/zniewagi (art. 216 kk) poprzez pomówienie mnie o postępowanie oraz właściwości, które mogą poniżyć mnie w opinii publicznej a także narazić na utratę zaufania potrzebnego dla właściwego wykonywania mojego zawodu.

W tym miejscu cytujemy obrażające nas słowa.

W tym stanie rzeczy, żądam natychmiastowego usunięcia w/w wpisu z forum.

Zawiadomienie niniejsze należy traktować jako wiadomość przekazaną w trybie art. 14 ust. 1 ustawy z 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204).

podpis

http://www.oil.org.pl/xml/oil/oil67/gazeta/numery/n2011/n201105/n20110510