Charakterystyka przestępczości

dr hab. inż. Andrzej Gałecki, prof. WSB

MODUŁ BEZPIECZEŃSTWA
Rozdział 7. Charakterystyka przestępczości

Zagadnienia do omówienia

1. **Pojęcie przestępczości.**
2. **Podział przestępstw ze względu na podmiot.**
3. **Przestępstwa o charakterze kryminalnym.**
4. **Przestępstwa o charakterze zorganizowanym.**
5. **Przestępstwa o charakterze gospodarczym.**
6. **Istota terroryzmu.**
7. **Klasyfikacja terroryzmu.**

Definicja przestępczości

„… jest to zawinione zachowanie się człowieka, zabronione przez ustawę pod groźbą kary jako społecznie niebezpieczne[1].”

Encyklopedia PWN[1]

„Przestępczość – ogół przestępstw popełnianych w pewnym okresie w danym kraju lub danym środowisku społecznym[2].”

Rozporządzenie Prezesa Rady Ministrów[2]

„… czyn społecznie szkodliwy, bezprawny, zawiniony, zagrożony karą[3].”

Rozporządzenie Prezesa Rady Ministrów[4]

[1] Encyklopedia popularna PWN, Wydawnictwo Naukowe PWN Spółka z.o.o. Warszawa 1993, s. 695.
[2] S. Wronkowska, M. Zmierczak, (red.) „Elementarne wiadomości o prawie karnym”, Warszawa 2007, s. 224-225.
[3] Encyklopedia popularna PWN, Wydawnictwo Naukowe PWN Spółka z.o.o. Warszawa 1993, s. 695.

Postrzeganie zjawiska przestępczości

Zjawisko przestępczości można postrzegać w kategoriach:

Jakościowych	Ilościowych
Czynniki charakteryzujące sprawcę:	**rozmiary przestępczości (ilość przestępstw w czasie)**
Społeczno-demograficzne	**nasilenie przestępczości (wysokość nasycenia)**
Psychologiczne	**dynamika przestępczości (przestępstwa w czasie)**
Czasowe	**struktura przestępczości (ilość i rodzaj przestępstw)**
Przestrzenne	**trudność pomiaru zjawiska przestępczości**

Źródło: Kryminologiczne podstawy prawa karnego, w: A.Marek (red) System prawa karnego, t.1, Zagadnienia ogólne, pod red. A.Marka, Wydawnictwo C.H.Beck, Warszawa 2010, str.99 – 140.

Określenie zjawiska przestępczości

Zjawisko przestępczości można także wyrazić jako:

Wyrażoną w czynach, które rzeczywiście zostały popełnione, a informacje o nich dotarły do organów ścigania poprzez ich własne źródła lub zawiadomienie

Przestępczość ujawniona (zarejestrowana)

Tzw. ciemna liczba tj. przestępstwa faktycznie popełnione, jednak informacja o nich nie została odnotowana w rejestrze, ani w żaden inny sposób nie dotarła do organów ścigania

Przestępczość ukryta (nieujawniona)

Wyrażona w czynach przestępczych, które miały miejsce:
- **na określonym terenie**
- **w danym czasie**

Przestępczość rzeczywista

Źródło: Kryminologiczne podstawy prawa karnego, w: A.Marek (red) System prawa karnego, t.1, Zagadnienia ogólne, pod red. A.Marka, Wydawnictwo C.H.Beck, Warszawa 2010, str.99 – 140.

Podział znamion typu czynu zabronionego

Z punktu widzenia kwalifikacji prawnej czynu podstawowe znaczenie ma ustalenie zrealizowania przez sprawcę stanu objętego ustawowymi znamionami czynu zabronionego[1].

W każdym typie przestępstwa można wyróżnić następujące grupy znamion[1]:

Źródło: M. Czechowska, Typizacja przestępstw, Uniwersytet Wrocławski https://prawo.uni.wroc.pl (pobrano 23.08.2021)

Podmiot przestępstwa

Podmiot przestępstwa należy utożsamiać z podmiotem czynnym – tj. sprawcą przestępstwa, którym może być[1]:

CZŁOWIEK

który jest:

- **osiągnął odpowiedni wiek**
- **przejawia odpowiedni stopień rozwoju umysłowego**
- **przejawia odpowiedni stopień rozwoju moralnego**
- **przejawia odpowiedni stopień rozwoju społecznego**
- **poczytalny**

Źródło: M. Czechowska, Typizacja przestępstw, Uniwersytet Wrocławski https://prawo.uni.wroc.pl (pobrano 23.08.2021)

Podział przestępstw ze względu na podmiot

Przestępstwa ze względu na podmiot można podzielić na[1]:

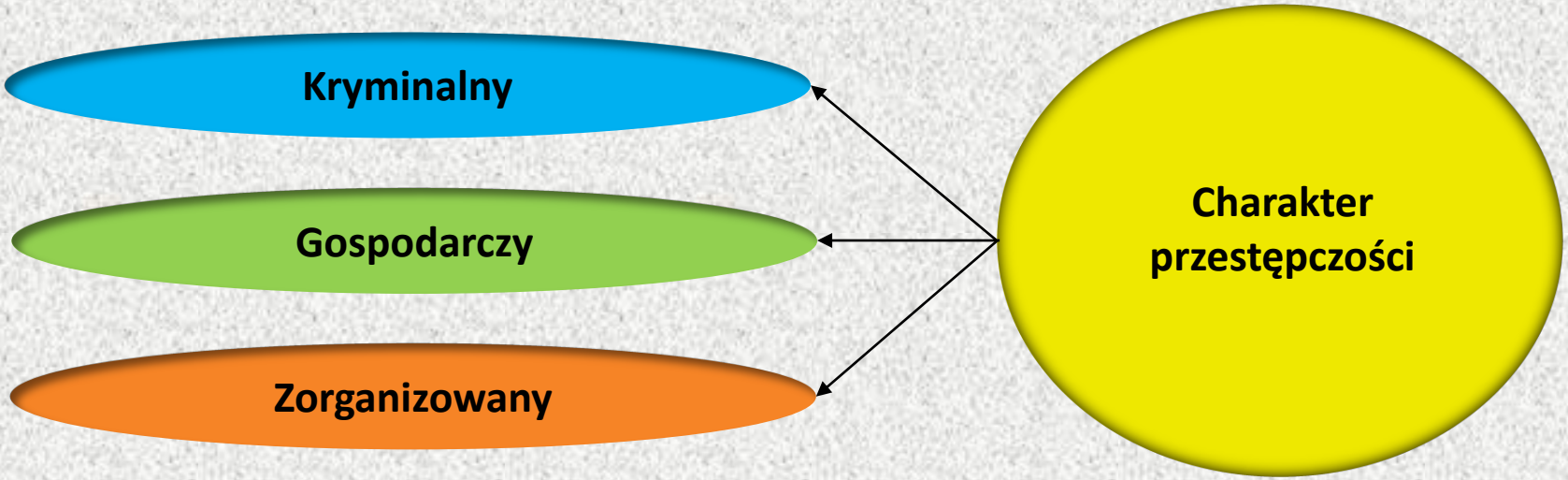
Przestępstwo powszechne → sprawcą może być każdy człowiek

Przestępstwo indywidualne → przestępstwo, w którym posiadanie przez sprawcę określonej cechy przewidzianej przez ustawę stanowi znamię typu czynu decydujące o karalności

- **Właściwe** → przestępstwo typu podstawowego, za które karalność jest uzależniona od posiadania przez sprawcę cechy przewidzianej przez ustawę
- **Niewłaściwe** → przestępstwo typu zmodyfikowanego (kwalifikowanego albo uprzywilejowanego)

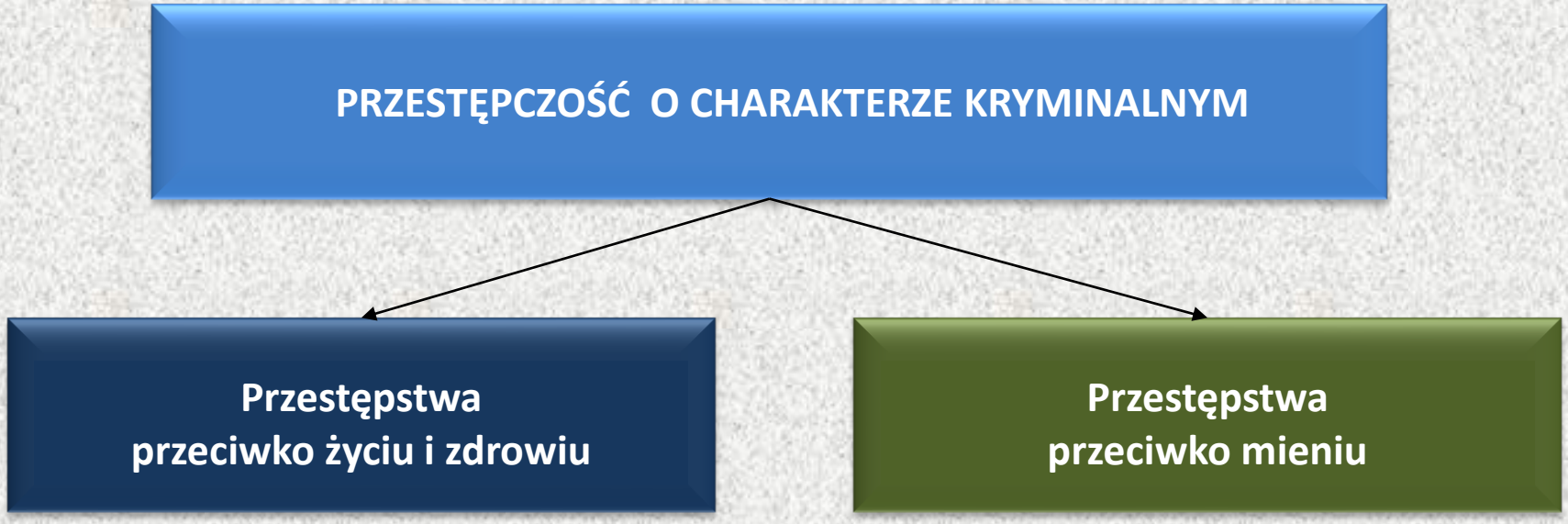
Źródło: M. Czechowska, Typizacja przestępstw, Uniwersytet Wrocławski https://prawo.uni.wroc.pl (pobrano 23.08.2021)

Charakter przestępczości



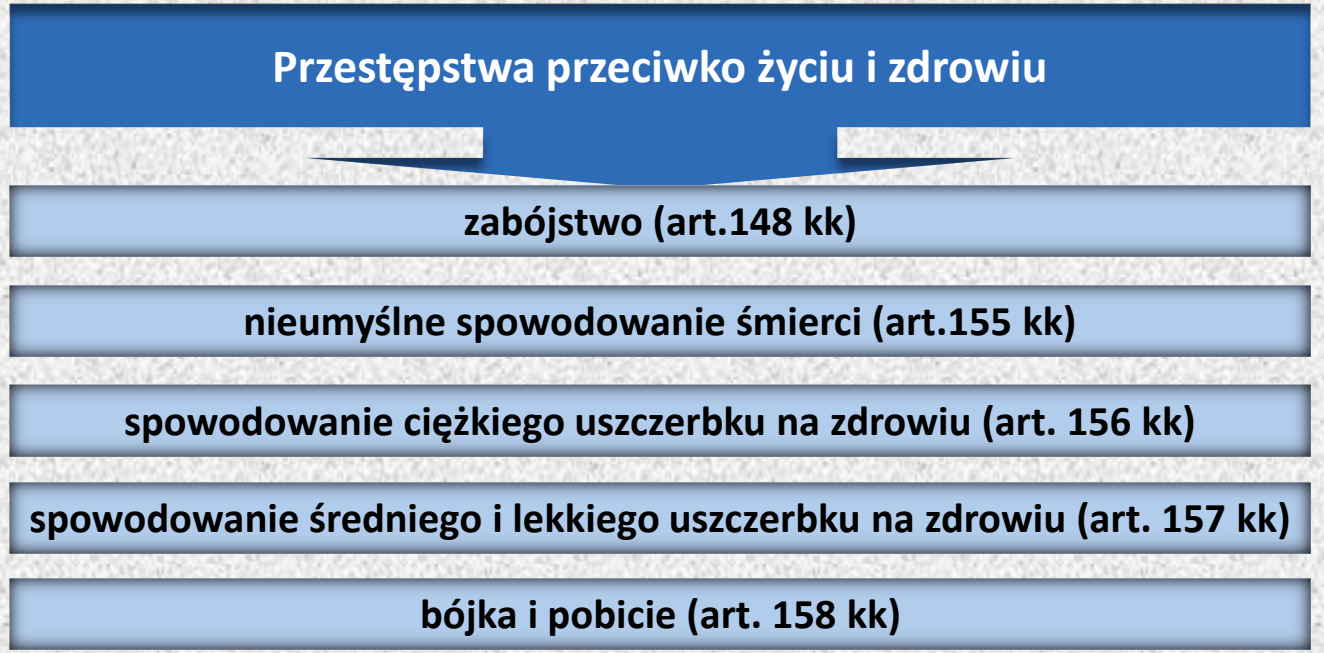
Źródło: Polityka kryminalna. Zapobieganie przestępczości. https://prawo.uni.wroc.pl › files › students-resources (pobrano 24.08.2021)

Przestępczość o charakterze kryminalnym



Źródło: Polityka kryminalna. Zapobieganie przestępczości. https://prawo.uni.wroc.pl › files › students-resources (pobrano 24.08.2021)

Przestępstwa przeciwko życiu i zdrowiu



Źródło: Polityka kryminalna. Zapobieganie przestępczości. https://prawo.uni.wroc.pl › files › students-resources (pobrano 24.08.2021)

Zabójstwo

Zabójstwo art. 148 kk

§ 1. Kto zabija człowieka

podlega karze pozbawienia wolności na czas nie krótszy od lat 8,
karze 25 lat pozbawienia wolności albo karze dożywotniego pozbawienia wolności

§ 2. Kto zabija człowieka

ze szczególnym okrucieństwem

w związku z wzięciem zakładnika, zgwałceniem albo rozbojem

w wyniku motywacji zasługującej na szczególne potępienie

z użyciem materiałów wybuchowych

podlega karze pozbawienia wolności na czas nie krótszy od lat 12, karze 25 lat pozbawienia wolności albo karze dożywotniego pozbawienia wolności

Źródło: Dz.U.2020.0.1444 t.j. - Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny Rozdział XIX.

Zabójstwo
Nieumyślne spowodowanie śmierci

Zabójstwo art. 148 kk

§ 3. Karze określonej w § 2 podlega
kto jednym czynem zabija więcej niż jedną osobę lub był wcześniej prawomocnie skazany za zabójstwo oraz sprawcą zabójstwa funkcjonariusza publicznego popełnionego podczas lub w związku z pełnieniem przez niego obowiązków służbowych związanych z ochroną bezpieczeństwa ludzi lub ochroną bezpieczeństwa lub porządku publicznego.

§ 4. Kto zabija człowieka pod wpływem silnego wzburzenia usprawiedliwionego okolicznościami
podlega karze pozbawienia wolności od roku do lat 10.

Niewymyślne spowodowanie śmierci art. 155 kk

Kto nieumyślnie powoduje śmierć człowieka,
podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Źródło: Dz.U.2020.0.1444 t.j. - Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny Rozdział XIX.

Spowodowanie ciężkiego uszczerbku na zdrowiu

Spowodowanie ciężkiego uszczerbku na zdrowiu art. 156 kk

§ 1. Kto powoduje ciężki uszczerbek na zdrowiu w postaci:

- **pozbawienia człowieka wzroku, słuchu, mowy**
- **pozbawienia człowieka zdolności płodzenia**
- **innego ciężkiego kalectwa**
- **ciężkiej choroby nieuleczalnej**
- **długotrwałej choroby realnie zagrażającej życiu**
- **trwałej choroby psychicznej**
- **całkowitej albo znacznej trwałej niezdolności do pracy w zawodzie**
- **trwałego, istotnego zeszpecenia lub zniekształcenia ciała**

podlega karze pozbawienia wolności na czas nie krótszy od lat 3

§ 2. Jeżeli sprawca działa nieumyślnie:
podlega karze pozbawienia wolności do lat 3

§ 3. Jeżeli następstwem czynu określonego w § 1 jest śmierć człowieka
sprawca podlega karze pozbawienia wolności od lat 5, karze 25 lat pozbawienia wolności albo karze dożywotniego pozbawienia wolności

Źródło: Dz.U.2020.0.1444 t.j. - Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny Rozdział XIX.

Spowodowanie średniego i lekkiego uszczerbku na zdrowiu

Spowodowanie średniego i lekkiego uszczerbku na zdrowiu art. 157 kk

§ 1. Kto powoduje naruszenie czynności narządu ciała lub rozstrój zdrowia, inny niż określony w art. 156 spowodowanie ciężkiego uszczerbku na zdrowiu § 1

podlega karze pozbawienia wolności od 3 miesięcy do lat 5

§ 2. Kto powoduje naruszenie czynności narządu ciała lub rozstrój zdrowia trwający nie dłużej niż 7 dni

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2

§ 3. Jeżeli sprawca czynu określonego w § 1 lub 2 działa nieumyślnie

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku

§ 4. Ściganie przestępstwa określonego w § 2 lub 3, jeżeli naruszenie czynności narządu ciała lub rozstrój zdrowia nie trwał dłużej niż 7 dni

odbywa się z oskarżenia prywatnego

§ 5. Jeżeli pokrzywdzonym jest osoba najbliższa

ściganie przestępstwa określonego w § 3 następuje na jej wniosek

Źródło: Dz.U.2020.0.1444 t.j. - Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny Rozdział XIX.

Udział w bójce lub pobiciu

Udział w bójce lub pobiciu art. 158

§ 1. Kto bierze udział w bójce lub pobiciu, w którym naraża się człowieka na bezpośrednie niebezpieczeństwo utraty życia albo nastąpienie skutku określonego

w art. 156 spowodowanie ciężkiego uszczerbku na zdrowiu § 1

w art. 157 spowodowanie średniego i lekkiego uszczerbku na zdrowiu § 1

podlega karze pozbawienia wolności do lat 3

§ 2. Jeżeli następstwem bójki lub pobicia jest ciężki uszczerbek na zdrowiu człowieka

podlega karze pozbawienia wolności od 6 miesięcy do lat 8

§ 3. Jeżeli następstwem bójki lub pobicia jest śmierć człowieka

podlega karze pozbawienia wolności od roku do lat 10

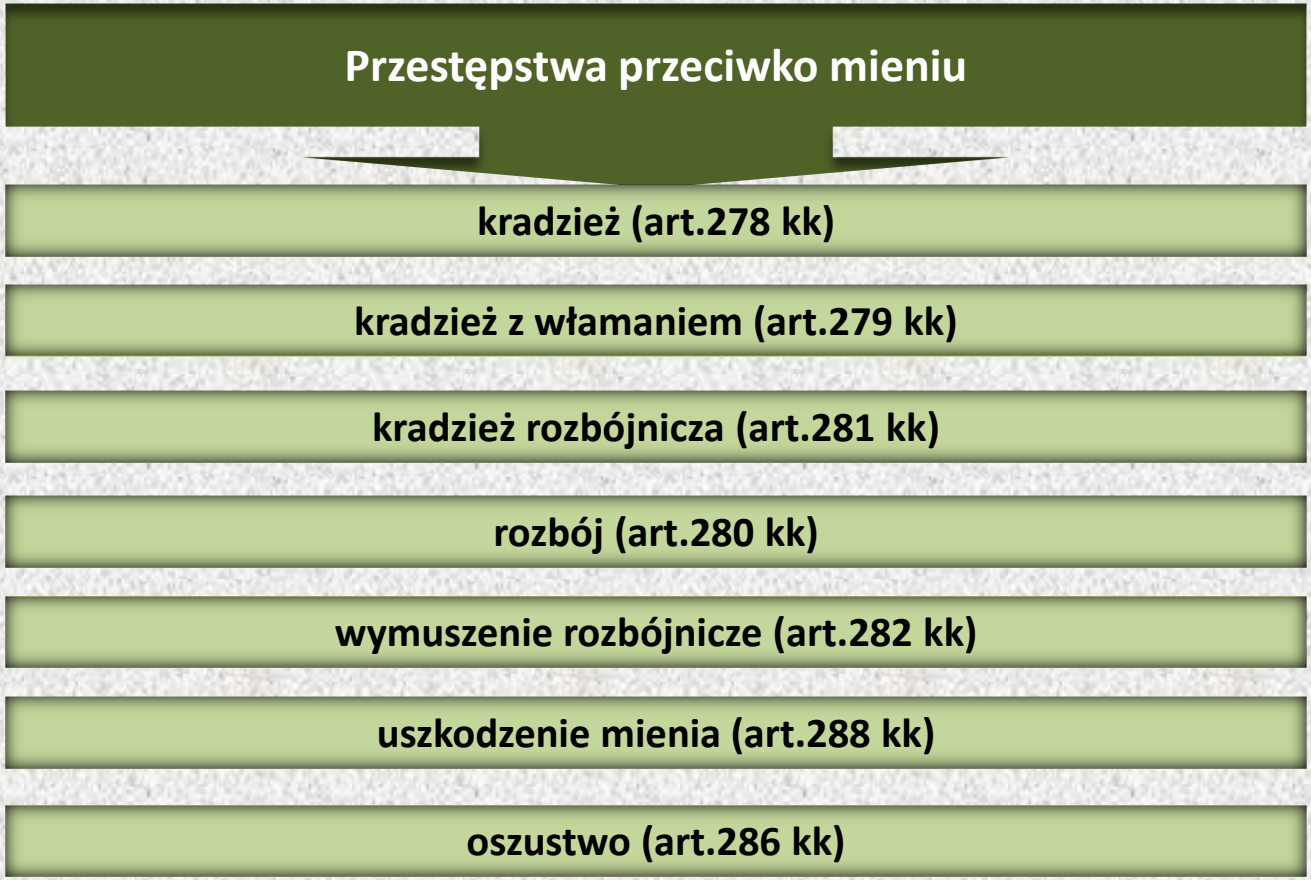
Art. 159. Użycie w bójce lub pobiciu niebezpiecznych przedmiotów art. 159

Kto, biorąc udział w bójce lub pobiciu człowieka, używa broni palnej, noża lub innego podobnie niebezpiecznego przedmiotu

podlega karze pozbawienia wolności od 6 miesięcy do lat 8

Źródło: Dz.U.2020.0.1444 t.j. - Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny Rozdział XIX.

Przestępstwa przeciwko mieniu



Źródło: Dz.U.2020.1444 t.j. | Akt obowiązujący Wersja od: 22 czerwca 2021 r Dział XXXV (pobrano 24.08.2021)

Kradzież

Kradzież art. 278

§ 1. Kto zabiera w celu przywłaszczenia cudzą rzecz ruchomą

podlega karze pozbawienia wolności od 3 miesięcy do lat 5

§ 2. Kto bez zgody osoby uprawnionej uzyskuje cudzy program komputerowy w celu osiągnięcia korzyści majątkowej

podlega karze pozbawienia wolności od 3 miesięcy do lat 5

§ 3. W wypadku mniejszej wagi

Sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku

Kradzież szczególnie zuchwała art. 278 a

§ 1. Kto dopuszcza się kradzieży szczególnie zuchwałej

podlega karze pozbawienia wolności od 6 miesięcy do lat 8

Kradzież z włamaniem art. 279

§ 1. Kto kradnie z włamaniem

podlega karze pozbawienia wolności od roku do lat 10

Źródło: Dz.U.2020.0.1444 t.j. - Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny Rozdział XIX.

Rozbój

Rozbój art. 280

§ 1. Kto kradnie, używając przemocy wobec osoby lub grożąc natychmiastowym jej użyciem albo doprowadzając człowieka do stanu nieprzytomności lub bezbronności

podlega karze pozbawienia wolności od lat 2 do 12

§ 2. Jeżeli sprawca rozboju posługuje się bronią palną, nożem lub innym podobnie niebezpiecznym przedmiotem lub środkiem obezwładniającym albo działa w inny sposób bezpośrednio zagrażający życiu lub wspólnie z inną osobą, która posługuje się taką bronią

podlega karze pozbawienia wolności na czas nie krótszy od lat 3

Kradzież rozbójnicza art. 281

Kto, w celu utrzymania się w posiadaniu zabranej rzeczy, bezpośrednio po dokonaniu kradzieży, używa przemocy wobec osoby lub grozi natychmiastowym jej użyciem albo doprowadza człowieka do stanu nieprzytomności lub bezbronności

podlega karze pozbawienia wolności od roku do lat 10

Wymuszenie rozbójnicze art. 282

Kto, w celu osiągnięcia korzyści majątkowej, przemocą, groźbą zamachu na życie lub zdrowie albo gwałtownego zamachu na mienie, doprowadza inną osobę do rozporządzenia mieniem własnym lub cudzym albo do zaprzestania działalności gospodarczej

podlega karze pozbawienia wolności od roku do lat 10

Źródło: Dz.U.2020.0.1444 t.j. - Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny Rozdział XIX.

Zniszczenie mienia ruchomego

Zniszczenie mienia ruchomego art. 288

§ 1. Kto cudzą rzecz niszczy, uszkadza lub czyni niezdatną do użytku

podlega karze pozbawienia wolności od 3 miesięcy do lat 5

§ 2. W wypadku mniejszej wagi

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku

§ 3. Kto przerywa lub uszkadza kabel podmorski albo narusza przepisy obowiązujące przy zakładaniu lub naprawie takiego kabla

podlega karze pozbawienia wolności od 3 miesięcy do lat 5

Źródło: Dz.U.2020.0.1444 t.j. - Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny Rozdział XIX.

Oszustwo

Oszustwo art. 286

§ 1. Kto, w celu osiągnięcia korzyści majątkowej, doprowadza inną osobę do niekorzystnego rozporządzenia własnym lub cudzym mieniem za pomocą wprowadzenia jej w błąd albo wyzyskania błędu lub niezdolności do należytego pojmowania przedsiębranego działania

podlega karze pozbawienia wolności od 6 miesięcy do lat 8

§ 2. Kto żąda korzyści majątkowej w zamian za zwrot bezprawnie zabranej rzeczy

podlega karze pozbawienia wolności od 6 miesięcy do lat 8

§ 3. W wypadku mniejszej wagi

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2

Źródło: Dz.U.2020.0.1444 t.j. - Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny Rozdział XIX.

Przestępstwa gospodarcze

Wyjaśnienie pojęcia przestępstwa gospodarcze

Pojęcie „przestępstwo gospodarcze”
stanowi zbiorcze i umowne nazwanie kategorii, głównie pozakodeksowych, przepisów karnych określających czyny zabronione mające związek z obrotem gospodarczym[1].

Przestępstwo gospodarcze
to zachowanie uczestników obrotu gospodarczego, z którego przynajmniej jeden jest podmiotem profesjonalnym i powstałe na skutek tych zachowań czyny społecznie szkodliwe w stopniu wyższym niż znikomy, bezprawne, zawinione oraz zagrożone karą[2].

Przestępstwami gospodarczymi
są czyny karalne godzące lub zagrażające ponadindywidualnym dobrom w sferze życia gospodarczego, polegające na naruszeniu zaufania, związanego z pozycją sprawcy, lub instytucją życia gospodarczego, grożące utratą zaufania społecznego gospodarczego lub jego podstawowych instytucji”[3].

[1] Przestępczość gospodarcza. Istota zjawiska. Zasady odpowiedzialności, mechanizmy przestępcze i metody działania sprawców, Warszawa (red. nauk. I. Malinowska, P. Łabuz, M. Michalski, T. Safjański), Księgarnia Beck, Warszawa 2018, s. 43.
[2] Encyklopedia zarządzania, Księgarnia Beck, s. 43.
[3] O. Górniok, Przestępczość gospodarcza i jej zwalczanie, Wydawnictwo Naukowe PWN, Warszawa 1994, s. 16.

Cechy przestępczości gospodarczej

utajony charakter

pozorna legalność

świadomość działania

brak elementów przemocy

zorganizowana forma działalności

powtarzalność czynów zabronionych

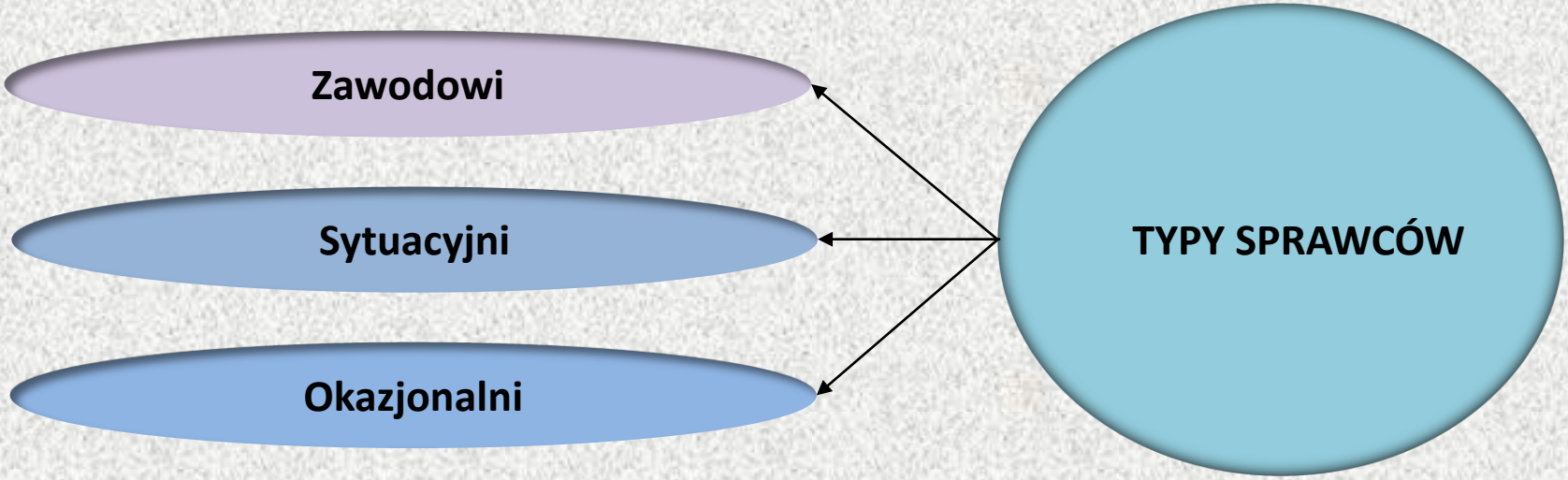
związek między przestępczą działalnością a pozycją sprawcy

determinowanie strat materialnych, a także niematerialnych

ofiarami są anonimowe osoby, instytucje, grupy społeczne, a także podmioty systemu gospodarczego

[1] L. Wilk, Przestępczość gospodarcza – pojęcie, przyczyny, sprawcy. Edukacja Prawnicza, 2012, nr 10 (136), s. 12.

Typy sprawców przestępstw gospodarczych



Sprawcy zawodowi

osoby utrzymujące się tylko z przestępczości gospodarczej,
popełniając przestępstwa w różnych gałęziach, wiążących się z obrotem gospodarczym[1].

Sprawcy sytuacyjni

osoby popełniające przestępstwa gospodarcze z uwagi na wystąpienie takiej konieczności,
celem zdobycia środków finansowych niezbędnych dla kontynuacji prowadzenia własnej, legalnej działalności[1].

Sprawcy okazjonalni

osoby popełniające przestępstwa gospodarcze w momentach,
w których nadarza się okazja do tego, by dzięki nim uzyskać znaczne korzyści materialne[1].

[1] K. Kozdra, Przestępczość gospodarcza – pojęcie, istota, cechy, NE, 2019, nr 30, s. 51.

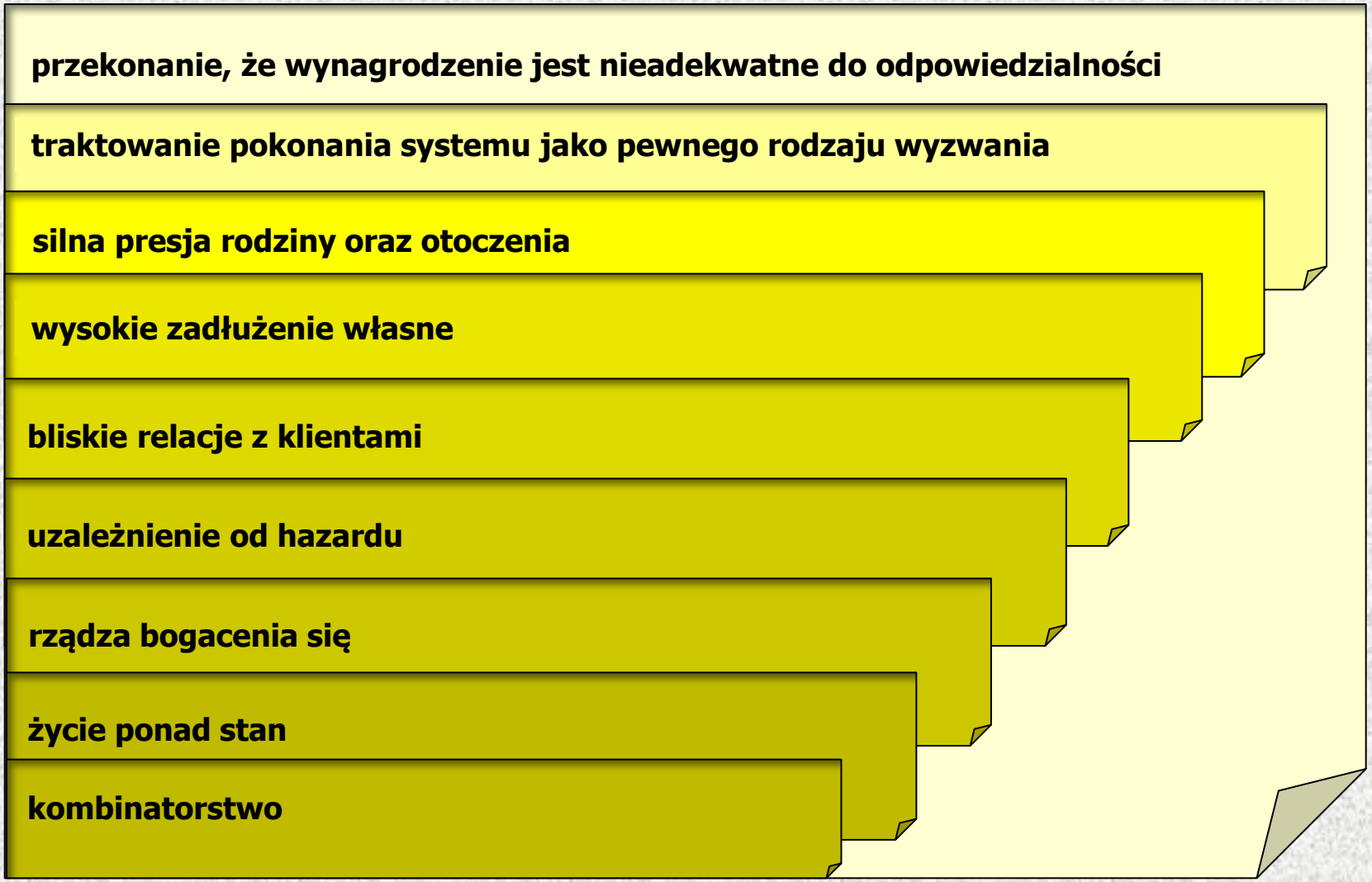
Przesłanki do popełniania przestępczości gospodarczej

Jedna z teorii odnoszących się do przyczyn popełniania przestępczości gospodarczej została opracowana przez D. R. Cressey'a[1]:

- **przymus finansowy**
- **okazja bezkarnego popełnienia przestępstwa**
- **psychiczna umiejętność uzasadnienia sobie, że popełniany czyn nie jest przestępstwem**

[1] M. Kutera, A. Hołda, S.T. Surdykowska, Oszustwa księgowe. Teoria i praktyka, Difin, Warszawa 2006, s. 159.

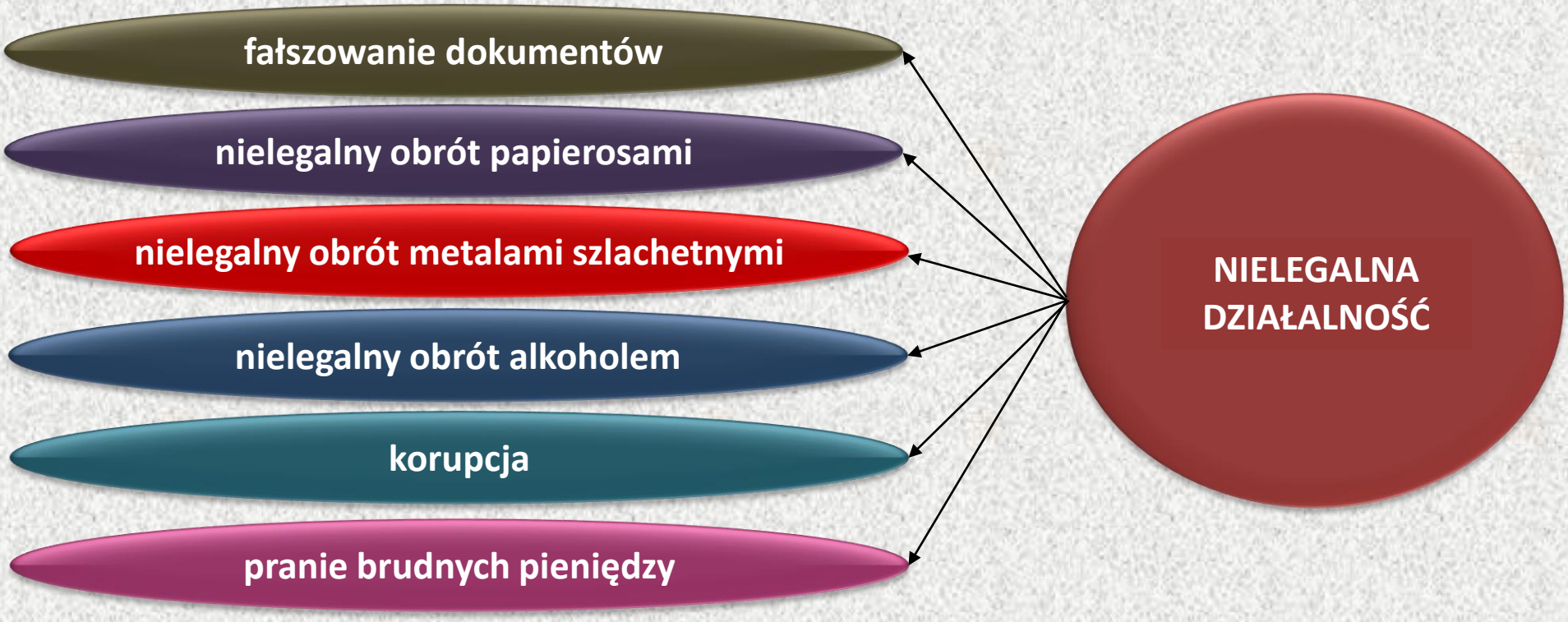
Motywy działania sprawców przestępczości gospodarczej



[1] M. Kutera, A. Hołda, S.T. Surdykowska, Oszustwa księgowe. Teoria i praktyka, Difin, Warszawa 2006, s. 159.

Nielegalna działalność

Z przestępstwami gospodarczymi współwystępuje często wiele innych rodzajów nielegalnej działalności, wśród których można wskazać m.in.[1]:



Źródło: I. Malinowska, Przestępne mechanizmy podatkowe. [w:] Przestępczość gospodarcza. Istota zjawiska. Zasady odpowiedzialności, mechanizmy przestępcze i metody działania sprawców. P. Łabuza, I. Malinowska (red.), CH BECK, Warszawa 2018, s. 118.

Przestępstwa gospodarcze i grożące za nie kary

Grupa	Rodzaj	Przepis	Zagrożenie karą
Przestępstwa na szkodę jednostek, w których osoba popełniająca przestępstwo pełni funkcje decyzyjne			
Nadużycie zaufania w obrocie gospodarczym	**Nadużycie uprawnień**	**Art. 296 k.k.**	**Kara pozbawienia wolności 3 m-ce – 5 lat**
	Niedopełnienie obowiązku	**Art. 296 k.k.**	**Kara pozbawienia wolności 3 m-ce – 5 lat**
	Naruszenie tajemnicy przedsiębiorstwa	**Art. 296 k.k.**	**Grzywna, kara ograniczenia wolności albo pozbawienia wolności do 2 lat**
Przestępstwa przeciwko mieniu	**Oszustwo**	**Art. 286 k. k.**	**Grzywna, kara ograniczenia wolności albo pozbawienia wolności do 2 lat**
	Przywłaszczenie mienia	**Art. 284 k. k.**	**Kara pozbawienia wolności 6 m-cy – 8 lat**
	Kradzież	**Art. 278 k. k.**	**Kara pozbawienia wolności do 3 lat**
	Oszustwo komputerowe	**Art. 278 k. k.**	**Kara pozbawienia wolności 3 m-ce – 5 lat**
Inne przestępstwa			

Źródło: P. Szymanowski, Funkcjonowanie systemu zwalczania gospodarczej przestępczości zorganizowanej w trójmieście na przestrzeni ostatniej dekady, Poznań 2021, s. 41.

Terroryzm

Pojęcie terroryzmu

Terroryzm
wg Departamentu Sprawiedliwości USA jest to:
,,(…) gwałtowne kryminalne zachowanie, mające na celu wpłynąć na sposób sprawowania władzy przez zastraszanie i przymus, zastraszyć i zmuszać ludność cywilną, lub wpłynąć na sposób sprawowania rządów przez zamach lub porwanie”[1].

Terroryzm
wg CIA to:
„groźba użycia przemocy lub jej użycie dla celów politycznych przez grupy lub jednostki, niezależnie czy działają one na rzecz czy też w opozycji do ustanowionej władzy państwowej, w sytuacji gdy powyższe działania mają zastraszyć czy przerazić więcej osób niż tylko bezpośrednie ofiary”.

Terroryzm
wg Departamentu Stanu USA to:
„umotywowana politycznie przemoc wobec celów nie biorących udziału w walce, stosowana przez subnarodowe grupy czy tajnych agentów”[2].

[1] S. Wojciechowski, Terroryzm. Analiza pojęcia, „Przegląd Bezpieczeństwa Wewnętrznego’’, nr 1, 2009 r., s. 64-65.
[2] http://portalsocjologa.pl/artykuly/spoleczne-oraz-psychologiczne-determinanty-wystepowania-zjawiska-terroryzmu-islamskiego/ (20.01.2018)

Pojęcie terroryzmu

Terroryzm
wg Federalnego Biura Śledczego (FBI) to:
„bezprawne użycie siły lub przemocy wobec osób lub mienia, celem zastraszenia lub wywarcia przymusu na ludność cywilną, rząd albo części wyżej wymienionych, co zmierza do promowania celów politycznych lub społecznych”[1].

Terroryzm
w rozumowaniu rosyjskim to:
„przemoc lub grożenie jej zastosowaniem w stosunku do osób i organizacji, zniszczenie lub groźba zniszczenia majątku i innych obiektów, mogąca grozić śmiercią ludzi, będąca przyczyną znacznej szkody w majątku lub powodująca wystąpienie innych społecznie niebezpiecznych następstw dokonana w celu naruszenia spokoju społecznego czy zastraszenia społeczeństwa”[2].

Terroryzm
we Francji to:
„rozmyślne działanie mające na celu, poprzez przemoc lub zastraszenie, obalenie instytucji demokratycznych bądź przejęcie kontroli nad terytorium narodowego, podlegającego władzy państwowej”[2].

[1] http://portalsocjologa.pl/artykuly/spoleczne-oraz-psychologiczne-determinanty-wystepowania-zjawiska-terroryzmu-islamskiego/ (20.01.2018)
[2] K. Załęski, Terroryzm w lotnictwie. Problem definicji, „Logistyka”, nr 3, 2012, s. 251.

Terroryzm

Terroryzm może być składnią następujących elementów[1]:

działania zaplanowane i/lub zrealizowane przez jedną osobę lub grupę, które mają charakter destrukcyjny, przemyślany i są niezgodne z prawem

owe działania wynikają z różnych motywów i mają odmienne cele, jak np. religijne, polityczne czy osobiste

podejmowane działania terrorystyczne są skierowane w naród lub inny podmiot międzynarodowy, jego przedstawicieli i instytucje

podejmowane działania terrorystyczne są skierowane na osoby publiczne związane lub nie związane ze światem polityki; obejmuje również ,,zwykłych'' obywateli oraz ich mienie

[1] S. Wojciechowski, Terroryzm. Analiza pojęcia, „Przegląd Bezpieczeństwa Wewnętrznego'', nr 1, 2009, s. 66.

Istota terroryzmu

Terroryzm wg S. Pikulskiego[1]:

Terroryzm utożsamia z działalnością przestępczą mającą tło polityczne, której dopuszczają się zorganizowane grupy przestępcze, mające charakter antypaństwowy.

Akty terrorystyczne przeprowadzane przez te ugrupowania mają na celu wymuszanie pewnych ustępstw, w odpowiedzi na żądania terrorystycznych grup przestępczych.

Osiąganie swych celów przez wspomniane grupy następuje w wyniku stosowania działań zastraszania, wywoływania paniki w danym państwie (opinii publicznej).

Działają one poprzez podkładanie ładunków wybuchowych w miejscach publicznych oraz dokonywanie zamachów na życie osobistości znanych, najczęściej polityków

[1] S. Pikulski, Prawne środki zwalczania terroryzmu, Olsztyn 2000, s. 13.

Istota terroryzmu

Terroryzm

należy wiązać ze zjawiskiem terroru, znanego jest już od wieków, a wywodzi się z łacińskiego języka co oznacza „stosowanie przemocy, okrucieństwa i gwałtu, zniszczenia, celem zastraszenia”[1].

Akty terrorystyczne przeprowadzane przez te ugrupowania mają na celu wymuszanie pewnych ustępstw, w odpowiedzi na żądania terrorystycznych grup przestępczych.

Współczesny terroryzm sprowadza się do podejmowanych przez różne ugrupowania aktów przemocy, albo stosowania gróźb i ich użycia w celu zaszantażowania władzy, ale również opinii publicznej[2].

Jest to swoista metoda walki mająca skutecznie doprowadzić terrorystów (stosujących terror) do tego, by mogli osiągnąć określone cele polityczne za pomocą zbrodni jako narzędzia swego działania, po to, żeby doprowadzić do wywołania ogólnego strachu[2].

[1] R. Marcinkowski, Encyklopedia Popularna, Warszawa 1982, s.787.

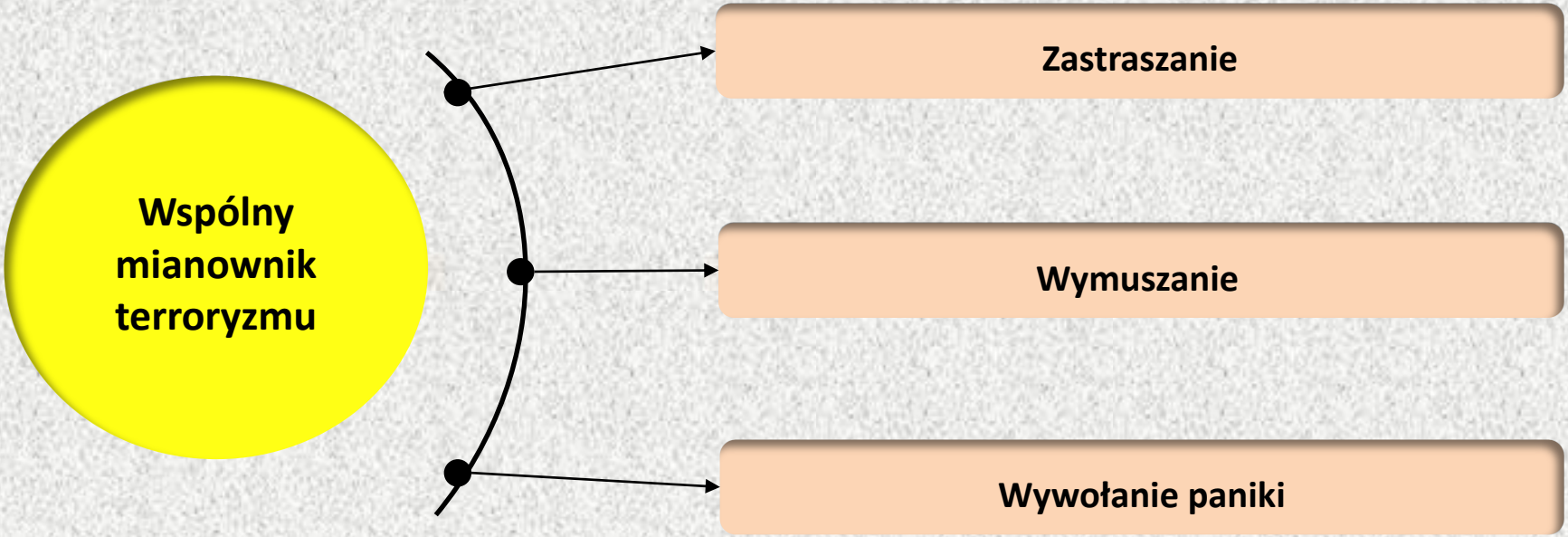
[2] R. Borkowski, Terroryzm ponowoczesny. Studium z antropologii polityki, Toruń 2006, s. 45-46.

Cechy charakterystyczne terroryzmu

- **przemoc zbrojna jest najlepszą metodę walki politycznej (fetyszyzacja przemocy)[1]**
- **stosowanie przez terrorystów przemocy i okrucieństwa, a także moralnego nihilizmu (brak wartości moralnych) w celu pokazania zarówno siły, jak i ich determinacji (gotowości na wszystko), a także wywołania ogólnego strachu przed terrorystami**
- **totalne zastraszanie, tak politycznych elit, jak i społeczeństwa**
- **nadanie rozgłosu działaniom terrorystów w massmediach poprzez ukazywanie skutków działań terrorystycznych**
- **szantażowanie polityczne (polityków), celem uzyskania zamierzonych zmian mających polityczny wydźwięk**
- **podejmowane przez terrorystów akty przemocy niekoniecznie muszą obalić władzę, ale zazwyczaj prowadzą do przygotowania podłoża dla rewolucji i mają spowodować anarchię w życiu publicznym, zastraszyć i zdemoralizować państwowych funkcjonariuszy**
- **ukazanie powszechnej siły terrorystów i spowodowanie, że wobec obywateli będą stosowane represje, co ma doprowadzić do ograniczenia przez państwo obywatelskich swobód i narastania nastrojów buntowniczych**

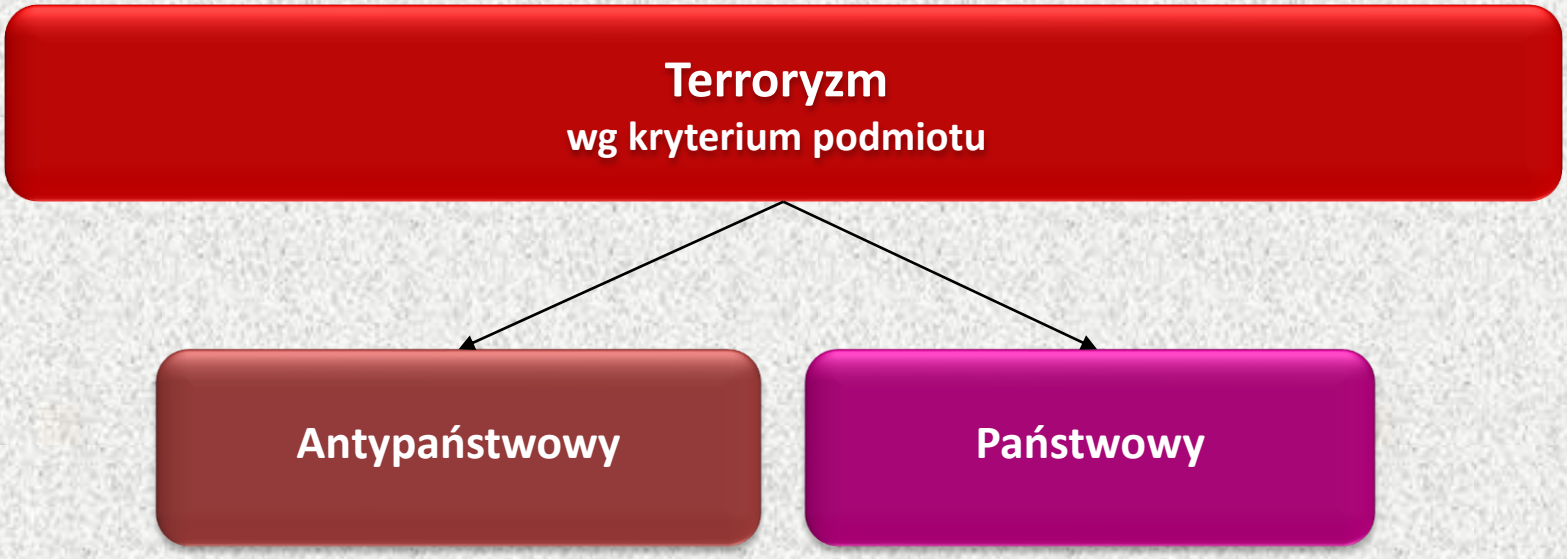
[1] R. Borkowski, Terroryzm ponowoczesny. Studium z antropologii polityki, Toruń 2006, s. 45-46.

„Wspólny mianownik” terroryzmu



Opracowano na podstawie: D. Wodziński, Oblicza terroryzmu w Europie zachodniej na przykładzie Francji i Belgii, Wyższa Szkoła Bezpieczeństwa, Poznań, 2017, s. 19.

Klasyfikacja terroryzmu

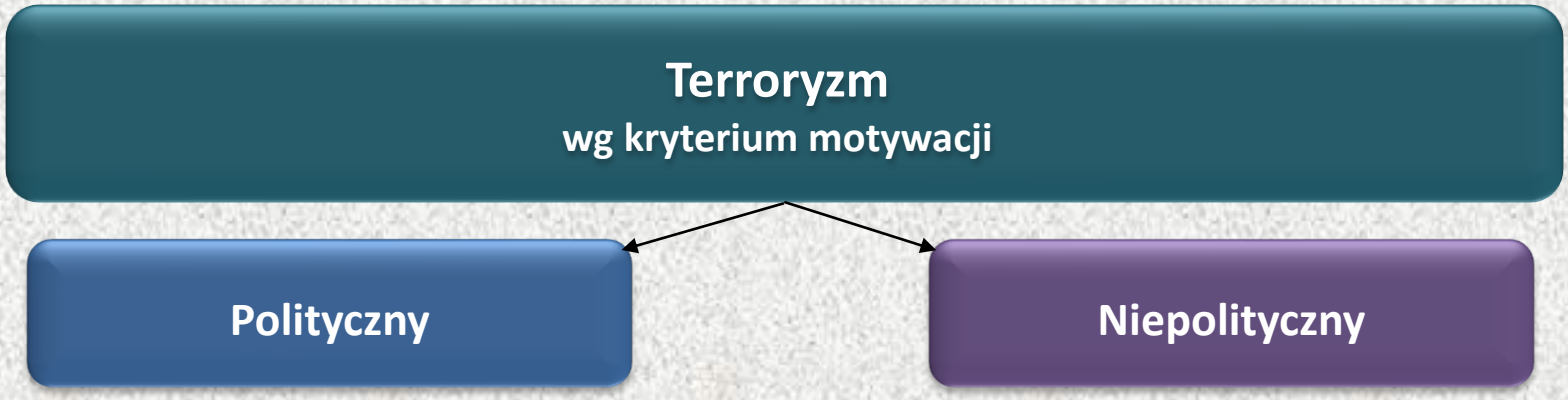


Terroryzm antypaństwowy
realizowany jest przez zgrupowania, ruchy lub indywidualne osoby mające na celu utratę stanu równowagi budowy państwa oraz ładu społecznego[1].

Terroryzm państwowy
"zastraszające działanie władzy państwowej wobec obywateli”[2].

[1] K. Karolczak, Encyklopedia terroryzmu, Warszawa 1995, s. 13–15.
[2] B. Hołyst, Kryminologia, Warszawa 1986, s. 116.

Klasyfikacja terroryzmu

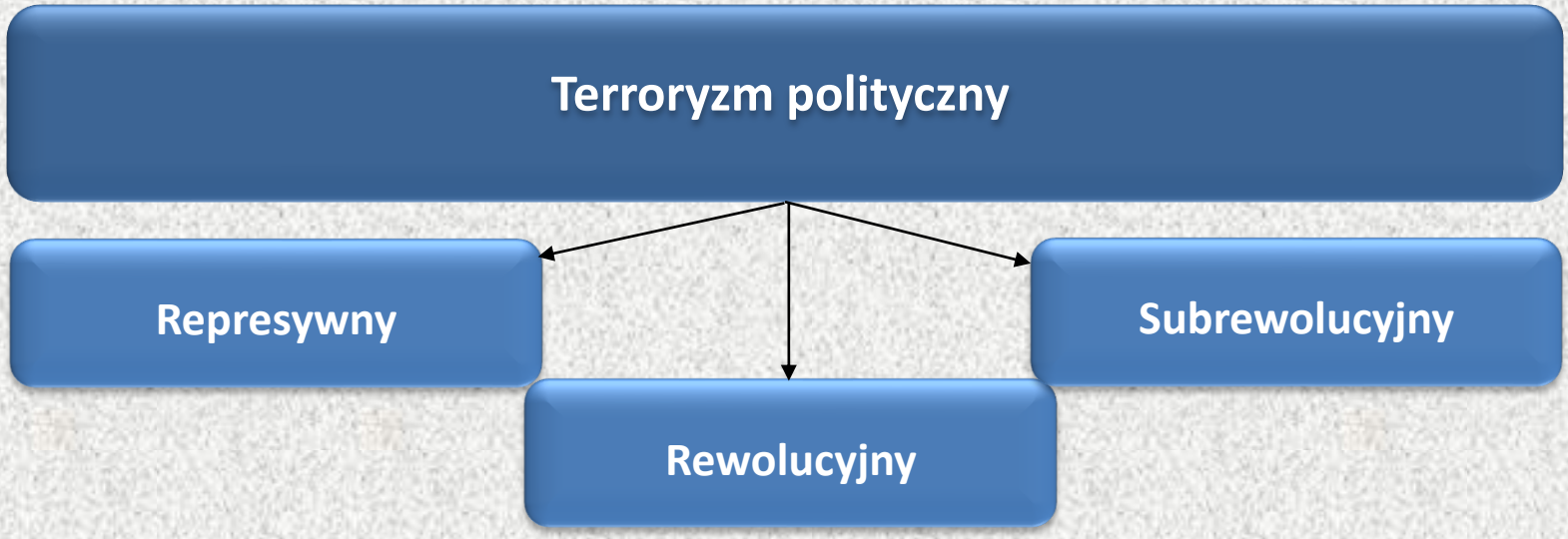


Terroryzm polityczny
sprawcy, wywołując stan zastraszenia, kierują się motywami politycznymi, w tym także kwestiami religijnymi lub ideologicznymi[1].

Terroryzm niepolityczny
nie mający żadnego powiązania z polityką, władzą, ze względu na motywację działania[2].

[1] K. Karolczak, Encyklopedia terroryzmu, Warszawa 1995, s. 13–15.
[2] T. Wałek, Pojęcie, geneza i klasyfikacja zjawisk terrorystycznych, Securitologia No 2/2018, s. 121.

Terroryzm polityczny



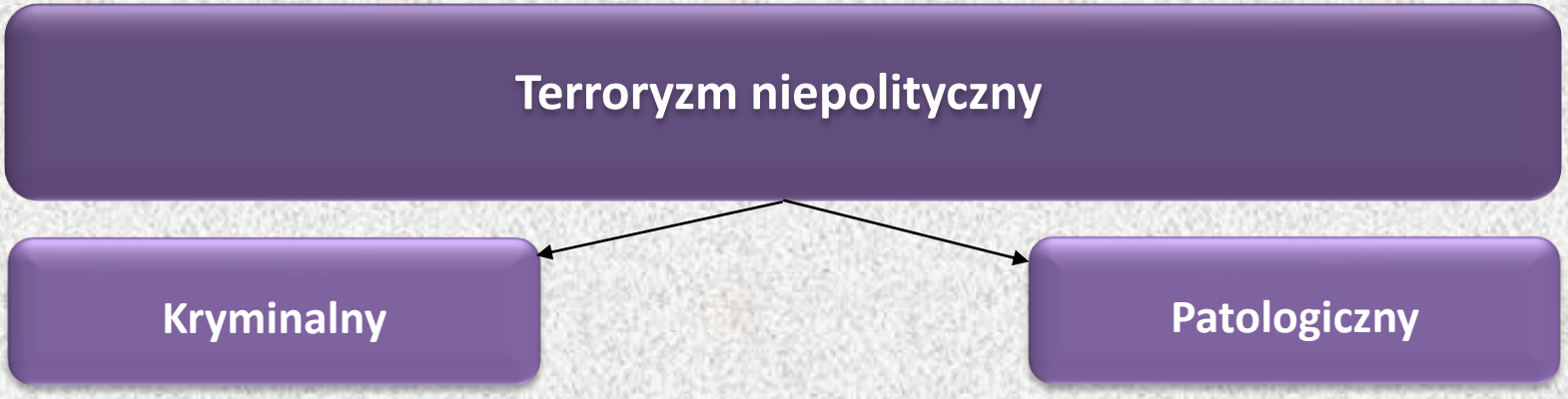
Terroryzm represywny
wykorzystywany głównie przez państwo i jego aparat policyjny do poskromienia oraz podporządkowania określonych grup i jednostek.

Terroryzm subrewolucyjny
działalność motywowanych ideologicznie niewielkich grup lub jednostek, które stosują przemoc w różnych celach, np. zastraszania, ukarania lub zemsty, lecz nie są w stanie przeprowadzić fundamentalnych zmian.

Terroryzm rewolucyjny
jego celem jest rewolucja zmierzająca do zasadniczych przemian w strukturze państwa.

Opracowano na podstawie: K. Wiak, Prawnokarne środki przeciwdziałania terroryzmowi, Lublin 2010, s. 21.

Terroryzm niepolityczny



Terroryzm kryminalny

obejmuje przestępstwa pospolite, popełniane przez sprawców wykorzystujących terrorystyczne metody działania w celu osiągnięcia zysku.

Terroryzm patologiczny

akty terrorystyczne popełniane przez osoby z zakłóceniami czynności psychicznych, których motywy nie dają się jednoznacznie ustalić, niewątpliwie są efektem frustracji lub nienawiści odczuwanej wobec określonych osób, grup społecznych lub instytucji.

Opracowano na podstawie: T. Wałek, Pojęcie, geneza i klasyfikacja zjawisk terrorystycznych, Securitologia No 2/2018 AWF, Kraków 2018, s. 121.

Inny podział terroryzmy

Terroryzm
wg A. Pawłowskiego

Indywidualny	**akty przemocy skierowane przeciwko życiu osób, dobranych konkretnie albo oznaczonych zaledwie grupowo**
Ekonomiczny	**godzi „w zastane stosunki gospodarcze, a zwłaszcza w prawo wykonywania tytułu własności przez fabrykantów, itd.”.**
Represyjny	**stosowany przez dominującą grupę społeczną, której przywileje zostają zagrożone**
Powstańczy	**o charakterze etniczno-nacjonalistyczno-separatystycznym**
Społeczno-rewolucyjny	**dążący do zmian politycznego systemu**

A. Pawłowski, Typologia terroryzmu politycznego, [w:] Terroryzm polityczny, (red.) Muszyński J., PWN, Warszawa 1991.

Cyberprzestępczość i cyberterroryzm

Cyberprzestrzeń stworzyła możliwości i zagrożenia

Zagrożenia

Korzyści

Komputery

Smartfony

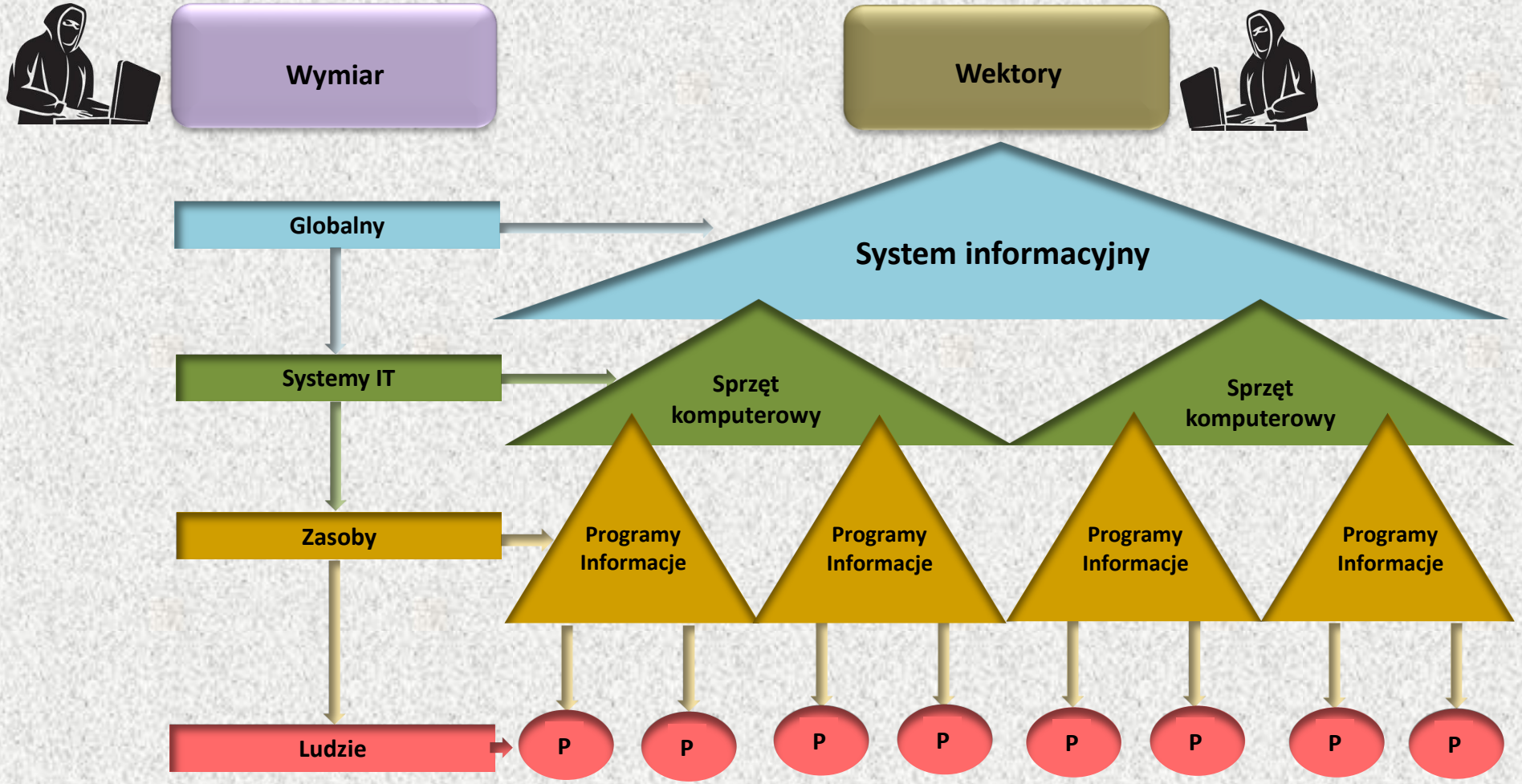
Tablety

Systemy informatyczne

Programy

MOŻLIWOŚCI	OGRANICZENIA
Przestrzeń Edukacyjna	Cyberprzestępstwa
Przestrzeń Badawcza	Obszar kooperacji negatywnej
Globalna Komunikacja- wymiana doświadczeń	Cyberinwigilacja
Rozwój e-biznesu	Cyberterroryzm
Propagowanie gospodarki opartej na wiedzy	Cyberwojna
Rozwój kultury, wirtualna ikonosfera	Walka elektroniczna
Globalna arena igrzysk gier i zabaw	Dezinformacja
Rozwój gospodarczy	Utrata „wolności” obywateli

Wektory cyberprzestępczości i cyberterroryzmu



Źródło clipard: https://pl.123rf.com/photo_21116517_karykatura-terrorysty-ilustracja.html?vti=mgxlopdn823xm1insc-1-63

Specyfika cyberprzestępczości

Przestępczość elektroniczna = Przestępczość komputerowa = Cyberprzestępczość

- Nieuprawniony dostęp do informacji
- Nieuprawniony dostęp do danych
- Naruszanie praw dostępu do zasobów
- Modyfikacja zasobów
- Propagowanie terroryzmu
- Pranie brudnych pieniędzy
- Zastraszanie szantaż

Internet

- Bezpieczeństwo informacji
- Bezpieczeństwo systemów IT

- Powielanie programów
- Sabotaż sprzętu i oprogramowania
- Propagowanie pornografii
- Oszustwa finansowe
- Namawianie do czynów przestępczych
- Uporczywe nękanie (Stalking)
- Propagowanie sekt religijnych

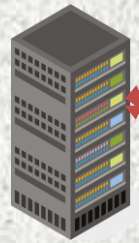
Klasyfikacje zagrożeń cyberbezpieczeństwa

Zagrożenia wymierzone w systemy informatyczne

- DoS DDoS DRDoS
- SYN flood Fork - Bomb

point-to-point

Internet link



Victim

Zagrożenia wymierzone w zasoby informacyjne

- Wirusy, Robaki, Trojany
- Kryptowirusy

point-to-point

Internet link

flooding
flooding
flooding
flooding
flooding
flooding

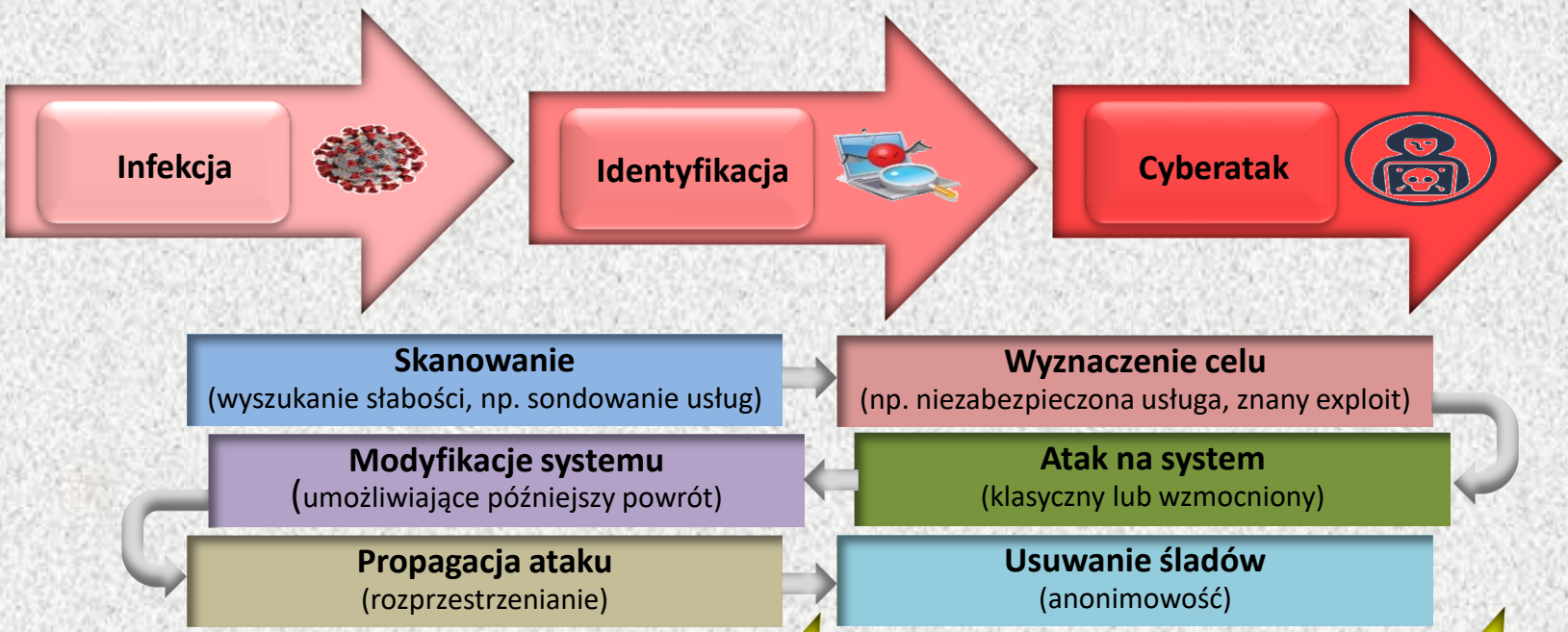
Amplifier

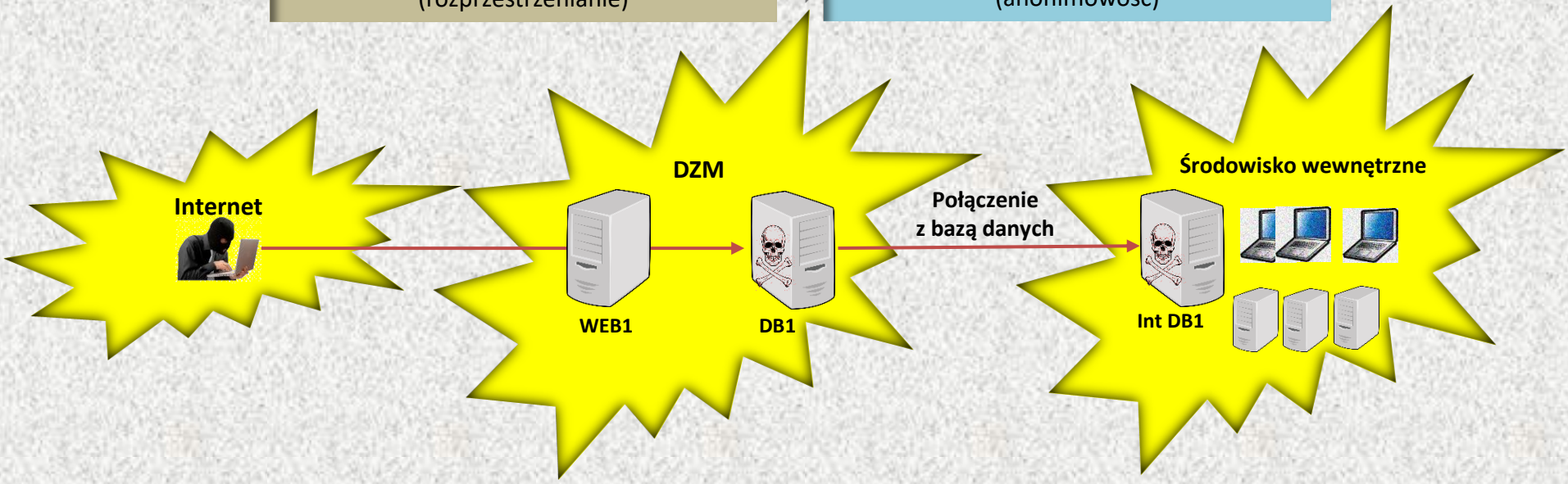
Victim

Zagrożenia wymierzone w celu łamania (uzyskania) haseł

- Brute Force
- Phishing

Standardowa technologia cyberataku





Źródło: Opracowano na podstawie: J. T. Luttgens, K. Mandia, Incydenty bezpieczeństwa. Metody reagowania w informatyczce śledczej, Wydawnictwo Helion, s. 31.

Współcześnie dominujące cyberzagrożenia

Wybrane cyberzagrożenia - **Denial of Service**

DoS

Ataki typu odmowa usługi są skierowane przeciwko sieciom i systemom komputerowym. Celem ataku DoS jest uniemożliwienie działania sieci komputerowej i jej usług, poprzez wykorzystanie do tego celu błędów w protokołach i aplikacjach.

DoS

Technologia ataku polega na przeciążeniu aplikacji serwującej określone dane poprzez wysyłanie dużej liczby pakietów w celu wyczerpania zasobów systemu, tak by doprowadzić do załamania pracy aplikacji.[1] Ataki DoS można również podzielić na: skierowane przeciwko sieci oraz przeciwko systemom komputerowym.

DDoS

Zwielokrotnienie ataku DoS poprzez jego przeprowadzanie jednocześnie z wielu sensorów. Atak rozpoczyna się z komputera, który wysyła odpowiedni rozkaz do węzłów, te z kolei wysyłają go dalej do agentów, aby przeprowadzić atak na ofiarę. Rezultatem jest załamanie pracy aplikacji świadczących usługi blokowanie dostępu do zasobów sieci.

DRDoS

Przebieg ataku polega na generowaniu specjalnych pakietów SYN, których adres jest sfałszowany – jest nim adres ofiary. Duża liczba takich pakietów jest wysyłana do sieci. Komputery, do których one docierają, odpowiadają na adres pochodzący z fałszywego nagłówka, w efekcie otrzymuje wiele pakietów, blokujących świadczenie normalnych usług.

Fork-bomba

Jest rodzajem ataku DoS, zakładającym, że w środowisku rozproszonym – wieloprocesowym tylko część procesów może być uruchomiona równocześnie. Przebieg ataku polega na szybkim „rozmnożeniu się" kopii programu (aplikacji) w celu wypełnienia tablicy procesów systemu operacyjnego, tym samym jego zablokowanie – powstaje tzw. bomba.[2]

Opracowano na podstawie: M. Czyżak, Wybrane aspekty zjawiska cyberterroryzmu.
T, Galanciak, Ataki typu DoS. Anatomia zagrożenia i możliwości obrony, Magazyn T3

Wybrane cyberzagrożenia - **Phishing**

Phishing ⇨ Atak socjotechniczny, masowy, polega na podszywaniu się pod stronę lub odpowiednio spreparowany mail. Zainfekowanie komputera szkodliwym oprogramowaniem czy też nakłonienie ofiary do określonych działań.

Clone phishing	**Prawdziwy e-mail posiadający załącznik lub link zostaje użyty przez przestępcę jako wzór przy tworzeniu wiadomości na potrzeby oszustwa. Załączniki lub linki zostają zastąpione złośliwymi wersjami, a następnie wysłane z adresu e-mail sfałszowanego tak, aby wyglądał jak ten należący do oryginalnego nadawcy.[1]**
Spear phishing	**Phishing spersonalizowany na konkretną grupę lub konkretny typ osób, np. administratorów systemu firmy.[1] „Upatrzona zdobycz" - Oszuści najpierw zbierają informacje na temat ofiary, co znacznie zwiększa ich szanse na powodzenie ataku.**
Whaling	**Celem tego typu ataków są dyrektorzy generalni, dyrektorzy finansowi i wszyscy inni dyrektorzy w branży lub konkretnej firmie. Whaling to jeszcze precyzyjniejszy rodzaj ataku phishingowego, ponieważ jego celem są osoby z kierownictwa wyższego szczebla i innych ważnych celów z branży biznesowej.**
Smishing	**Rodzaj ataku wykorzystujący komunikatory tekstowe lub SMS-y. Popularną techniką smishingu jest wysłanie na telefon komórkowy wiadomości SMS zawierającej łącze do kliknięcia lub numer do oddzwonienia. Przykładem tego ataku jest wiadomość SMS wyglądająca jakby została wysłana przez bank.**
Vishing	**Vishing ma taki sam cel, jak inne rodzaje ataku phishingowego. W tym przypadku także chodzi o kradzież wrażliwych danych osobowych lub firmowych. Ten rodzaj ataku jest przeprowadzany za pośrednictwem połączenia głosowego. Stąd litera „v" (od angielskiego słowa voice oznaczającego głos).[2]**

Opracowano na podstawie: Fake subpoenas harpoon 2,100 corporate fat cats (ang.), za: https://pl.wikipedia.org/wiki/Phishing
Jakie są typy phishingu? https://www.trendmicro.com/pl_pl/what-is/phishing/types-of-phishing.html [dostęp 2022-01-23]

Forma phishingu - **Pharming**

Pharming to bardziej niebezpieczna dla użytkownika oraz trudniejsza do wykrycia forma phishingu. Charakterystyczne dla pharmingu jest to, że nawet po wpisaniu prawidłowego adresu strony www, ofiara zostanie przekierowana na fałszywą (choć mogącą wyglądać tak samo) stronę WWW.

Opracowano na podstawie: D. Jurkiewicz, prezentacja nt. Cyberprzestrzenne zagrożenia, WSB, Poznań 2019.

Phishing

Poczta e-mail

Poczta e-mail

PHISHING

Tradycyjnie - kliknięcie w link lub pobrania załącznika

Obecnie - niezabezpieczone sieci domowe i pracowników zdalnych

Ataki phishingowe bazują na wykorzystywaniu złośliwego oprogramowania

Ransomware

Wirusy

Remote Access Trojan

Źródło: Cyberzagrożenia pracy zdalnej 2020: od botnetów do phishingu: https://alebank.pl/cyberzagrozenia-pracy-zdalnej-2020-od-botnetow-do-phishingu

Wybrane cyberzagrożenia - **Ransomware**

Ransomware

Ransomware należy do tzw. złośliwego oprogramowania (malware), blokują dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych (często poprzez techniki szyfrujące), a następnie żąda od ofiary okupu za przywrócenie stanu pierwotnego.

IDS / PC Cyborg

Pierwsze przypadki ataków z użyciem oprogramowania szyfrującego miały miejsce już w 1989 r. ransomware AIDS / PC Cyborg brał na cel przede wszystkim komputery firm z sektora medycznego. Przenoszony na dyskietkach 5,25 cala podszywał się pod ankietę dotyczącą ryzyka zarażenia się wirusem HIV. Wiadomość o okupie była drukowana na podłączonej do komputera drukarce.[1]

Gpcode, CryptoLocker

Już w 2006 r. pojawiła się cała gama trojanów stosujących szyfrowanie RSA (np. Gpcode, Crypzip, MayArchive) a nastepnie CryptoLocker. Cel ataku otrzymywał wiadomość e-mail z ukrytym jako dokument plikiem wykonywalnym. Po jego uruchomieniu CryptoLocker szyfrował pliki o wybranych rozszerzeniach zarówno na dysku lokalnym, jak i dostępnych zasobach sieciowych.

Petya

Zastosowano w nim odmienną metodę blokowania dostępu do danych ofiary. Celem ataku jest zaszyfrowanie nie tylko plików użytkownika, ale również plik MFT (master file table), co w konsekwencji uniemożliwia odczytanie struktury katalogów lub uruchomienie systemu Windows. Ransomware przesyłano jako złośliwy załącznik udający CV kandydata lub link do niego.

WannaCry

WannaCry to program ransomware, wykorzystujący exploit o nazwie EternalBlue, który niektórych źródeł został zaprojektowany w amerykańskiej agencji bezpieczeństwa narodowego w celu atakowania komputerów z systemem Windows. Struktura kodu WannaCry przypomina te z wcześniejszych ataków północnokoreańskiej grupy Lazarus.

Opracowano na podstawie: Ł. Dudkowski / Seqred, Ransomware – co to jest i jak go usunąć? Jak się zabezpieczyć?, https://seqred.pl/ransomware-co-to-jest-jak-sie-zabezpieczyc-jak-usunac/ (pobrano 27.07.2020)

Ransomware

Media społecznościowe

Sieć Darknet

RANSOMWARE

Ransomware w załączonych do maili dokumentach związanych z COVID-19

Do tej kategorii należą złośliwe narzędzia

NetWalker

Ransomware-GVZ

CoViper

Źródło: Cyberzagrożenia pracy zdalnej 2020: od botnetów do phishingu: https://alebank.pl/cyberzagrozenia-pracy-zdalnej-2020-od-botnetow-do-phishingu

Wybrane cyberzagrożenia - **Advanced Persistent Threats**

Ataki typu APT (ang. Advanced Persistent Threat)
to najnowsze typy ataków dedykowanych, uwzględniające specyfikę danej instytucji, wykorzystujące często inne metody: malware, phishing, itp

Charakteryzują je trzy cechy (definicja podana za CERT Polska):

- **atakujący opanował zaawansowane metody ataku na komputery i sieci komputerowe**
- **posiada umiejętność tworzenia własnego kodu w oprogramowaniu wykorzystującego luki w zabezpieczeniu**
- **atakujący ma jasno określone i sprecyzowane cele – wykonuje z góry ustalone rozkazy i zadania**
- **atakujący jest zorganizowany, zmotywowany i posiada odpowiednie środki finansowe**

Opracowano na podstawie: Bezpieczeństwo bankowości elektronicznej. II Raport specjalny (maj 2015), Obserwatorium BIZ, s. 14.

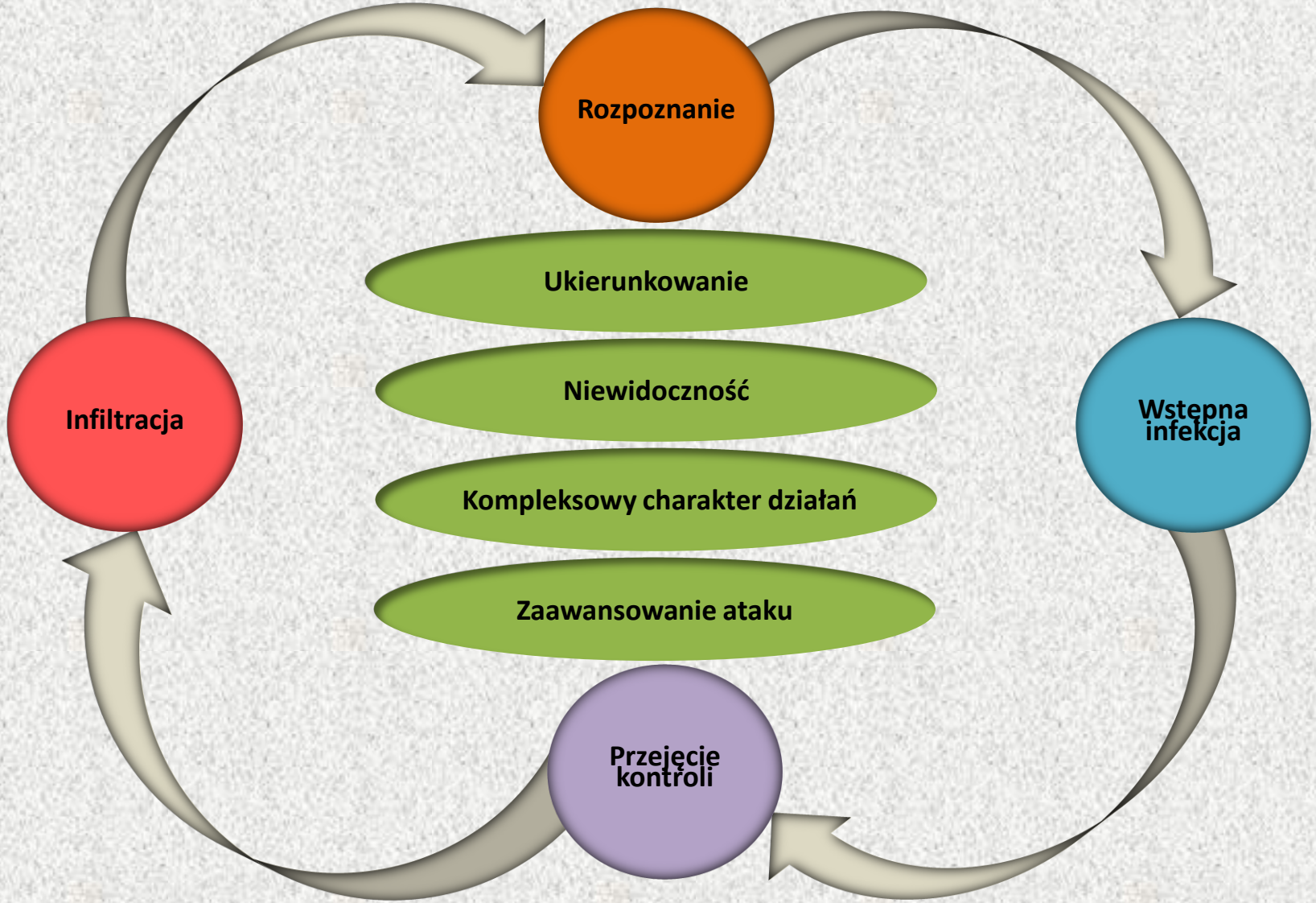
Idea ATP (Advanced Persistent Threats)

APT „jest formą wielostopniowego ataku prowadzonego w większym ukryciu, wymierzonego w szczególności dla osiągnięcia sprecyzowanego celu, najczęściej cyberszpiegostwa”.[1]

Zaawansowanie (Advanced)	**Zaawansowanie APT wynika z zastosowania wyrafinowanych narzędzi i jest obliczone na przeprowadzenie akcji sabotażowych, kradzież zastrzeżonych informacji, wyłudzenia czy szantaże. Hakerzy stojący za APT są nie tylko doskonale wykształceni, ale i korzystają z szerokiej gamy narzędzi.**[1]
Długotrwałość (Persistent)	**Ataki nie są prowadzone incydentalnie, lecz wynikają z wytycznych służących realizacji większego przedsięwzięcia, co niekoniecznie oznacza to nieustannego wykonywania złośliwego kodu na komputerach ofiary. Stąd atakujący utrzymują pewien poziom interakcji wymagany do osiągnięcia ich celów.**
Zagrożenie (Threat)	**Zagrożenie jest związane przede wszystkim z czynnikiem ludzkim i dotyczy grup działających na wysokim poziomie zorganizowania i nie wynika tu z samej dostępności narzędzia w postaci chociażby malware, ale z kompleksowego podejścia stosujących je podmiotów.**

[1] A. Rot, B. Olszewski, Zaawansowane ataki typu APT jako nowa forma zagrożeń dla cyberbezpieczeństwa, Informatyka Ekonomiczna Business Informatics 2(40), 2016, s. 85-87.

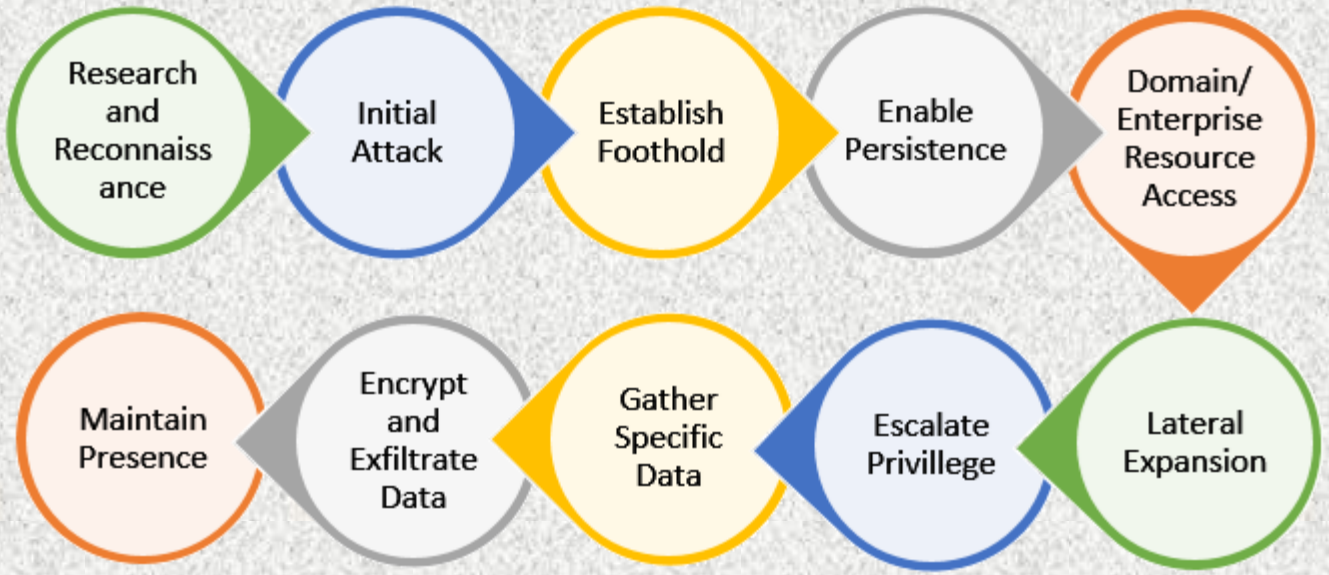
Główne etapy cyklu ATP (Advanced Persistent Threats)



[1] A. Rot, B. Olszewski, Zaawansowane ataki typu APT jako nowa forma zagrożeń dla cyberbezpieczeństwa, Informatyka Ekonomiczna Business Informatics 2(40), 2016, s. 85-87.

Cykl życia ataku APT

**Cykl życia ataków APT jest nieco podobny do konwencjonalnych ataków.
Składa się ze wszystkich etapów, w tym wstępnego rozpoznania, wstępnego kompromisu, ustanowienia „przyczółka”, eskalacji przywilejów, ekspansji bocznej, utrzymania obecności i zakończenia misji.**



[1] R. Thomas, A little about Advanced Persistent Threats
https://secvibe.com/a-little-about-advanced-persistent-threats-4b7d40cab49 (dostęp 02.02.2022)

Identyfikacja etapów APT

Rozpoznanie umożliwia	wskazanie (dokonanie wyboru) potencjalnych wektorów ataku.
	określenie podatności i katalogu osób w obrębie organizacji, mogących w sposób aktywny lub bierny umożliwić ominięcie zabezpieczeń sieciowych.
	identyfikacji zabezpieczeń fizycznych i informatycznych organizacji, np.: rodzaj stosowanych systemów operacyjnych, architektura sieci, udostępnione numery IP.
Wstępne zainfekowanie jest następstwem	uzyskania dostępu do jednego z elementów składowych sieci informatycznej wybranej osoby, posiadającej uprawnienia wysokiego poziomu.
	okoliczności nieautoryzowanego wykorzystywania prywatnych urządzeń w miejscu pracy oraz włączanie ich w sieć korporacyjną i internetową.
	wprowadzenia malware w postaci konia trojańskiego lub aplikacji umożliwiającej prowadzenie zdalnych czynności administracyjnych.
Przejęcie kontroli	nad pożądanymi funkcjonalnościami systemu i jego użytkownikami w celu ostatecznego uzyskania dostępu do danych stanowiących główny cel operacji.
	nad integralną częścią aktualnie penetrowanych zasobów sieciowych lub personalnie konkretnego użytkownika, informacji leżących wyłącznie w jego gestii.
	w postaci uzyskania danych, służących skompromitowaniu konkretnej osoby lub gdy mają one stanowić punkt wyjścia do przeprowadzenia właściwego APT.
Infiltracja	działania służące poszerzeniu dostępu i przyznaniu dodatkowych przywilejów w systemie, co skutkuje dalszym umocowaniem i „rozmyciem" obecności intruza.
	rozpoczyna się pozyskiwanie/niszczenie właściwych danych stanowiących obiekt zainteresowania jego samego lub zlecającej strony trzeciej.
	po jego zakończeniu następuje wycofanie z systemu i zatarcie nie tylko śladów działań, ale i wszelkich danych umożliwiających określenie źródła pochodzenia ataku.

A. Rot, B. Olszewski, Zaawansowane ataki typu APT , …, s. 88.

Ogólna struktura ATP (Advanced Persistent Threats)

Wymienione elementy stanowią kluczowe elementy całego procesu[1]

A. Rot, B. Olszewski, Zaawansowane ataki typu APT , …, s. 89.

Wykorzystanie podatności w atakach APT

Socjotechnika i ogólnodostępne zasoby informacji na temat konkretnego pracownika

- **Blogi**
- **Media społecznościowe**
- **Media branżowe**
- **Strony firmowe**

pozwalają wytypować osoby posiadające dostęp do:

- **Danych wrażliwych**
- **Danych osobowych**
- **Loginów**
- **Haseł**

umożliwia penetrację zasobów sieciowych organizacji lub mogące służyć swoją wiedzą na drodze do uzyskania kolejnych informacji, stanowiących ostateczny obiekt zainteresowania lub punkt wyjścia dla następnego etapu APT[1]

Poprzez profil psychologiczny i zawodowy danego pracownika, dokonuje się oceny jego potencjalnych słabości możliwych do wykorzystania, także w ramach szantażu czy bezpośredniej oferty związanej z gratyfikacją finansową w zamian za udostępnienie posiadanych zdolności i środków wynikających z funkcji pełnionych w organizacji[1]

[1] A. Rot, B. Olszewski, Zaawansowane ataki typu APT jako nowa forma zagrożeń dla cyberbezpieczeństwa, Informatyka Ekonomiczna Business Informatics 2(40), 2016, s. 90.

Dziękuję za uwagę

dr hab. inż. Andrzej Gałecki, prof. WSB

MODUŁ BEZPIECZEŃSTWA
Rozdział 7. Charakterystyka przestępczości