
UTH
UCZELNIA
TECHNICZNO-HANDLOWA
im. H. Chodkowskiej
w Warszawie
Twoja
przyszłość
zaczyna się w UTH.



UCZELNIA TECHNICZNO-HANDLOWA im. H. Chodkowskiej w Warszawie

dr inż. Michał Malinowski

https://www.drmalinowski.edu.pl/

mgr Małgorzata Musiał

https://mmusial.owlstown.net

Cyberprzemoc i jej zapobieganie

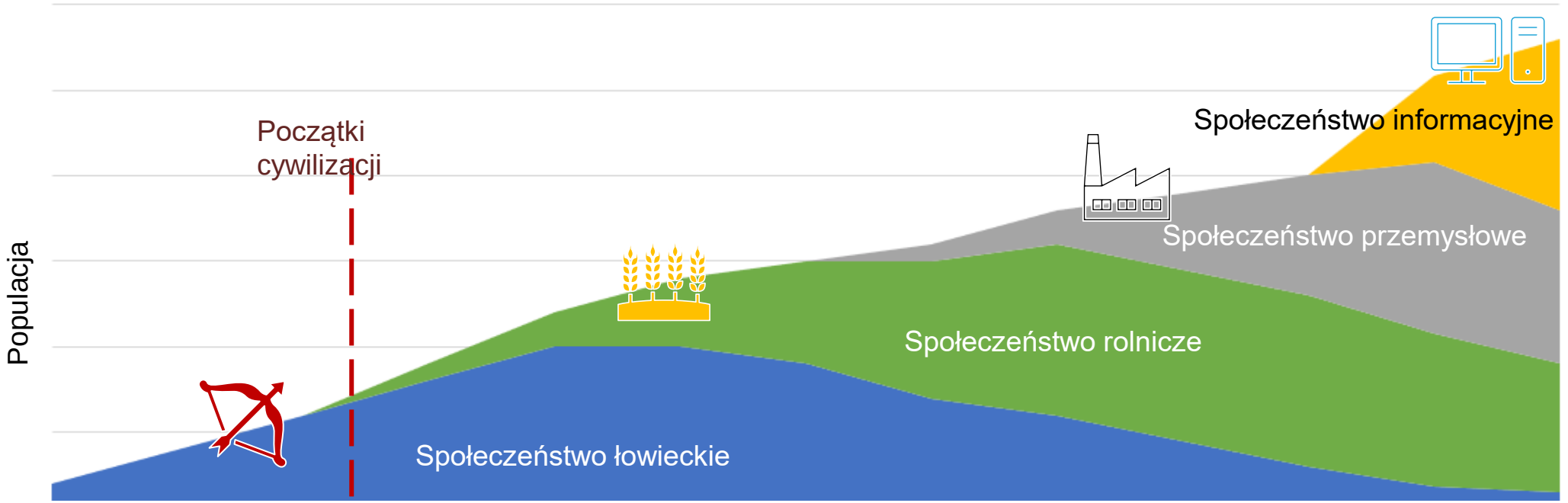
czyli

Jak polskie prawo radzi sobie z cyberprzestępczością

Cyberbezpieczny z UTH

Gdzie teraz jesteśmy… ?





Informacja - najważniejszy zasób

Społeczeństwo informacyjne

podstawą społeczeństwa informacyjnego
jest gospodarka oparta na wiedzy (dane, informacje),
a jej zasadniczym zasobem gospodarczym
są informacje skumulowane w bazach.

Kreacja informacji

Tworzenie danych
Zbieranie danych
Analiza danych
Udostępnianie danych
Konsolidacja danych
Zbiory danych

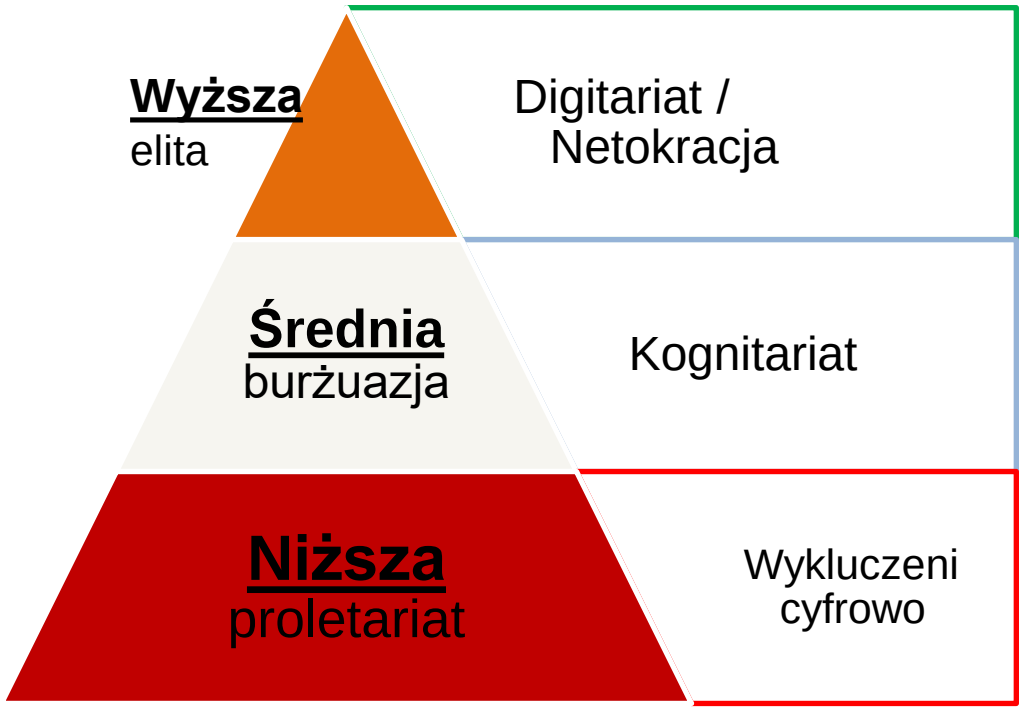
Autor



Czytelnik



Klasy społeczne



Destrukcja informacji

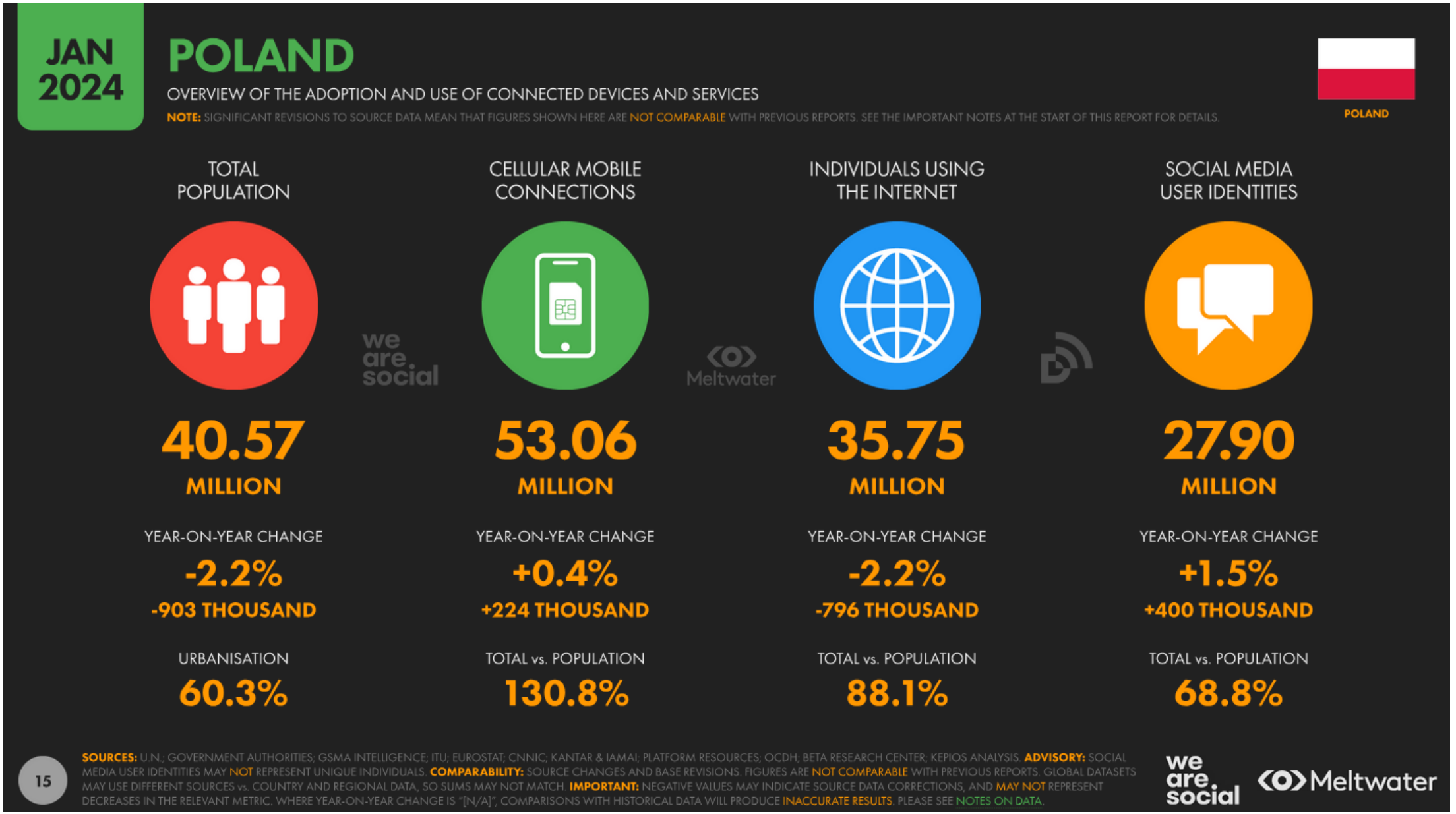
Usuwanie danych
Dezinformacja
Zniekształcenie danych
Brak aktualizacji
Zaniedbania w archiwizacji
Ataki cybernetyczne

Obrońca



Atakujący




JAN 2024
POLAND
OVERVIEW OF THE ADOPTION AND USE OF CONNECTED DEVICES AND SERVICES
NOTE: SIGNIFICANT REVISIONS TO SOURCE DATA MEAN THAT FIGURES SHOWN HERE ARE NOT COMPARABLE WITH PREVIOUS REPORTS. SEE THE IMPORTANT NOTES AT THE START OF THIS REPORT FOR DETAILS.
POLAND
TOTAL POPULATION
CELLULAR MOBILE CONNECTIONS
INDIVIDUALS USING THE INTERNET
SOCIAL MEDIA USER IDENTITIES
we are social
Meltwater
40.57 MILLION
53.06 MILLION
35.75 MILLION
27.90 MILLION
YEAR-ON-YEAR CHANGE
-2.2%
-903 THOUSAND
YEAR-ON-YEAR CHANGE
+0.4%
+224 THOUSAND
YEAR-ON-YEAR CHANGE
-2.2%
-796 THOUSAND
YEAR-ON-YEAR CHANGE
+1.5%
+400 THOUSAND
URBANISATION
60.3%
TOTAL vs. POPULATION
130.8%
TOTAL vs. POPULATION
88.1%
TOTAL vs. POPULATION
68.8%
15
SOURCES: U.N.; GOVERNMENT AUTHORITIES; GSMA INTELLIGENCE; ITU; EUROSTAT; CNNIC; KANTAR & IAMAI; PLATFORM RESOURCES; OCDH; BETA RESEARCH CENTER; KEPIOS ANALYSIS. ADVISORY: SOCIAL MEDIA USER IDENTITIES MAY NOT REPRESENT UNIQUE INDIVIDUALS. COMPARABILITY: SOURCE CHANGES AND BASE REVISIONS. FIGURES ARE NOT COMPARABLE WITH PREVIOUS REPORTS. GLOBAL DATASETS MAY USE DIFFERENT SOURCES vs. COUNTRY AND REGIONAL DATA, SO SUMS MAY NOT MATCH. IMPORTANT: NEGATIVE VALUES MAY INDICATE SOURCE DATA CORRECTIONS, AND MAY NOT REPRESENT DECREASES IN THE RELEVANT METRIC. WHERE YEAR-ON-YEAR CHANGE IS "[N/A]", COMPARISONS WITH HISTORICAL DATA WILL PRODUCE INACCURATE RESULTS. PLEASE SEE NOTES ON DATA.
we are social
Meltwater

Cyberprzemoc

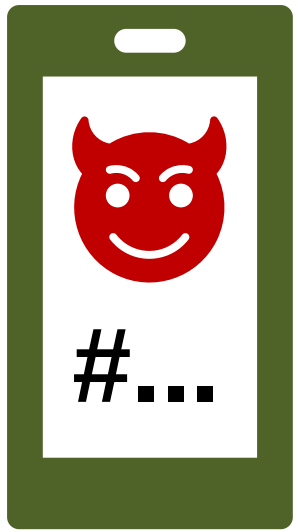
Cyberprzemoc (ang. cyberbullying) to forma przemocy, która ma miejsce w cyberprzestrzeni, głównie za pośrednictwem Internetu i urządzeń mobilnych.

Polega na celowym i powtarzalnym działaniu mającym na celu zaszkodzenie drugiej osobie, często w sposób trudny do wykrycia i udowodnienia.

Cyberprzemoc jest szczególnie niebezpieczna, ponieważ może mieć trwały wpływ na zdrowie psychiczne ofiary (uraz) i jest trudna do kontrolowania z uwagi na anonimowość sprawców oraz szybkość rozprzestrzeniania się informacji w sieci.



Cyberprzemoc



Cyberprzemoc

- **Nękanie (ang. harassment)** — Powtarzalne wysyłanie obraźliwych, groźnych lub poniżających wiadomości.
- **Zniesławienie (ang. defamation)** — Rozpowszechnianie nieprawdziwych informacji lub plotek mających na celu naruszenie dobrego imienia ofiary.
- **Wykluczenie (ang. exclusion)** — Celowe pomijanie danej osoby w grupach, społecznościach internetowych czy komunikatorach.
- **Podszywanie się (ang. impersonation)** — Kradzież tożsamości w celu działania na szkodę ofiary, np. publikowania kompromitujących treści w jej imieniu.
- **Upublicznianie prywatnych informacji (ang. doxing)** — Ujawnianie poufnych danych, takich jak adres, numer telefonu, zdjęcia bez zgody właściciela.
- **Cyberstalking** — Obsesyjne śledzenie i nękanie ofiary za pomocą narzędzi cyfrowych.
- **Sextortion i revenge porn** — Wykorzystywanie intymnych materiałów (zdjęć, filmów) do szantażu lub kompromitowania ofiary.
- **Trolling** — Prowokacyjne komentarze mające na celu wywołanie emocjonalnej reakcji lub eskalację konfliktu.

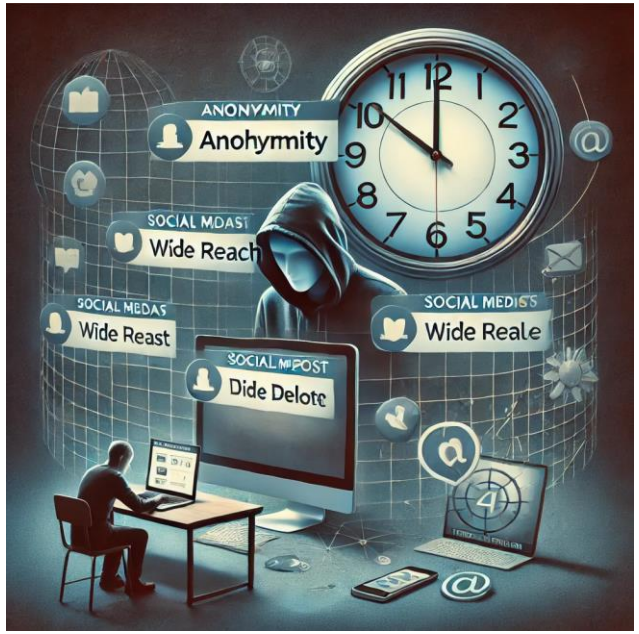
Cechy Cyberprzemocy

Anonimowość sprawcy

- Sprawcy często ukrywają swoją tożsamość, co utrudnia ich identyfikację.

Szeroki zasięg

- Treści publikowane w Internecie mogą dotrzeć do szerokiego grona odbiorców w krótkim czasie.



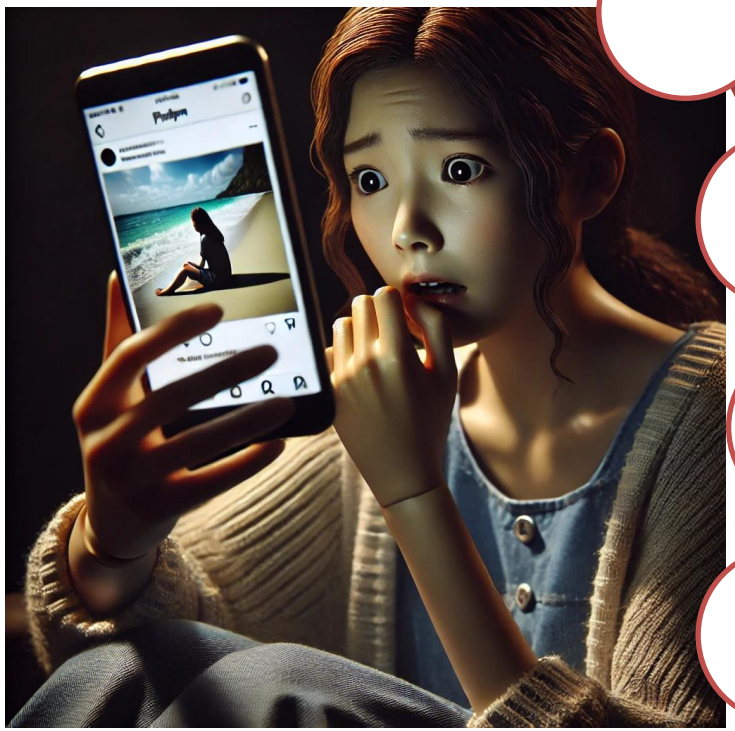
Brak granic czasowych

- Cyberprzemoc może odbywać się przez całą dobę.

Trudność usunięcia treści

- Usunięcie kompromitujących materiałów z internetu bywa praktycznie niemożliwe.

Skutki Cyberprzemocy



Psychiczne
- lęk, depresja, obniżone poczucie własnej wartości, a w skrajnych przypadkach myśli samobójcze.

Społeczne
- wycofanie z życia społecznego, trudności w budowaniu relacji międzyludzkich.

Zawodowe i edukacyjne
- obniżenie wyników w nauce lub pracy, absencje.

Prawne
- sprawcy mogą zostać pociągnięci do odpowiedzialności prawnej, np. za zniesławienie czy groźby karalne.

Finansowe
- koszty związane z utratą prywatnych danych (np. oszustwa finansowe, kradzież tożsamości), utrata dochodów z powodu uszczerbku na reputacji zawodowej lub społecznej.

Jak przeciwdziałać cyberprzemocy?

Edukacja i świadomość

- Uświadamianie dzieci i młodzieży na temat zagrożeń w internecie.
- Nauka krytycznego podejścia do treści w sieci i rozpoznawania sytuacji cyberprzemocy.



Tworzenie bezpiecznej przestrzeni online

- Platformy internetowe powinny oferować narzędzia do raportowania nadużyć.
- Administratorzy powinni aktywnie monitorować i reagować na nieodpowiednie zachowania.

Jak przeciwdziałać cyberprzemocy?



Ochrona prywatności

- Unikanie udostępniania zbyt wielu danych osobowych w sieci.

Wsparcie psychologiczne

- Zapewnienie psychologicznej pomocy ofiarom cyberprzemocy.
- Zachęcanie do rozmowy o problemie z zaufaną osobą.

Jak przeciwdziałać cyberprzemocy?

Zgłaszanie przypadków cyberprzemocy

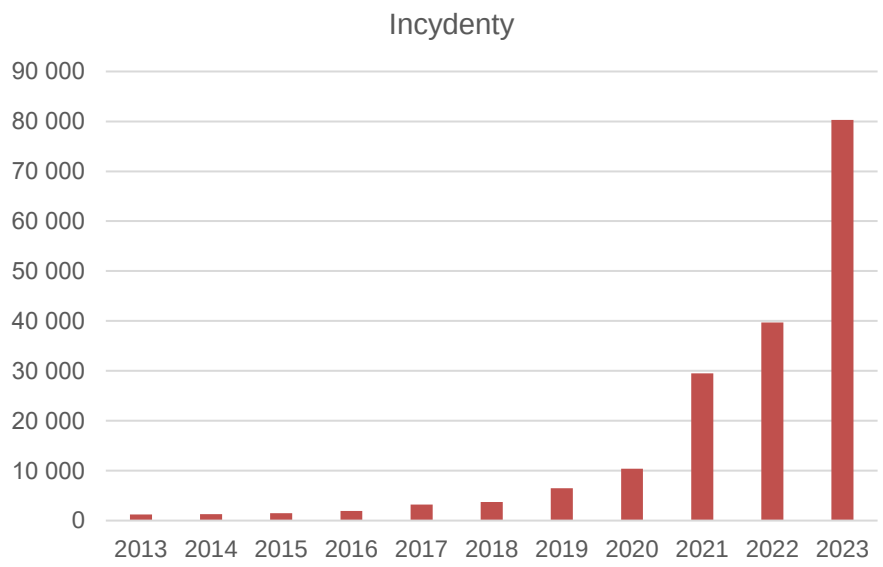
- Informowanie odpowiednich organów, np. policji, gdy dochodzi do łamania prawa.
- Zbieranie dowodów (zrzuty ekranu, zapis wiadomości) w celu ułatwienia działań prawnych.



Prawne regulacje

- Cyberprzemoc jest ścigana na podstawie przepisów kodeksu karnego, np. za stalking, groźby czy naruszenie dóbr osobistych.

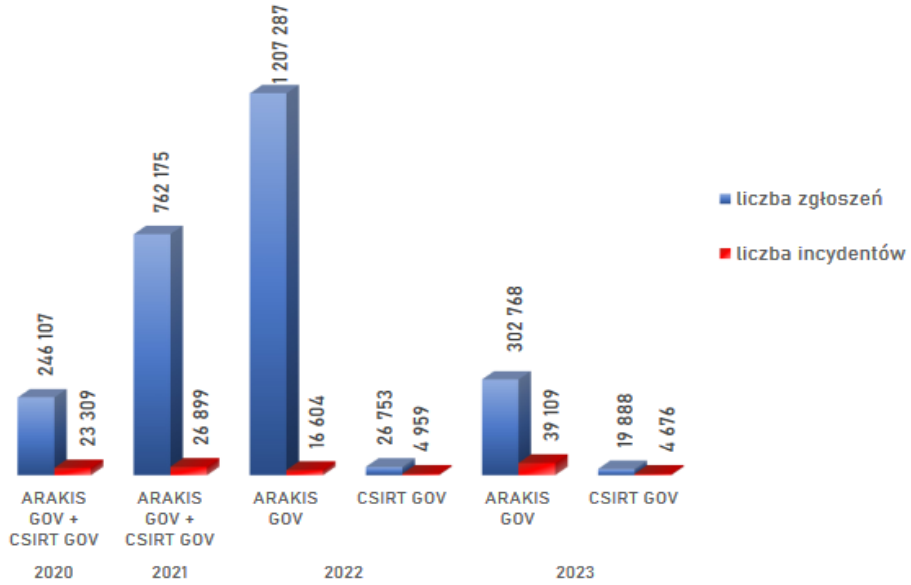
Incydenty bezpieczeństwa



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

Liczba incydentów: **80 267** (2023)

Liczba incydentów bezpieczeństwa



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%

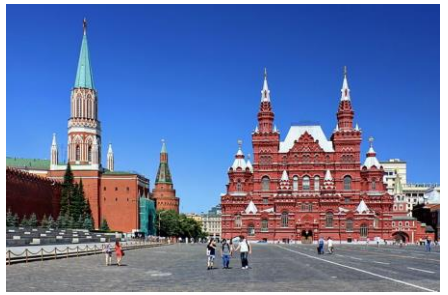
Raport roczny z działalności CERT POLSKA (CSIRT NASK)
https://cert.pl/uploads/docs/Raport_CP_2023.pdf

Wykorzystywanie AI do cyberprzemocy

Deepfake:	Tworzenie fałszywych, realistycznych treści wideo lub audio (np. kompromitujących filmów) przy użyciu technologii deepfake, które mogą być wykorzystane do szantażu lub ośmieszania ofiary.
Boty i automatyzacja:	Używanie AI do generowania masowych obraźliwych wiadomości, komentarzy lub spamu skierowanego przeciwko konkretnej osobie.
Profilowanie i targetowanie:	AI może być wykorzystywana do analizy danych ofiary (np. z mediów społecznościowych), aby lepiej dostosować strategię nękania lub trolling.
Generatywne AI:	Wykorzystywanie narzędzi AI do tworzenia fałszywych historii, dokumentów czy innych materiałów mających na celu kompromitowanie ofiary.







Cyberprzestępstwo

Cyberprzemoc jest często formą cyberprzestępczości

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



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

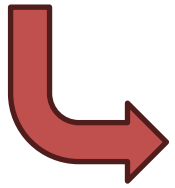
Cyberprzestępczość to każde działanie przestępcze wykonane z wykorzystaniem technologii informatycznych, które jest skierowane przeciwko poufności, integralności i dostępności systemów komputerowych, sieci lub danych.

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.

Formy popełniania cyberprzestępstw

I generacja
Cyberprzestępczość indywidualna
(lata 80. i 90.)

Działania indywidualnych hakerów, polegające na włamaniach do systemów komputerowych lub tworzeniu wirusów.

II generacja
Cyberprzestępczość sieciowa
(lata 2000–2010)

Pojawienie się zorganizowanych grup przestępczych oraz złośliwego oprogramowania (trojany, robaki, phishing spyware), rozpowszechnianych przez Internet lub inne sieci komputerowe.

III generacja
Cyberprzestępczość zorganizowana
(lata 2010–2020)

Ataki na infrastrukturę krytyczną oraz duże organizacje, prowadzone przez zaawansowane grupy cyberprzestępcze, często sponsorowane wrogie państwa lub aktywistów (np. DDoS, APT, ransomware).

IV generacja
Cyberprzestępczość nowych technologii
(od 2020)

Cyberprzestępczość wykorzystująca AI, IoT, blockchain oraz kryptowaluty. Ataki skierowane na systemy automatyczne oraz inteligentne urządzenia (np.: ataki Adversarialne, Prompt Injection, zatruwanie danych).

V generacja
Cyberprzestępczość kwantowa

Zagrożenia wynikające z rozwoju komputerów kwantowych i neurotechnologii, zdolne do przełamywania zabezpieczeń i manipulowania danymi na ogromną skalę i w wielu wymiarach.

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



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.

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.

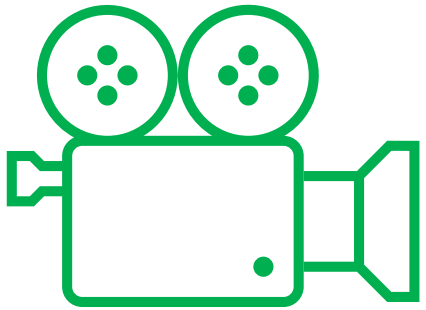
Prawa autorskie

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

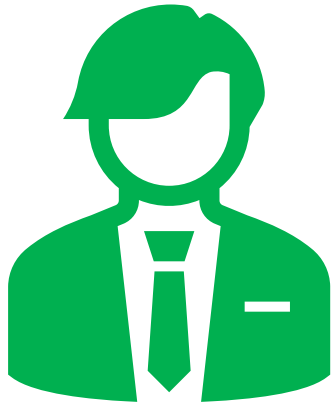
Ochrona danych osobowych

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.



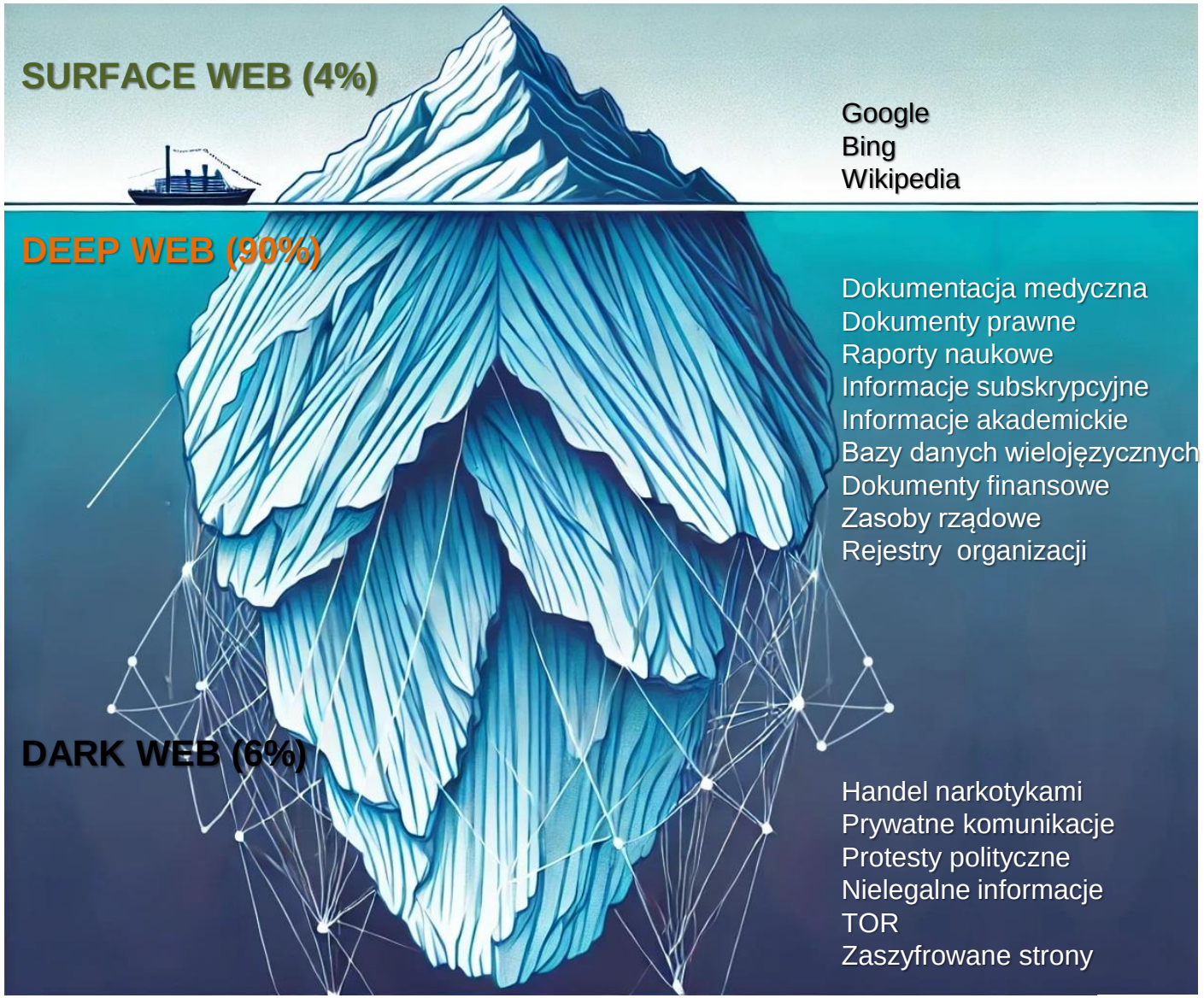
Dz.U. 2018 poz. 1000
https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001000

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.



Więcej

Dawka informacji ze świata technologii, sztucznej inteligencji oraz cyberbezpieczeństwa.

UCZELNIA
TECHNICZNO-HANDLOWA
im. H. Chodkowskiej
w Warszawie

Dziękuję za uwagę !

Cyberbezpieczny z UTH