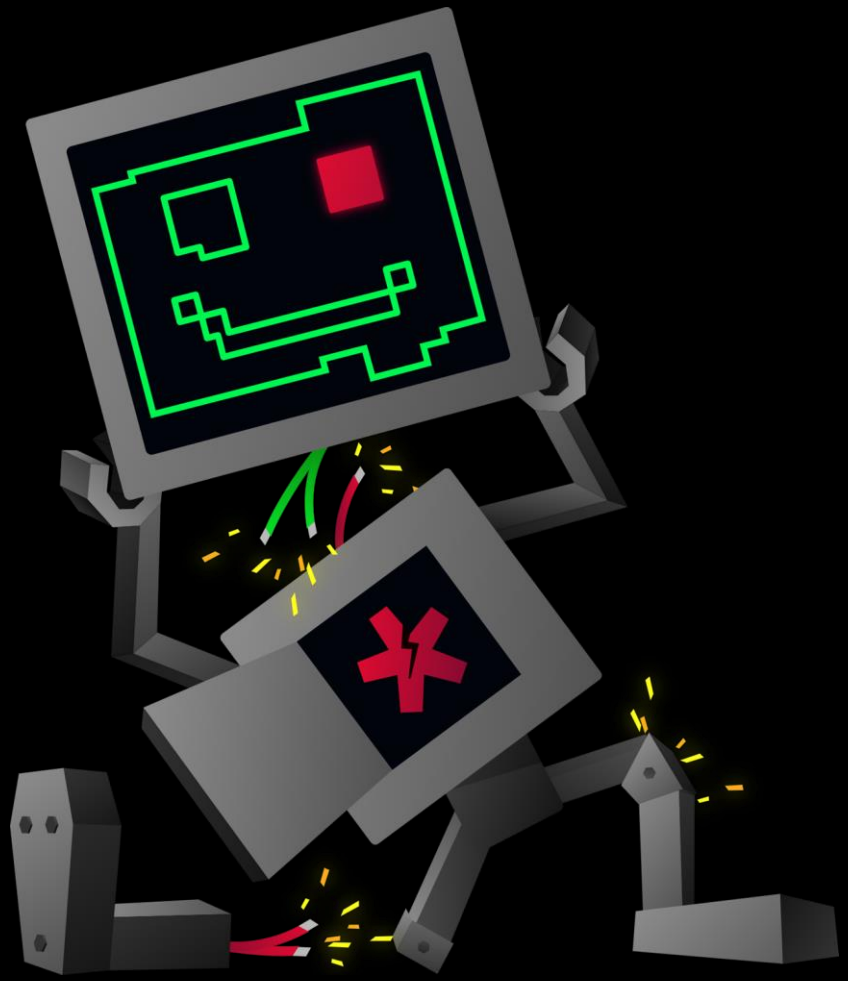
THE H@CK SUMMIT



C:\>

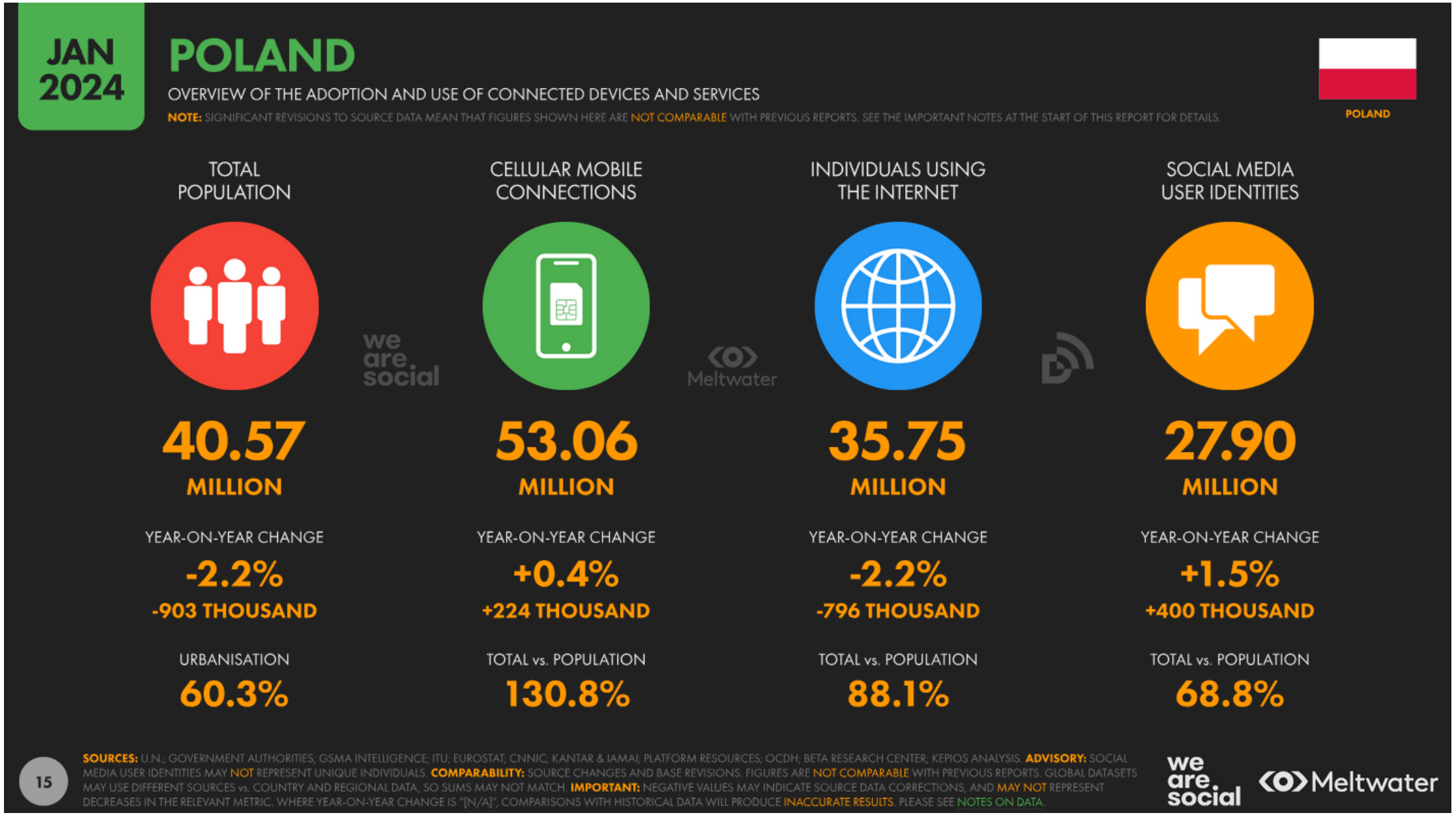
# Rzeczywistość prawna polskiej cyberprzestępczości

**płk dr inż. Michał Malinowski**
**Szef Oddziału, DKWOC**

thehacksummit.com 17-18 października 2024 PGE Narodowy + Online

ORGANIZATORZY:

ACADEMIC PARTNERS





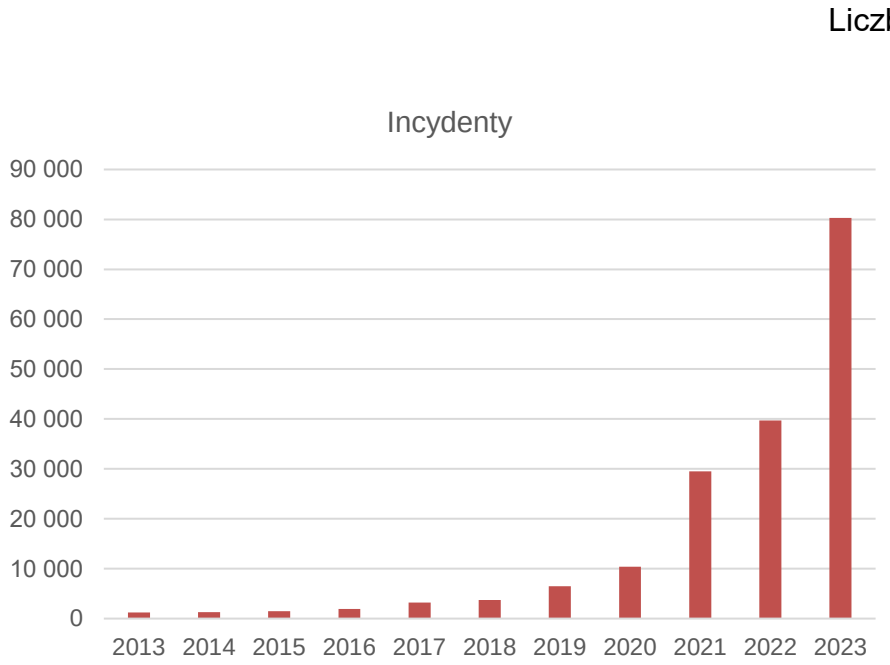

*Digital 2024 Poland*
https://indd.adobe.com/view/2a9fa0ac-970a-47ef-b308-be5fcf3bc93d?allowFullscreen=true&wmode=opaque

# Cel prezentacji

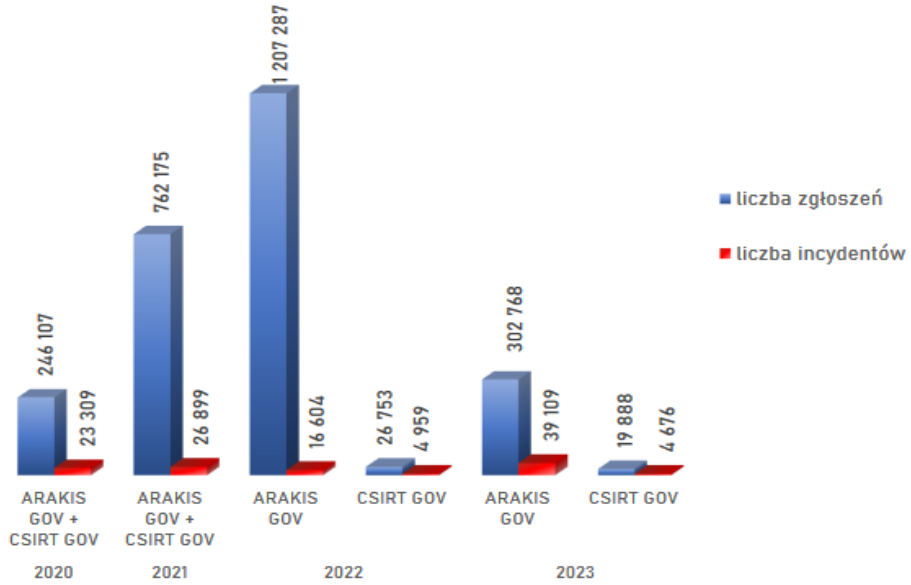
**Określenie pojęcia cyberprzestępczości.**

**Przegląd przepisów polskiego prawa dotyczących cyberbezpieczeństwa.**

# Incydenty bezpieczeństwa




Liczba incydentów bezpieczeństwa




*Raport roczny z działalności CERT POLSKA (CSIRT NASK)*
https://cert.pl/uploads/docs/Raport_CP_2023.pdf

Liczba incydentów: **80 267** (2023)

*Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 (CSIRT GOV)*
https://csirt.gov.pl/download/3/220/RaportostaniebezpieczenstwacyberprzestrzeniRPw2023.pdf

Liczba incydentów: **43 785** (2023)

~1 incydent na 282 użytkowników w roku

# Incydenty bezpieczeństwa

Typy incydentów obsłużonych przez CERT Polska w 2023 r.

| Typy incydentów | Liczba incydentów | Procent wszystkich |
|---|---|---|
| Oszustwa komputerowe | 75 917 | 94,58% |
| Szkodliwe oprogramowanie | 1 650 | 2,06% |
| Podatne usługi | 964 | 1,20% |
| Obraźliwe i nielegalne treści | 584 | 0,73% |
| Włamania | 418 | 0,52% |
| Dostępność zasobów | 385 | 0,48% |
| Próby włamań | 205 | 0,26% |
| Atak na bezpieczeństwo informacji | 59 | 0,07% |
| Inne | 56 | 0,07% |
| Gromadzenie informacji | 29 | 0,04% |
| Razem | 80 267 | 100,00% |

Incydenty obsłużone przez CERT Polska w 2023 r.
w podziale na sektor gospodarki (>1%)

| Sektor gospodarki | Liczba incydentów | Procent wszystkich |
|---|---|---|
| Handel hurtowy i detaliczny | 19 253 | 23,99% |
| Infrastruktura rynków finansowych | 18 943 | 23,61% |
| Media | 10 191 | 12,70% |
| Energetyka | 9 196 | 11,46% |
| Poczta i usługi kurierskie | 5 319 | 6,63% |
| Infrastruktura cyfrowa | 5 101 | 6,35% |
| Bankowość | 2 481 | 3,09% |
| Produkcja | 2 353 | 2,93% |
| Administracja publiczna | 2 234 | 2,78% |
| Osoby fizyczne | 2 105 | 2,62% |
| Usługi inne | 902 | 1,12% |
| ..... | | |
| Razem | 80 278 | 100,00% |

*Raport roczny z działalności CERT POLSKA* (CSIRT NASK)
https://cert.pl/uploads/docs/Raport_CP_2023.pdf

# Cyberprzestępstwo

Badanie dotyczące stosowania definicji cyberprzestępstwa przeprowadzone w czerwcu i lipcu 2024r

Treść pytania:

*Zwracam się do Państwa w trybie zapytania do BIP.*
*Czy w ramach swoich działań (nazwa instytucji) wykorzystuje definicję Cyberprzestępstwa.*

*Jeśli tak to jaką?*

Pytanie zostało wysłane do:

- Centralne Biuro Zwalczania Cyberprzestępczości
- CSIRT NASK
- CSIRT GOV
- CSIRT MON

# Cyberprzestępstwo

Odpowiadając na wiadomość elektroniczną (…) w sprawie definicji cyberprzestępstwa wykorzystywanej przez Policję informuję, że pojęcie cyberprzestępstwa nie zostało dotychczas zdefiniowane w polskim prawodawstwie.

Funkcjonuje natomiast wiele tworzonych doraźnie, w zależności od potrzeb, definicji opierających się na najprostszym założeniu, iż cyberprzestępczość stanowią przestępstwa popełniane za pomocą komputerów oraz Internetu.

Ponadto niektóre podmioty międzynarodowe, jak np. ONZ, Unia Europejska czy Interpol, opracowały definicję cyberprzestępczości na własne potrzeby.


*Odpowiedź z dnia 11 czerwca 2024r.*
*Centralne Biuro Zwalczania Cyberprzestępczości*

# Cyberprzestępstwo

W ramach swoich działań CSIRT NASK stosuje się do powszechnie obowiązujących przepisów prawa, tj. ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa i rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie)

*Odpowiedź z dnia 8 lipca 2024r.*
*CSIRT NASK / CERT Polska*

# Cyberprzestępstwo

CSIRT GOV, w ramach swoich działań, wykorzystuje definicje zawarte w ustawie z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* (Dz. z 2023 r. poz. 913, z późn. zm.), która stanowi podstawę działania Zespołu.

Należy wskazać, iż przedmiotowy akt prawny nie zawiera definicji cyberprzestępstwa, wobec czego CSIRT GOV nie wykorzystuje konkretnej, legalnej definicji wskazanego terminu.

Zgodnie natomiast z art. 40 ust. 2 ww. ustawy, CSIRT GOV przekazuje organom ścigania informacje stanowiące tajemnice prawnie chronione, w tym tajemnice przedsiębiorstwa, w związku z incydentem wyczerpującym znamiona przestępstwa.

*Odpowiedź z dnia 17 lipca 2024r.*
*CSIRT GOV / ABW*

# Cyberprzestępstwo

Zgodnie z wewnętrznymi regulacjami w MON, DKWOC obsługuje CISIRT MON. Obsługa ta dotyczy technicznych aspektów wykrywania, oceny faktycznej i likwidacji incydentów komputerowych, a nie ich oceny i kwalifikacji prawnej.

Poza tym, użyte w aktach prawnych terminy nie są informacją publiczną, która powinna być definiowana przez podmioty publiczne (w tym przypadku MON).

CSIRT MON nie zajmuje się cyberprzestępczością w szerokim i wąskim tego słowa znaczeniu.

Incydenty na które reaguje CSIRT MON są analizowane i przekazywane do Żandarmerii Wojskowej lub Prokuratury, które poprzez wyspecjalizowane komórki dokonują dalszych czynności i klasyfikacji prawnych poszczególnych incydentów.

*Odpowiedź z dnia 24 lipca 2024r.*
*CSIRT MON / DKWOC*

# Cyberprzestępstwo

## Podsumowanie

*Polskie prawodawstwo do dzisiaj nie stworzyło jednolitej definicji cyberprzestępczości.*

*Pojęcie przestępczości komputerowej nie jest jednoznacznie zdefiniowane nawet na gruncie Kodeksu karnego. Funkcjonuje natomiast wiele tworzonych doraźnie, w zależności od potrzeb, definicji opierających się na najprostszym założeniu, iż ogólnie są to przestępstwa popełniane za pomocą komputerów oraz Internetu.*

*Cyberprzestępczość – próba diagnozy zjawiska* , Kwartalnik Policyjny
https://kwartalnik.csp.edu.pl/kp/archiwum-1/2017/nr-42017/3730,Cyberprzestepczosc-proba-diagnozy-zjawiska.html

CSIRT GOV oraz CSIRT MON przekazują do organów ścigania
(Policja, Prokuratura lub Żandarma Wojskowa)
incydenty wyczerpującym znamiona przestępstwa

# Międzynarodowe określenia CyberCrime

| Źródło | Określenie cyberprzestępczości | Adres URL |
|---|---|---|
| **Konwencja Rady Europy o cyberprzestępczości (Konwencja Budapeszteńska)** | Konwencja określa cyberprzestępstwa jako działania przestępcze skierowane przeciwko poufności, integralności i dostępności systemów komputerowych, sieci oraz danych, a także nadużycia związane z takimi systemami, sieciami i danymi. | https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185; |
| **Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE** | Dyrektywa określa cyberprzestępczość jako nielegalne działania wymierzone w systemy informatyczne, w tym nieuprawniony dostęp, ingerencję w systemy i dane oraz zakłócanie funkcjonowania systemów. | https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32013L0040 |
| **Organizacja Narodów Zjednoczonych (ONZ) UNODC** | UNODC określa cyberprzestępczość jako przestępstwa, w których komputer jest narzędziem, celem lub miejscem przestępstwa, obejmujące szeroki zakres działań od oszustw internetowych po ataki na infrastrukturę krytyczną. | https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf |
| **Europol** | Europol określa cyberprzestępczość jako przestępstwa, które są popełniane przy użyciu technologii informatycznych lub są wymierzone w takie technologie, w tym ataki hakerskie, dystrybucję złośliwego oprogramowania i przestępstwa związane z ciemną stroną internetu (Darknet). | https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime |
| **Interpol** | Interpol określa cyberprzestępczość jako przestępstwa obejmujące ataki na systemy komputerowe, oszustwa internetowe, kradzież tożsamości oraz inne nielegalne działania prowadzone w cyberprzestrzeni. | https://www.interpol.int/Crimes/Cybercrime |

# Międzynarodowe określenia CyberCrime

## Wspólne cechy

### Nielegalne działanie
- wszystkie definicje wskazują na przestępcze wykorzystanie technologii.

### Działania przeciwko poufności, integralności i dostępności
- te kluczowe aspekty cyberbezpieczeństwa.

### Nieuprawniony dostęp do systemów i danych
- uzyskiwanie dostępu do systemów informatycznych bez zgody.

### Ingerencja w systemy i dane
- manipulacja lub uszkodzenie danych i funkcji systemów.

### Oszustwo informatyczne
- działania mające na celu wprowadzenie w błąd lub wyłudzenie korzyści majątkowych.

### Atak na infrastrukturę krytyczną
- działania celujące w kluczowe dla funkcjonowania państwa lub organizacji systemy.

### Działanie związane z „ciemną stroną” Internetu
- wykorzystanie anonimowości Internetu do prowadzenia nielegalnych aktywności.

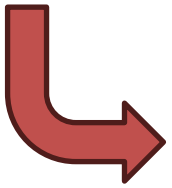
# Próba definicji

**Cyberprzestępczość** to każde działanie przestępcze wykonane z wykorzystaniem technologii informatycznych, które jest skierowane przeciwko poufności, integralności i dostępności systemów komputerowych, sieci lub danych.

Obejmuje szeroki zakres działań, w tym nieuprawniony dostęp, manipulacje systemami i danymi, zakłócanie funkcjonowania systemów, ataki na infrastrukturę krytyczną, dystrybucję złośliwego oprogramowania oraz działania związane z ciemną stroną internetu (Darknet).

Cyberprzestępczość rozumiana jest jako globalne zjawisko, gdzie komputer może być narzędziem, celem lub miejscem przestępstwa.

Dodatkowo, obejmuje wykorzystanie sztucznej inteligencji do tworzenia i propagowania oszustw, manipulowanie algorytmami, oraz inne działania mające na celu wykorzystanie lub zakłócenie systemów AI w sposób niezgodny z prawem.



**Wersja skrócona**

**Cyberprzestępczość** – działania przestępcze realizowane z użyciem systemów informatycznych, które naruszają poufność, integralność lub dostępność danych i systemów komputerowych, obejmujące nieuprawniony dostęp, manipulacje danymi, zakłócenia funkcjonalności systemów, ataki na infrastrukturę krytyczną, dystrybucję złośliwego oprogramowania, jak również oszustwa, manipulację algorytmami oraz szkodliwe wykorzystanie sztucznej inteligencji.

# Dlaczego warto formalnie zdefiniować

**Jasność przepisów prawnych**
ułatwi jednoznaczną interpretację przepisów, co zwiększy skuteczność egzekwowania prawa.

**Skuteczniejszą walka z cyberprzestępczością**
pomoże lepiej zorganizować działania organów ścigania oraz instytucji zajmujących się cyberbezpieczeństwem.

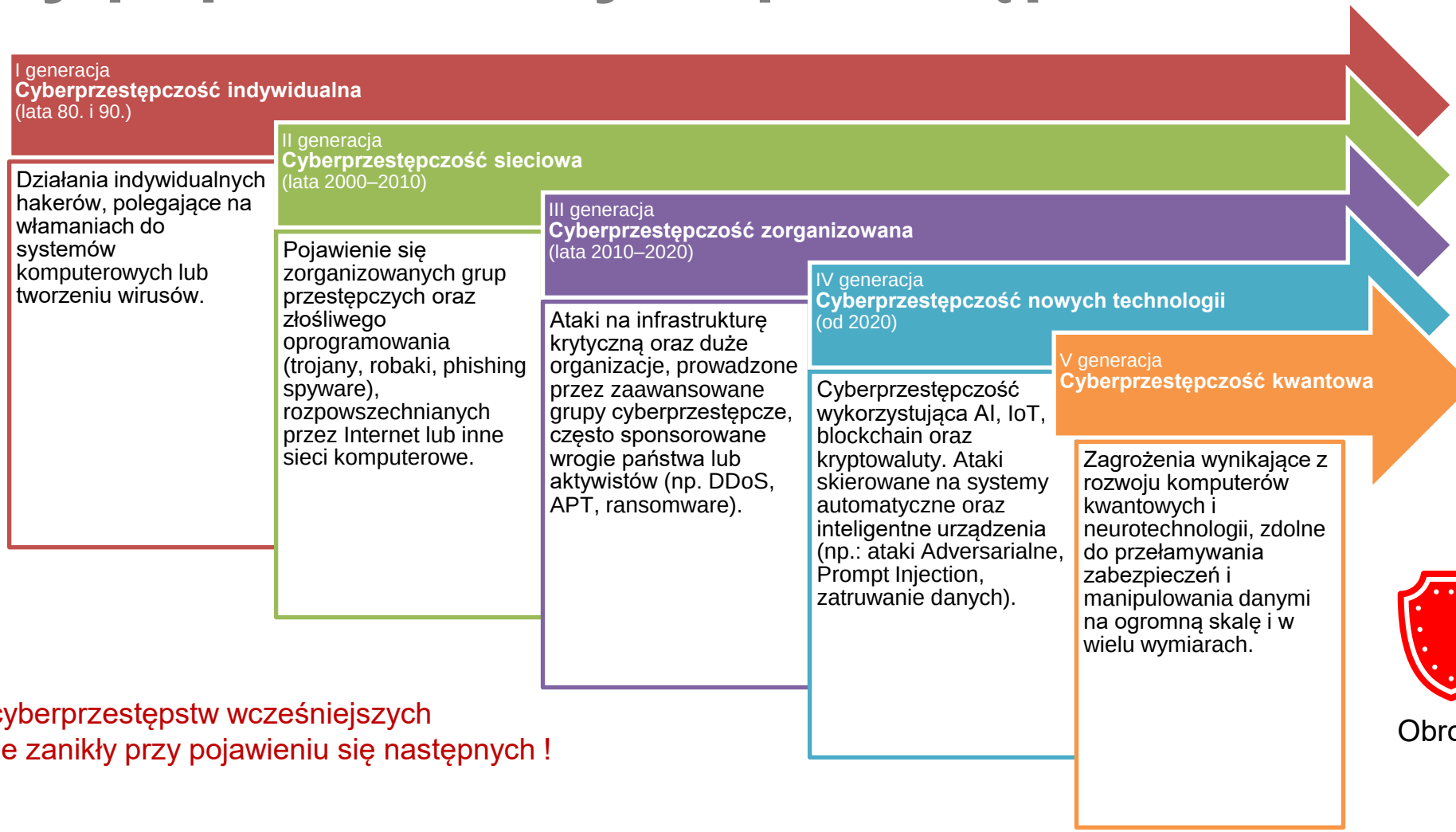
**Adaptację do nowych technologii**
pozwoli prawu nadążyć za dynamicznie zmieniającymi się zagrożeniami technologicznymi, takimi jak AI czy kryptowaluty.

**Spójność z międzynarodowymi aktami prawa**
ułatwi współpracę międzynarodową w ściganiu cyberprzestępców działających globalnie.

**Zwiększenie świadomości społecznej**
pomoże lepiej uświadomić obywatelom, jakie działania są klasyfikowane jako cyberprzestępstwa, co zwiększy prewencję.

**Wykorzystanie odmiennych od klasycznych metod śledczych**
wymaga odmiennych narzędzi i metod dochodzeniowych, takich jak analiza cyfrowych śladów czy monitorowanie sieci.

# Formy popełniania cyberprzestępstw




**Kto pierwszy?**

Obrońca Atakujący

Przypadki cyberprzestępstw wcześniejszych generacji nie zanikły przy pojawieniu się następnych !

# To jak sobie poradzić …. ?

# Kodeks Karny

W *Kodeksie Karnym* są zawarte przestępstwa które można utożsamiać z pojęciem cyberprzestępczości, między innymi:

**Przestępstwa ściśle komputerowe**

Działania bezpośrednio skierowane na systemy komputerowe, zgodne z przepisami rozdziału XXXIII Kodeksu Karnego.

**Przestępstwa związane z treściami**

Rozpowszechnianie nielegalnych treści, takich jak pornografia dziecięca (art. 202 KK) oraz propagowanie nienawiści (art. 256 KK).

**Przestępstwa związane ze sprowadzeniem zagrożenia powszechnego**

Zakłócanie funkcjonowania systemów teleinformatycznych (art. 165 KK).

**Przestępstwa związane z nękaniem (cyberstalkingiem) i kradzieżą tożsamości**

Uporczywe nękanie innych osób lub kradzież tożsamości (art. 190a KK).

*Dz.U.2024.0.17 t.j. - Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny*
https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19970880553

# Rozdział XXXIII KK
## Przestępstwa przeciwko ochronie informacji

### Ujawnienie i wykorzystanie informacji niejawnych

- **Art. 265 KK:** Ujawnienie lub wykorzystanie informacji niejawnych, zwłaszcza „tajnych” lub „ściśle tajnych”.
- **Art. 266 KK:** Ujawnienie informacji uzyskanej w związku z pełnioną funkcją, pracą lub działalnością publiczną, społeczną czy naukową.

Artykuły te dotyczą naruszeń związanych z informacjami niejawnymi, szczególnie tych, które mogą stanowić zagrożenie dla bezpieczeństwa państwa lub interesów instytucji publicznych.

*Pracownik instytucji państwowej udostępnia tajne informacje dotyczące bezpieczeństwa narodowego zewnętrznym podmiotom.*

*Funkcjonariusz publiczny przekazuje dane zastrzeżone dotyczące negocjacji handlowych firmie konkurencyjnej.*

# Rozdział XXXIII KK
## Przestępstwa przeciwko ochronie informacji

### Bezprawne uzyskiwanie dostępu do informacji

- **Art. 267 KK:** Bezprawne uzyskanie dostępu do informacji poprzez przełamanie zabezpieczeń, podsłuchy, podłączenie do sieci telekomunikacyjnej.
- **Art. 269b KK:** Wytwarzanie, pozyskiwanie, zbywanie lub udostępnianie narzędzi przeznaczonych do popełniania przestępstw informatycznych.

Artykuły te obejmują działania związane z uzyskaniem nieuprawnionego dostępu do informacji, jak również udostępnianie narzędzi umożliwiających popełnianie cyberprzestępstw.

*Atak hakerski na system bankowy w celu pozyskania danych klientów, które następnie są wykorzystane w oszustwach finansowych.*

*Osoba udostępnia programy do łamania haseł na forach internetowych, które są wykorzystywane przez cyberprzestępców do włamań do systemów.*

# Rozdział XXXIII KK
## Przestępstwa przeciwko ochronie informacji

### Niszczenie, uszkadzanie i zmienianie danych informatycznych

- **Art. 268 KK:** Utrudnianie dostępu do informacji poprzez niszczenie, uszkadzanie lub zmienianie jej zapisu.
- **Art. 268a KK:** Niszczenie, usuwanie lub zmienianie danych informatycznych, co powoduje zakłócenia w systemach przetwarzania danych.
- **Art. 269 KK:** Niszczenie, usuwanie lub zmienianie danych informatycznych o szczególnym znaczeniu dla obronności kraju lub funkcjonowania administracji publicznej.

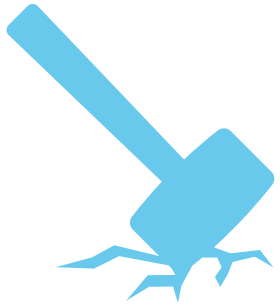
Artykuły te koncentrują się na przestępstwach związanych z niszczeniem lub modyfikowaniem danych informatycznych, które mogą zakłócać funkcjonowanie ważnych systemów.

*Haker usuwa kluczowe pliki z serwera przedsiębiorstwa, uniemożliwiając ich odtworzenie i powodując chaos operacyjny.*

*Cyberprzestępcy przeprowadzają atak ransomware, blokując dostęp do danych firmowych i żądając okupu za ich odblokowanie.*

*Cyberatak na infrastrukturę energetyczną kraju, prowadzący do zakłócenia dostaw prądu na dużym obszarze.*

# Rozdział XXXIII KK
## Przestępstwa przeciwko ochronie informacji



### Zakłócanie pracy systemów teleinformatycznych

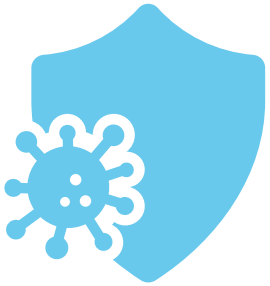
- **Art. 269a KK:** Zakłócanie pracy systemów informatycznych lub teleinformatycznych poprzez usunięcie, zniszczenie, uszkodzenie danych lub utrudnienie dostępu do nich..

Ten artykuł dotyczy przestępstw związanych z celowym zakłócaniem pracy systemów teleinformatycznych, co może prowadzić do znacznych zakłóceń w dostępie do usług lub danych.

*Atak DDoS na serwery banków, który blokuje dostęp klientów do ich kont i powoduje utratę reputacji banku.*

*Atak hakerski na dostawcę internetu powoduje przerwę w dostępie do sieci, uniemożliwiając korzystanie z bankowości online i pracy zdalnej.*

# Rozdział XXXIII KK
## Przestępstwa przeciwko ochronie informacji



### Działania w celu wykrycia błędów w systemach informatycznych

- **Art. 269c KK:** Wyjątek dla osób, które uzyskują dostęp do systemów w celu wykrycia luk w zabezpieczeniach i niezwłocznie informują o nich dysponenta systemu.

Ten artykuł stanowi wyjątek od odpowiedzialności karnej dla osób działających w dobrej wierze, w celu poprawy zabezpieczeń systemów informatycznych.

*Badacz bezpieczeństwa odkrywa lukę w zabezpieczeniach systemu bankowego i informuje o tym bank, zamiast wykorzystać ją do popełnienia przestępstwa.*

*Programista odkrywa lukę w Serwisie WWW Jednostki Wojskowej i niezwłocznie informuje o niej odpowiednie służby, zamiast wykorzystać ją do modyfikacji strony*

# Przepisy dziedzinowe

Przepisy i regulacje dziedzinowe zawierają w sobie aspekty związane z działaniami utożsamianymi z cyberprzestępczością:

**Prawa autorskie:**

Chroni przed piractwem internetowym, nielegalnym udostępnianiem materiałów i oprogramowania.

**Ochrona danych osobowych:**

Zapewnia ochronę przed wyciekami danych, nielegalnym przetwarzaniem i phishingiem.

**Usługi elektroniczne:**

Reguluje zabezpieczenia transakcji e-commerce i ochronę danych użytkowników.

**Płatności elektroniczne:**

Przeciwdziała oszustwom w płatnościach online i zapewnia ochronę środków finansowych.

**Prawo telekomunikacyjne:**

Chroni sieci przed atakami i zapewnia poufność komunikacji.

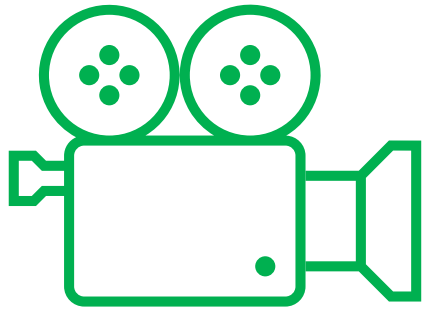
# Prawa autorskie

*Nieautoryzowane streamowanie filmów na platformie internetowej bez odpowiedniej licencji.*

*Instalacja oprogramowania biurowego na wielu komputerach przy posiadaniu licencji tylko na jedno urządzenie.*

## Ustawa z dnia 4 lutego 1994 r.
## o prawie autorskim i prawach pokrewnych (art. 115-123)

- Naruszenie praw autorskich w usługach streamingowych: nieautoryzowane emitowanie treści chronionych przez prawo autorskie.
- Piractwo internetowe: udostępnianie i pobieranie treści chronionych prawem autorskim z sieci bez odpowiedniej licencji.
- Nielegalne rozpowszechnianie oprogramowania: dystrybucja kopii programów komputerowych bez zgody posiadacza praw autorskich.
- Reverse engineering: dekompilacja oprogramowania w celach niezgodnych z licencją.



*Dz.U. 1994 nr 24 poz. 83*
https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19940240083

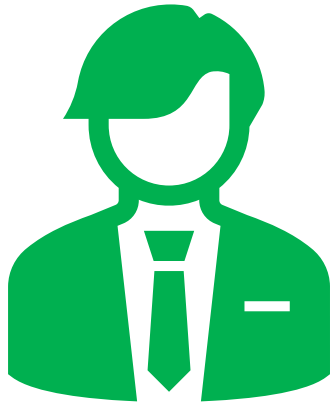
# Ochrona danych osobowych

*Niezabezpieczenie danych klientów przez firmę, co prowadzi do wycieku danych osobowych, takich jak adresy e-mail i numery telefonów.*

*Utworzenie i wykorzystanie fałszywych stron internetowych do phishingu, mających na celu wyłudzenie danych osobowych.*

## Ustawa z dnia 10 maja 2018 r.
## o ochronie danych osobowych (art. 101-108)

- Wyciek danych osobowych: niezabezpieczenie danych klientów przed cyberatakami skutkujące ich ujawnieniem.
- Naruszenie zasad RODO: brak zgody na przetwarzanie danych lub nieprzestrzeganie praw osób, których dane dotyczą.
- Ataki phishingowe na dane osobowe: wyłudzanie informacji osobistych, takich jak numery PESEL przez fałszywe strony internetowe.
- Nielegalne profilowanie: wykorzystywanie danych osobowych do tworzenia profili użytkowników bez ich wiedzy i zgody.



*Dz.U. 2018 poz. 1000*
https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001000

# Usługi elektroniczne

*Włamanie do platformy e-commerce i kradzież danych kart kredytowych użytkowników.*

*Wysyłanie niezamówionej korespondencji reklamowej do użytkowników bez ich zgody.*

## Ustawa z dnia 18 lipca 2002 r.
## o świadczeniu usług drogą elektroniczną (art. 23-25)

- Niezabezpieczona transakcja e-commerce: brak odpowiednich środków ochrony danych w procesie sprzedaży online.
- Nieprzestrzeganie zasad informacyjnych: brak jasnych informacji o przetwarzaniu danych klientów w serwisach e-commerce.
- Ataki na systemy e-commerce: włamania do platform sprzedażowych i kradzież danych kart kredytowych użytkowników.
- Spam i niechciane komunikaty: wysyłanie niezamówionej korespondencji w celach marketingowych bez zgody odbiorcy.

*Dz.U. 2002 nr 144 poz. 1204*
https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20021441204

# Płatności elektroniczne

Wykorzystanie podrobionych danych identyfikacyjnych w procesie autentykacji płatności online.

*Oszustwo finansowe polegające na manipulowaniu transakcjami elektronicznymi w celu nieautoryzowanego przekierowania środków z konta klienta.*

## Ustawa z dnia 19 sierpnia 2011 r.
## o usługach płatniczych (art. 150-153d)

- Przeciwdziałanie oszustwom: obowiązek monitorowania transakcji w celu zapobiegania nadużyciom finansowym.
- Autentykacja płatności: mechanizmy weryfikacji tożsamości klienta przy transakcjach elektronicznych.
- Ochrona środków finansowych: regulacje dotyczące ochrony środków na rachunkach klientów w przypadku naruszenia bezpieczeństwa.
- Zgłaszanie incydentów: procedury raportowania podejrzanych działań do właściwych organów nadzorczych.

*Dz.U. 2011 nr 199 poz. 1175*
https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20111991175

# Prawo telekomunikacyjne

*Przeprowadzenie ataku DDoS na serwery telekomunikacyjne, co prowadzi do zakłóceń w dostępie do sieci oraz usług komunikacyjnych.*

*Podsłuchiwanie rozmów telefonicznych bez zgody użytkowników i odpowiednich organów.*

## Ustawa z dnia 16 lipca 2004 r.
## Prawo telekomunikacyjne (art. 208-210)

- Bezpieczeństwo sieci telekomunikacyjnych: ochrona przed nieautoryzowanym dostępem i atakami typu DDoS na infrastrukturę krytyczną.
- Tajność komunikowania: zasady ochrony przekazywanych informacji, obowiązek zachowania poufności przez operatorów.
- Zarządzanie incydentami: procedury reagowania na naruszenia bezpieczeństwa i wycieki danych w sektorze telekomunikacyjnym.
- Wymogi dot. sprzętu i oprogramowania: przepisy regulujące bezpieczeństwo urządzeń i oprogramowania wykorzystywanych do transmisji danych.

*Dz.U. 2004 nr 171 poz. 1800*
https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20041711800

# Centralna organizacja

Zapewnia merytoryczne ramy funkcjonowania organów odpowiedzialnych za Cyberbezpieczęństwo na szczeblu krajowym i w kontekście międzynarodowym. W tym w szczególności w zakresie:

**Tworzenia strategii ochrony cyberbezpieczeństwa:**

Opracowują narodowe strategie, które określają zasady i cele w zakresie ochrony przed cyberzagrożeniami.

**Wdrażania przepisów i regulacji dotyczących cyberprzestępczości:**

Zapewniają, że wszelkie działania są zgodne z krajowymi i międzynarodowymi regulacjami prawnymi.

**Współpracy międzynarodowa w zakresie zwalczania cyberzagrożeń:**

Uczestniczą w wymianie informacji i wspólnych działaniach z organizacjami międzynarodowymi.

**Nadzoru nad zgodnością działań z przepisami prawa:**

Sprawdzają, czy organizacje i instytucje przestrzegają obowiązujących przepisów w zakresie cyberbezpieczeństwa.

# Krajowy system cyberbezpieczeństwa

## Ustawa z dnia 5 lipca 2018 r.
## o krajowym systemie cyberbezpieczeństwa (art. 73-76)

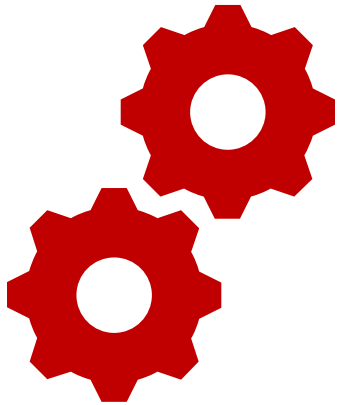
- Określa podstawowe zasady funkcjonowania Krajowego Systemu Cyberbezpieczeństwa (KSC).
- Określa podmioty odpowiedzialne za cyberbezpieczeństwo, ich obowiązki oraz uprawnienia.
- Definiuje usługi kluczowe oraz infrastrukturę krytyczną, które podlegają szczególnej ochronie przed cyberatakami.

*Dz.U. 2018 poz. 1560*
https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560

# Strategia cyberbezpieczeństwa RP

## Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r.
## w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024

- Wyznacza główne cele i kierunki rozwoju narodowego cyberbezpieczeństwa.
- Wzmacnianie odporność państwa na cyberataki.
- Rozwija kompetencje i współpracę międzynarodową.
- Implementacja strategii poprzez konkretne inicjatywy, projekty i regulacje.

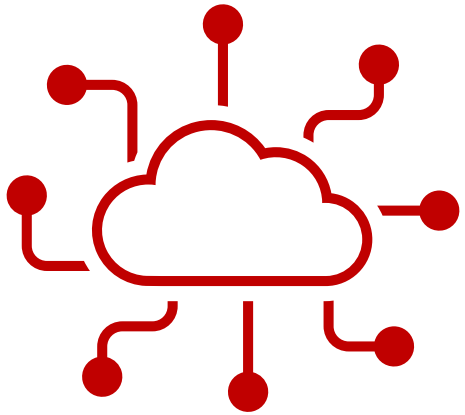


*M.P. 2019 poz. 1037*
https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WMP20190001037

# Narodowe standardy cyberbezpieczeństwa

**Zbiór rekomendacji standaryzujących rozwiązania zabezpieczające w sieciach i systemach informacyjnych**

- Wyznaczanie kierunków dla polityki bezpieczeństwa informacji w sektorze prywatnym i publicznym.
- Znaczenie standardów dla ochrony infrastruktury krytycznej i podniesienia poziomu świadomości cybernetycznej w organizacjach.
- Zalecenia i najlepsze praktyki dotyczące zarządzania ryzykiem cybernetycznym.



*Narodowe Standardy Cyberbezpieczeństwa*
https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber

# Dyrektywa NIS2

**NIS 2 (Network and Information Security Directive 2)** to zaktualizowana dyrektywa UE dotycząca poprawy cyberbezpieczeństwa w sektorach krytycznych, takich jak energetyka, transport, finanse i infrastruktura cyfrowa.

NIS 2 wprowadza surowsze wymogi dotyczące zgłaszania incydentów, rozszerza zakres podmiotów objętych regulacjami i wzmacnia współpracę między państwami członkowskimi w zakresie ochrony przed cyberzagrożeniami. Jej celem jest zwiększenie odporności na cyberataki w całej UE.

## Oś czasu wdrożenia Dyrektywy NIS2

**14 XII 2022** – Przyjęcie dyrektywy NIS2 przez Parlament Europejski i Radę (Dyrektywa (UE) 2022/2555).

**27 XII 2022** – Publikacja dyrektywy NIS2 w Dzienniku Urzędowym Unii Europejskiej (Dyrektywa (UE) 2022/2555).

**16 I 2023** – Wejście w życie dyrektywy NIS2 (Dyrektywa (UE) 2022/2555).

**17 VII 2023** – Komisja Europejska podaje wytyczne dotyczące stosowania przepisów dyrektywy NIS2 (Dyrektywa (UE) 2022/2555).

**17 X 2024** – Państwa członkowskie przyjmują i publikują przepisy niezbędne do wykonania dyrektywy NIS2 (Dyrektywa (UE) 2022/2555).

**18 X 2024** – Państwa członkowskie stosują przepisy dyrektywy NIS2 (Dyrektywa (UE) 2022/2555).

**18 X 2024** – Uchyla się art. 19 rozporządzenia (UE) nr 910/2014 oraz art. 40 i 41 dyrektywy (UE) 2018/1972 przez dyrektywę NIS2 (Dyrektywa (UE) 2022/2555).

*Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022*
https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

# Rozporządzenie AI Acta

**AI Act (Artificial Intelligence Act)** to rozporządzenie Unii Europejskiej mające na celu uregulowanie stosowania sztucznej inteligencji.

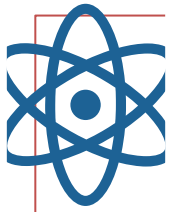
Jego głównym celem jest zapewnienie, że systemy AI są bezpieczne, przejrzyste i zgodne z wartościami UE. Rozporządzenie wprowadza klasyfikację systemów AI według poziomu ryzyka oraz nakłada surowe wymogi na te o wysokim ryzyku, takie jak systemy wykorzystywane w zdrowiu czy sądownictwie. AI Act ma wspierać innowacje, jednocześnie chroniąc prawa obywateli.

## Oś czasu wdrożenia Dyrektywy AI Act

- **2 sierpnia 2024** – Wejście w życie rozporządzenia.
- **2 lutego 2025** – Wdrożenie przepisów dotyczących podstawowych definicji, zakresu stosowania, klasyfikacji i oceny zgodności systemów AI wysokiego ryzyka przez kraje członkowski.
- **2 maja 2025** – Zastosowanie kodeksów postępowania.
- **2 sierpnia 2025** – Obowiązywanie zasad zarządzania i obowiązków dla ogólnego zastosowania AI (GPAI).
- **2 sierpnia 2026** – Rozpoczęcie stosowania przepisów EU AI Act dla systemów AI .
- **2 sierpnia 2027** – Stosowanie całego EU AI Act dla wszystkich kategorii ryzyka .
- **Do 2 sierpnia 2031 r.** – Komisja Europejska przeprowadzi ocenę egzekwowania rozporządzenia i przedłoży sprawozdanie Parlamentowi Europejskiemu, Radzie oraz Europejskiemu Komitetowi Ekonomiczno-Społecznemu.

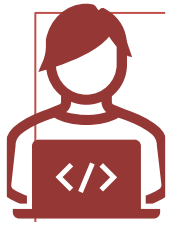
*Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r.*
https://eur-lex.europa.eu/eli/reg/2024/1689/oj/pol

# Kierunki rozwoju prawa



**Komputery kwantowe**

**Fake news**



**Wojny algorytmów**

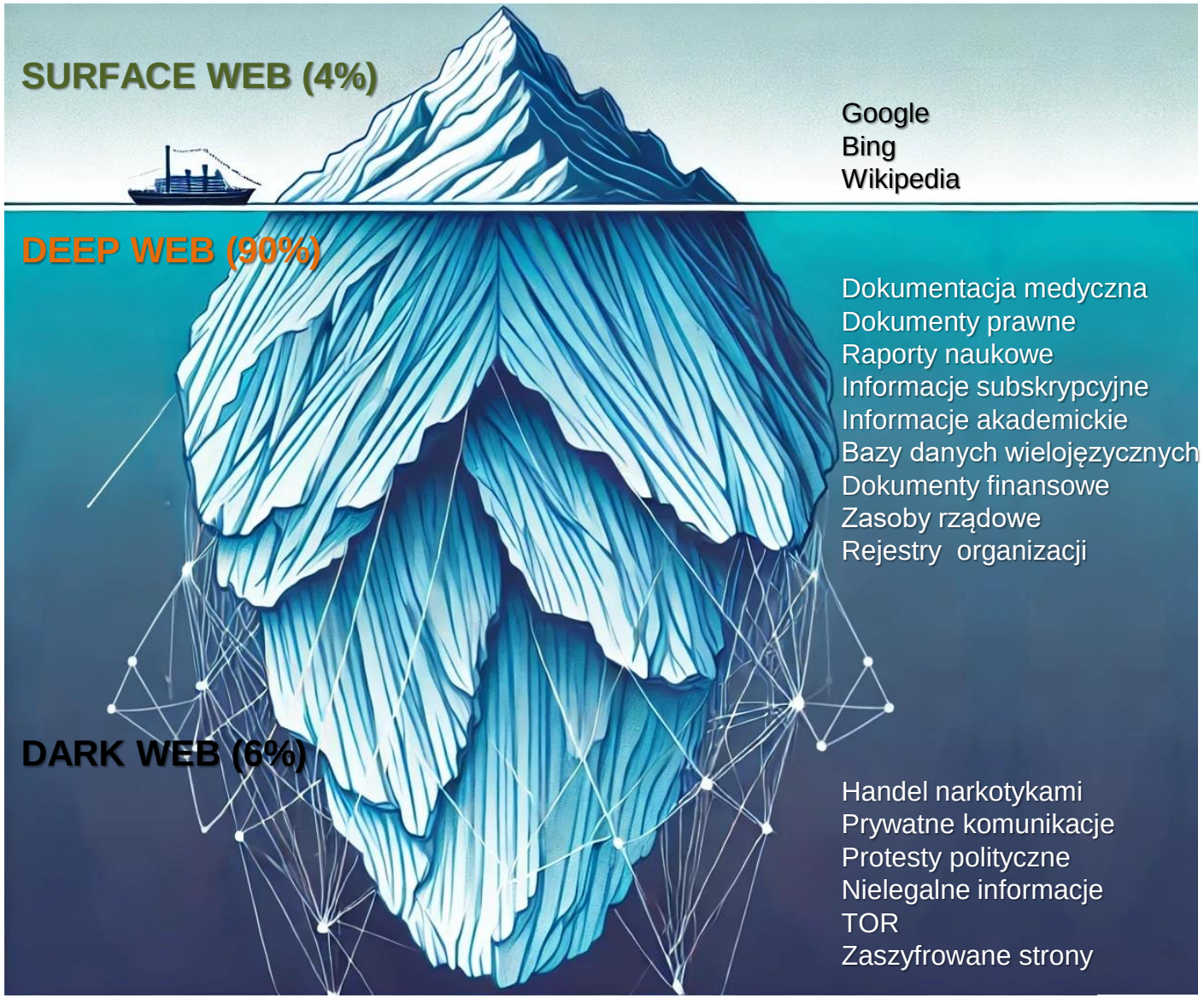
**Sztuczna inteligencja**

**Bezpieczeństwo dzieci online**

**Internet Rzeczy (IoT)**

# Darknet

**Ciemna strona Internetu**



# Korelacja cyberzagrożeń z aktami prawa

| Zagrożenie cyberbezpieczeństwa | Odpowiadające akty prawne | Gdzie zgłosić |
|---|---|---|
| Phishing | Kodeks Karny - Art. 269b KK | Policja, CSIRT |
| Ataki ransomware | Kodeks Karny - Art. 269b KK, Ustawa o usługach płatniczych | Policja, ABW, KNF |
| Malware | Kodeks Karny - Art. 269b KK | Policja, CSIRT |
| Ataki DDoS | Kodeks Karny - Art. 269a KK | Policja, CSIRT |
| Wycieki danych | Ustawa o ochronie danych osobowych | UODO, Policja, GIODO |
| Insider Threats | Ustawa o ochronie danych osobowych | UODO, Policja |
| Exploity zeroday | Ustawa o krajowym systemie cyberbezpieczeństwa | Policja, CSIRT |
| Ataki Man-in-the-Middle (MITM) | Kodeks Karny - Art. 269b KK | Policja, CSIRT |
| SQL Injection | Kodeks Karny - Art. 269b KK | Policja |
| Cross-Site Scripting (XSS) | Kodeks Karny - Art. 269b KK | Policja |
| Ataki na infrastrukturę krytyczną | Rozporządzenie Rady Ministrów w sprawie usług kluczowych | CSIRT, ABW |
| Spoofing | Kodeks Karny - Art. 269b KK | Policja |
| Inżynieria społeczna | Kodeks Karny - Art. 269b KK | Policja |
| Cryptojacking | Kodeks Karny - Art. 269b KK | Policja, CSIRT |
| Bezpieczeństwo Internetu Rzeczy (IoT) | Ustawa Prawo telekomunikacyjne | UKE, Policja, CSIRT |
| Ataki sieciowe | Kodeks Karny - Art. 269a KK | Policja, ABW, NASK, CSIRT |
| Kradzież konta lub przedmiotu w grze online | Kodeks Karny - Art. 268 KK, Ustawa o świadczeniu usług drogą elektroniczną | Policja |

**CSIRT NASK (CERT POLSKA)**: pełniący rolę krajowego zespołu reagowania na incydenty komputerowe.
**CSIRT GOV (ABW)**: odpowiedzialny za administrację rządową.
**CSIRT MON (DKWOC)**: odpowiedzialny za sektor obronności i bezpieczeństwa państwa.

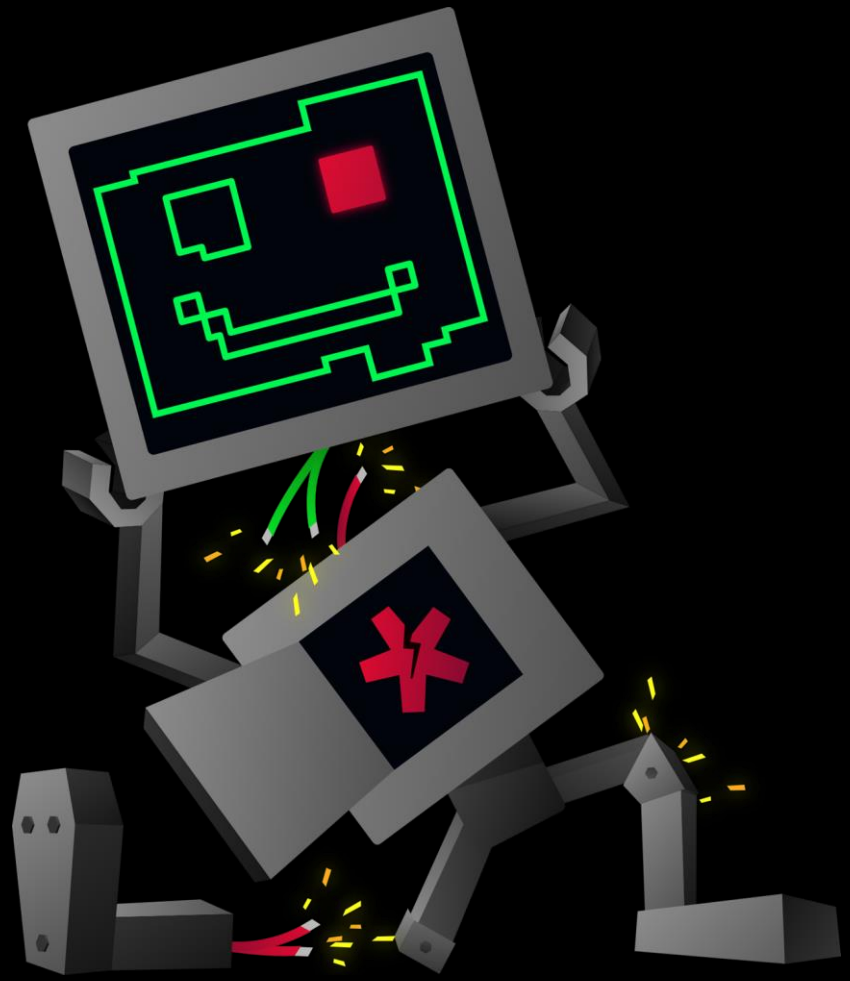
# Zakończenie

**Treść prezentacji w postaci PDF dostępna jest pod**

THE H@CK SUMMIT

# Dziękujemy za uwagę!

**Zapraszamy do zadawania pytań oraz oceny wystąpienia pod nagraniem.**



## Kod QR i link do oceny

https://thehacksummit.com/user.html#!/lecture/THS24-cd83/rate

thehacksummit.com | 17-18 października 2024 | PGE Narodowy + Online

ORGANIZATORZY:

ACADEMIC PARTNERS