26.10.2020 – 09.11.2020

Dzień dobry młodzieży!

W związku z dużą ilością zakażeń COVID – 19 powracamy na zdalne nauczanie. Wykorzystajcie ten czas najlepiej jak potraficie. Pamiętajcie, aby właściwie połączyć naukę z czasem wolnym 😊 Mam nadzieję, że wrócimy jak najszybciej do szkoły i będziemy mieli normalne lekcje. Życzę Wam i Waszym rodzinom dużo zdrowia. Dbajcie o siebie i innych.

Moi drodzy, przed Wami tematyka na najbliższe dwa tygodnie. Przeczytajcie proszę poniższy tekst, obejrzycie filmiki z linków, rozwiążcie zadania które znajdują się na końcu. Temat omówimy sobie przy najbliższym spotkaniu na TEAMS.

Temat: Terroryzm i Cyberterroryzm

1. Czym jest terroryzm ?

Terroryzm definiuje się jako "działania pojedynczych osób lub grup usiłujących za pomocą aktów terrorystycznych wymusić na rządach państw określone ustępstwa"

Próbę zdefiniowania zjawiska terroryzmu podejmowały również organizacje międzynarodowe. Według Komisji Europejskiej terroryzm oznacza "wszelkie celowe akty popełnione przez pojedyncze osoby lub organizacje przeciw jednemu lub kilku państwom, ich instytucjom lub ludności, w celu zastraszania oraz poważnego osłabienia lub zniszczenia struktury politycznej, gospodarczej i społecznej kraju". Natomiast zgodnie z definicją zaproponowaną przez Zgromadzenie Parlamentarne Rady Europy, terroryzm to "każdy czyn popełniony przez osobę lub grupę osób z udziałem przemocy lub groźby jej użycia przeciwko państwu, jego instytucjom, ludności w ogólności lub konkretnym jednostkom, motywowanym przez separatystyczne aspiracje, ekstremistyczne koncepcje ideologiczne, fanatyzm lub irracjonalne i subiektywne czynniki, zorientowany na stworzenie klimatu terroru wśród osób publicznych, określonych jednostek lub grup w społeczeństwie bądź w całym społeczeństwie."

Zamach z 11 września 2001 r. stał się punktem zwrotnym w walce z terroryzmem wielu państw świata

Powyższe definicje świadczą o braku jednego uniwersalnego wyjaśnienia zjawiska terroryzmu. Mimo to na potrzeby niniejszej lekcji warto przyjąć ogólną definicję terroryzmu przedstawioną w Słowniku terminów z zakresu bezpieczeństwa narodowego Akademii Obrony Narodowej w Warszawie. Zgodnie z jej treścią terroryzm to "teoria i praktyka określająca różnie umotywowane ideologicznie, planowane i zorganizowane działania pojedynczych osób lub grup, skutkujące naruszeniem istniejącego porządku prawnego, podjęte w celu wymuszenia od władz, państw społeczeństw określonych zachowań i świadczeń, często naruszające dobra osób postronnych."

2. Rodzaje terroryzmu – terroryzm polityczny i terroryzm kryminalny

W literaturze wyróżnia się – w zależności od przyjętych kryteriów – wiele rodzajów terroryzmu. Często stosowanym rozróżnieniem jest podział na terroryzm polityczny i terroryzm kryminalny. Jak sama nazwa wskazuje, pierwszy z nich motywowany jest celami politycznymi, do których można zaliczyć:

- zmianę elity rządzącej,
- zmianę systemu politycznego (jego podstaw czy też struktury),
- wymuszenie implementacji pewnych rozwiązań prawnych,
- poszerzenie praw lub autonomii danej grupy społecznej,
- oderwanie części terytorium danego państwa i założenie nowego państwa lub przyłączenie do już istniejącego.

Przykładem działań terrorystycznych o podłożu politycznym były akcje organizowane przez Irlandzką Armię Republikańską

Cechą charakterystyczną terroryzmu kryminalnego jest to, że stanowi on działanie z **pobudek materialnych**, a nie ideowych. Działania tego rodzaju sprowadzają się zazwyczaj do porwań dla okupu, niszczenia mienia, sabotażu czy też szantażu. Warto w tym miejscu podkreślić, że grupy uprawiające terroryzm polityczny bardzo często stosują również terroryzm kryminalny, z którego czerpią dochody przeznaczane na finansowanie działalności politycznej.

Porwania, szczególnie dzieci, są jednym z najczęstszych przejawów terroryzmu kryminalnego

Można stwierdzić, że większość działań z zakresu terroryzmu politycznego należy do kategorii **terroryzmu zbiorowego** (celem ataków są w nim zbiorowości ludzkie), natomiast terroryzm kryminalny jest najczęściej wymierzony w pojedyncze osoby (**terroryzm indywidualny**). Dzieje się tak dlatego, że takie działanie jest łatwiejsze do zorganizowania oraz efektywniejsze, jeśli chodzi o zdobycie określonych dochodów (porywając jedną osobę, w stosunkowo nietrudny sposób można zdobyć pokaźny okup).

3. Wybrane organizacje terrorystyczne na świecie

Terroryzm był obecny na świecie już od najdawniejszych czasów. Skrytobójstwem, jako formą terroryzmu indywidualnego – zamachami na pojedyncze osoby zajmujące wysokie pozycje w społeczeństwie, posługiwały się już w I w. w Izraelu antyrzymskie stronnictwa zelotów i sykariuszy. Za skrytobójstwo należy uznać również udany zamach na Juliusza Cezara, przeprowadzony przez spiskowców 15 marca 44 r. p.n.e. W XIX w. metody terrorystyczne były stosowane bardzo często przez stronnictwa niepodległościowe we Włoszech, Irlandii, a także – w czasie powstania styczniowego – w Polsce. Spośród grup terrorystycznych najaktywniejszych w okresie międzywojennym (lata 1918-1939), należy wymienić anarchistyczną hiszpańską organizację Los Solidarios, Crvenę Pravdę z Jugosławii, czy też Żelazną Gwardię z Rumunii. W okresie zimnej wojny krwawe zamachy przeprowadzały również Czerwone Brygady we Włoszech, Frakcję Czerwonej Armii (RAF) w Niemczech oraz Irlandzka Armia Republikańska (IRA) w Wielkiej Brytanii.

Dzisiejszy świat także nie jest wolny od takich zorganizowanych grup, które nie tylko jawnie przyznają się do swojej działalności, ale również przeprowadzają coraz krwawsze akcje, odbierając życie ogromnej liczbie niewinnych ludzi.

4. Zapobieganie terroryzmowi i metody jego zwalczania

Współcześnie wypracowano 4 sposoby walki z różnego rodzaju organizacjami terrorystycznymi. Warto jednak podkreślić, że żaden z nich nie jest uniwersalny – każdy ma swoje zalety oraz wady. Z tego względu wykorzystanie odpowiedniego rozwiązania powinno być poprzedzone wnikliwą analizą konkretnego przypadku.

Jedną z metod jest **bezpośrednia walka** zarówno z pojedynczymi terrorystami, jak i organizacjami, która może przybrać formę działań ochronnych lub ofensywnych. Pierwsze mogą być realizowane poprzez wzmacnianie ochrony zagrożonych obiektów (np. budynków rządowych i lotnisk) oraz osób (np. prominentnych polityków i wpływowych biznesmenów). Drugie natomiast mogą obejmować operacje policji lub sił zbrojnych prowadzące do aresztowania osób podejrzanych o planowanie i realizację działań terrorystycznych, rozbicia struktur organizacji terrorystycznych czy też udaremnienia zamachów. Przedsięwzięcia związane z walką bezpośrednią są działaniami wszechstronnymi. Angażują one siły policyjne, wojskowe, służby specjalne, ratownicze i pozostałe struktury państwowe, w związku z czym wymagają specjalistycznej koordynacji i dokładnego planowania.

Inne rozwiązanie polega na **likwidacji przyczyn zagrożenia**. Jest to niezwykle trudne, gdyż współczesny terroryzm to zjawisko bardzo skomplikowane. Niełatwo określić pobudki terrorystów – bardzo rzadko mają one **charakter obiektywny** (tzn. rzadko są wyraźnie obserwowalne i dotyczą np. niedemokratycznego reżimu politycznego, kryzysu gospodarczego czy też zewnętrznej agresji). U podłoża współczesnego terroryzmu często leżą radykalne poglądy terrorystów, wyznawane przez nich teorie, a niekiedy również ich zaburzenia psychiczne.

Kolejna metoda walki z terroryzmem koncentruje się na **utrudnianiu terrorystom zdolności do działania**. Polega na ograniczaniu i likwidacji źródeł ich finansowania, dostaw broni i materiałów wybuchowych (ilustracja 7), powstrzymywaniu propagandy oraz procesów rekrutacji nowych członków. Wydaje się, że sposób ten jest dzisiaj najczęściej wykorzystywany w odniesieniu do terroryzmu międzynarodowego.

Każda przechwycona partia nielegalnej broni obniża morale przeciwnika

Następny sposób to **oddziaływanie na intencje terrorystów**. Polega na przekonywaniu ich, aby nie podejmowali ataków, choć są w stanie je wykonać. Może przybrać formę ustępstw lub zdecydowanej polityki antyterrorystycznej. W obu przypadkach metoda ta może przynieść skutek odwrotny do zamierzonego – ustępstwa mogą być uznane za oznakę słabości i zachęcić zamachowców do realizacji ich planów (gdyż uznają oni, że osiągnięcie celów jest w takiej sytuacji bardziej prawdopodobne), a zdecydowana polityka antyterrorystyczna może zostać uznana jako przejaw wrogości i zmobilizować terrorystów do bardziej okrutnego działania.

!!! Podczas spotkania TEAMS rozwiążemy sobie kilka zadań o tematyce terroryzmu !!!

CYBERTERRORYZM

Zjawiska takie, jak globalizacja, rozwój technologiczny i powszechne wykorzystanie Internetu doprowadziły do powstania cyberprzestrzeni – cyfrowej przestrzeni przetwarzania i wymiany informacji. Tworzą ją wszystkie systemy i sieci teleinformatyczne, zachodzące pomiędzy nimi powiązania oraz relacje między nimi a ich użytkownikami oraz między samymi użytkownikami.

Cyberprzestrzeń jest dzisiaj wykorzystywana przez różnych użytkowników – począwszy od instytucji państwowych, przez firmy prywatne, a skończywszy na domowych użytkownikach Internetu. Z tego względu ochrona cyberprzestrzeni stała się jednym z podstawowych celów strategicznych w obszarze bezpieczeństwa każdego państwa. Swobodny przepływ osób, towarów, informacji i kapitału w dużym stopniu uzależnia bezpieczeństwo państwa od stworzenia skutecznych mechanizmów zapobiegania zagrożeniom przestrzeni cyfrowej i zwalczania ich skutków.

Jednym z największych niebezpieczeństw jest **cyberterroryzm**, który stanowi jedną z form cyberprzestępstwa. Polega on na wykorzystywaniu zdobyczy technologii informacyjnej w celu wyrządzenia szkody (np. zniszczenia lub modyfikacji zasobów informacyjnych, spowodowania utraty życia bądź zdrowia czy też doprowadzenia do utraty mienia przez ofiary ataku).

Podłożem cyberterroryzmu mogą być zarówno cele polityczne (ideowe), jak i pobudki materialne (chęć osiągnięcia zysku). Z tego względu celem ataków cyberterrorystycznych mogą być instytucje państwowe, jednostki prowadzące działalność gospodarczą, instytuty badawcze, osoby prywatne i inne. Jednak najczęściej celami są państwowe systemy teleinformatyczne, zapewniające prawidłowe funkcjonowanie:

- administracji państwowej,
- sił zbrojnych i innych instytucji zajmujących się obroną narodową,
- instytucji odpowiedzialnych za bezpieczeństwo wewnętrzne i zewnętrzne państwa,
- łączności i sieci telekomunikacyjnych,
- sieci zaopatrzenia w energię, wodę i gaz,
- sieci i instytucji finansowych,
- służb ratowniczych.

Cyberterroryzm to celowe działania na szkodę sieci teleinformatycznych. Ogólnie mogą one przyjmować formy:

- zabiegów zmierzających do zakłócania działania systemów,
- nieupoważnionego wprowadzania, kopiowania, modyfikowania lub usuwania danych,
- łamania zabezpieczeń w celu przejęcia kontroli nad poszczególnymi elementami sieci.

Zazwyczaj cyberterroryści wykorzystują Internet w podobny sposób, jak zorganizowane grupy przestępcze lub indywidualni przestępcy. Ich najczęstsze działania to:

- włamania do obcych komputerów (***hacking***) oraz do systemów informatycznych (***cracking***) w celu osiągnięcia materialnej korzyści,
- wykorzystywanie programów umożliwiających wejście do serwera z pominięciem zabezpieczeń (***back door***),
- podsłuchiwanie informacji przekazywanych między komputerami i przechwytywanie haseł oraz loginów (***sniffing***),
- podszywanie się pod inny komputer (***IP spoofing***),
- wysyłanie wirusów i robaków komputerowych,
- wyłudzanie poufnych informacji (***phishing***).

Najczęściej stosowane metody ataków na sieci internetowe instytucji państwowych prezentuje poniższa grafika interaktywna.

Warto również podkreślić, że współcześnie terroryści wykorzystują Internet nie tylko jako przestrzeń, w której mogą przeprowadzać ataki. Staje się on również narzędziem propagandy, rozpowszechniania idei oraz rekrutowania nowych członków do swojej organizacji.

Uwzględniając charakterystykę metod wykorzystywanych przez te grupy, można wyróżnić następujące przykłady **konsekwencji ataków cyberterrorystycznych**:

- kradzież i przechwytywanie cennych informacji,
- ujawnienie tajnych oraz prywatnych informacji (w tym danych osobowych),
- zniszczenie (usunięcie) danych o kluczowym znaczeniu,
- straty materialne,
- paraliż przedsiębiorstw prywatnych i instytucji państwowych,
- paraliż komunikacyjny,
- blokowanie stron internetowych,
- wzrost popularności grup terrorystycznych,
- wzrost liczebności członków grup terrorystycznych.

Praca domowa !!!

***macie 2 tygodnie na jej wykonanie. Rozwiązane zadanie proszę wysłać w wersji elektronicznej (może być .doc, .pdf .jpg)**

na mój mail: maciej.gapys@soswdnr.pl

do dnia 09.11.2020

↓

Ćwiczenie 1

Połącz w pary pojęcia z odpowiednimi wyjaśnieniami.

cyberprzestępstwo	Czyn zabroniony popełniony w przestrzeni cyfrowej.
teleinformatyczna infrastruktura krytyczna	Cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne.
cyberterroryzm	Działalność zabroniona o charakterze terrorystycznym popełniona w obszarze cyberprzestrzeni.
cyberprzestrzeń	Teleinformatyczne systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty kluczowe ze względu na bezpieczeństwo państwa i jego obywateli.

Ćwiczenie 2

Połącz nazwy metod stosowanych przez cyberterrorystów z ich wyjaśnieniami.

IP spoofing	Wyłudzanie poufnych informacji.
hacking	Podsłuchiwanie informacji przekazywanych między komputerami i przechwytywanie haseł i loginów.
sniffing	Włamania do obcych systemów informatycznych.
phishing	Wykorzystywanie programów umożliwiających wejście do serwera z pominięciem zabezpieczeń.
cracking	Podszywanie się pod inny komputer.
back door	Włamania do obcych komputerów.

Notatka do druku i wklejenia do zeszytu

Temat: Terroryzm i cyberterroryzm

Terroryzm

- Nie istnieje jedna uniwersalna definicja terroryzmu. Zarówno naukowcy, jak i organizacje międzynarodowe przedstawiają różnorodne koncepcje wyjaśniające to zjawisko.
- Ogólnie przyjąć można, że terroryzm to teoria i praktyka obejmująca różnie umotywowane ideologicznie, planowane i zorganizowane działania pojedynczych osób lub grup. Skutkują one naruszeniem istniejącego porządku prawnego i są podejmowane w celu wymuszenia na władzach, państw i społeczeństw określonych zachowań i świadczeń, często godzących w dobro osób postronnych.
- Wyróżnia się terroryzm polityczny i kryminalny. Jak sama nazwa wskazuje, pierwszy motywowany jest celami politycznymi, zaś drugi pobudkami materialnymi.
- Współcześnie wypracowano kilka sposobów walki z terroryzmem, jednak żaden z nich nie jest uniwersalny i każdy ma swoje zalety oraz wady. Z tego względu wykorzystanie danego sposobu powinno być poprzedzone wnikliwą analizą przypadku, w którym dany sposób ma być zastosowany.
- Zagrożenie terrorystyczne jest niezwykle niebezpieczne. Dlatego też w celu jego uniknięcia oraz minimalizacji rezultatów działań terrorystycznych istotne jest odpowiednie postępowanie zarówno przed wystąpieniem zagrożenia, jak i w jego trakcie.

Cyberterroryzm

- We współczesnym świecie jednym z największych zagrożeń bezpieczeństwa jest cyberterroryzm.
- Cyberterroryzm stanowi jedną z form przestępstwa i przejawia się jako wykorzystywanie zdobyczy technologii informacyjnej w celu wyrządzenia szkody.
- Podłożem cyberterroryzmu mogą być zarówno cele polityczne (ideowe), jak i pobudki materialne (chęć osiągnięcia zysku). Z tego względu celem ataków cyberterrorystycznych mogą być nie tylko instytucje państwowe, ale również jednostki prowadzące działalność gospodarczą, instytuty badawcze czy też osoby prywatne.
- Cyberterroryści coraz częściej wykorzystują Internet jako narzędzie propagandy i rekrutacji.
- Do najczęstszych działań cyberterrorystów zaliczyć należy m.in.: włamania do obcych komputerów oraz systemów informatycznych, wkradanie się na serwery z pominięciem zabezpieczeń, podsłuchiwanie przekazywanych informacji, wysyłanie szkodliwego oprogramowania czy też podszywanie się pod inny komputer.
- Cyberterroryzm i cyberprzestępstwa, choć na ogół kojarzone z zagrożeniem funkcjonowania państwa, mogą mieć również negatywne konsekwencje dla osób prywatnych. W wyniku ataków cybernetycznych mogą m.in. zostać ujawnione dane osobiste i inne poufne informacje.
- W związku z narastającymi na świecie zagrożeniami w obszarze szeroko pojętej teleinformatyki rząd Rzeczypospolitej Polskiej przyjął Rządowy program ochrony cyberprzestrzeni RP na lata 2011-2016. Dokument ten definiuje cele rządu w zakresie bezpieczeństwa teleinformatycznego oraz inicjuje podstawowe działania gwarantujące bezpieczeństwo.