ZAGROŻENIA W SIECI

Małgorzata Sitarczyk
WYDZIAŁ PEDAGOGIKI I PSYCHOLOGII
WSEI

ATRAKCYJNOŚĆ INTERNETU

- Polisensoryczny charakter dostarczanych informacji, wielobarwny, animowany obraz, bogactwo treści słuchowych i obrazowych.
- Wszechstronna dostępność (prosty i szybki dostęp do informacji).
- Różnorodność kontaktów społecznych.
- Płynność tożsamości odbiorcy i nadawcy informacji.
- Poczucie przynależności do wspólnoty.
- Anonimowość odbiorcy i nadawcy.
- Zrównanie statusów społecznych, ekonomicznych.
- Tymczasowy, niezobowiązujący charakter wszelkich nawiązywanych interakcji.

ATRAKCYJNOŚĆ INTERNETU

- Pokonywanie ograniczeń przestrzennych i czasowych.
- Rozciąganie i koncentracja czasu.
- Możliwość relacji czasowych asynchronicznych i synchronicznych.
- Możliwość permanentnego zapisu informacji.
- Możliwość nie tylko dobierania, ale także kreowania treści i przestrzeni wirtualnej.
- Wszechstronne możliwości wykorzystania w ramach różnych form działalności człowieka: nauki, pracy, rozrywki, odpoczynku, czynności codziennych, praktyk religijnych itp.

9 STYLÓW WIRTUALNEGO FUNKCJONOWANIA W INTERNECIE:

- psychopatyczny (antysocjalny)
- narcystyczny
- schizoidalny
- paranoidalny
- depresyjno-maniakalny
- masochistyczny
- obsesyjno – kompulsyjny
- histeryczny
- dysocjacyjny (Ginowicz, 2005).

ZAGROŻENIA W SIE

- AGRESJA ELEKTRONICZNA
- PROMOWANIE TREŚCI NIEBEZPIECZNYCH

  [PRO-ANA, rasizm, pornografia z udziałem dzieci]
- SPONSORING
- ZACHĘCANIE DO HAZARDU, NARKOTYKÓW
- KRADZIEŻE WIRTUALNE
- NETOHOLIZM

Agresja elektroniczna to zbiór wrogich zachowań, który realizowany jest za pomocą Internetu lub telefonów komórkowych, określanych zbiorczo jako tzw. nowe media lub współczesne technologie komunikacyjne [Pyżalski, 2009]

cechy wyróżniające agresję elektroniczną:

- **anonimowość**
- **ciągłość oddziaływania**
- **nieograniczona lub tzw. niewidzialna publiczność** (*invisible audience*)
- **efekt kabiny pilota** [Walrave i Heirman, 2009]
- **łatwość atakowania nieznajomych ofiar** [Pyżalski, 2009]
- **asynchroniczny charakter interakcji** (dziś obraźliwy tekst, zdjęcie- zamieszczony jutro np. na kilka godzin przed ważnym egzaminem).

ANONIMOWOŚĆ

- **Anonimowy akt agresji posiada znacznie większy potencjał wiktymizacyjny.**
- Ofiara anonimowego ataku nie wie, czy jest prześladowana „przez jednego sprawcę czy przez więcej osób; czy sprawcą jest chłopak czy dziewczyna, kolega czy wróg, ktoś znajomy czy osoba obca”.
- Tego typu niepewność powoduje, że zagrożenie ze strony sprawcy odbierane jest jako bardzo prawdopodobne i bolesne [Walrave i Heirman,2009].

ANONIMOWOŚĆ

- Akt agresji elektronicznej, w której sprawca jest anonimowy, może powodować, że po stronie nieujawniającego swojej tożsamości agresora wystąpi **rozhamowanie** (*disinhibition*) i zaangażuje się on w dysfunkcjonalne zachowania, których nigdy by nie podjął w przypadku gdyby jego tożsamość była znana [Joinson, 2009].
- **AGRESOR JEST ANONIMOWY ==➔ ROZHAMOWANIE**
- Oczywiście anonimowość nie stanowi jedynej przyczyny wystąpienia **rozhamowania** – chociaż jest ona jednym z bardziej istotnych jego motorów. Eliminuje ona, przynajmniej w momencie popełnienia aktu agresji elektronicznej, ryzyko zidentyfikowania i ewentualnego ukarania sprawcy – co także w niektórych przypadkach może stanowić zachętę do podejmowania tego typu działań.
- **AGRESOR CZUJE SIĘ BEZKARNYM =➔ ROZHAMOWANIE**

CIĄGŁOŚĆ ODDZIAŁYWANIA

- **Dostęp do ofiary nie jest ograniczony w czasie i przestrzeni** [Walrave i Heirman, 2009].

- Ciągłość oddziaływania polega na tym, iż ofiara agresji elektronicznej dostępna jest dla sprawcy właściwie bez przerwy i nie posiada miejsca, w którym może się ukryć [Slonje i Smih, 2008; Walrave i Heirman, 2009].

- Tego typu mechanizm jest w szczególności obecny w przypadku tych aktów agresji elektronicznej, gdzie sprawcy publikują jakieś materiały dotyczące ofiary – np. umieszczają kompromitujące ją informacje w Internecie. Bez względu na to gdzie przebywa ofiara – jest ona świadoma, że akt agresji „trwa" i jest powtarzany w przypadku każdego dostępu do obraźliwych materiałów, którego dokonują inni użytkownicy Internetu.

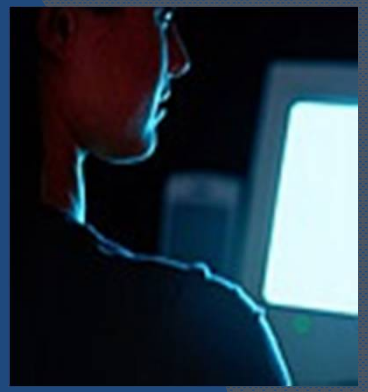
UPUBLICZNIENIE

- **Upublicznienie-** różnica w ilości osób, świadków agresji w stosunku do sytuacji realnych.
- Świadomość „*publicznego poniżenia*” jest podstawowym mechanizmem, który może prowadzić u ofiar do skrajnych reakcji wywołanych wiktymizacją.

- Tak było z dużym prawdopodobieństwem w przypadku młodego mężczyzny ze Strzegomia, który powiesił się po tym jak pewna nastolatka umieściła w Internecie krótki film w którym opowiada intymne szczegóły swoich prawdziwych lub wyimaginowanych spotkań z ofiarą [Wiadomości WP, 2009].

EFEKT KABINY PILOTA

(*cockpit effect*)



- Walrave i Heirman (2009) porównują **sprawcę agresji elektronicznej do pilota bombowca, który mógł bombardować miasta, gdyż nie widział bezpośrednio cierpienia swoich ofiar.**
- Technologie komunikacyjne sprawiają, że sprawca agresji elektronicznej komunikuje się w sposób zapośredniczony – ma kontakt z ekranem i klawiaturą komputera lub telefonu komórkowego a nie z rzeczywistą ofiarą.
- W takiej sytuacji ograniczony jest kanał komunikacji niewerbalne, który stanowi nośnik komunikatów dotyczących emocji. Oznacza to, że niektóre osoby mogą angażować się we wrogie wobec innych działania bez świadomości, że ich zachowania krzywdzą innych [Pyżalski, 2009].

ŁATWOŚĆ AKTAKOWANIA NIEZNAJOMYCH

- W cyberprzestrzeni mamy do czynienia z wieloma osobami i/lub ich reprezentacjami w postaci profili, stron internetowych, itp.
- Ta styczność pozwala na stosunkowo łatwe i nie powiązane zwykle z negatywnymi konsekwencjami dla sprawcy atakowanie osób, z którymi sprawcy nie łączą żadne relacje zarówno w cyberprzestrzeni jak i w świecie offline (realnym).
- Dodatkowo, szczególnie w sytuacjach mniej poważnych ataków (np. obrażania w pokoju czatowym), ofiary stosunkowo rzadko będą podejmować próbę odszukania sprawców w celu wyciągnięcia konsekwencji.

ASYNCHRONICZNOŚĆ RELACJI W CZASIE

- Wirtualna przestrzeń umożliwia przygotowanie ataków i uruchomienie ich w ważnym dla ofiary momencie.
- Permanentny zapis informacji- pamięć ludzka już dawno utraciłaby te dane.
- Zmiana sytuacji danej osoby- stare informacje nadal krążą w sieci.
- *Kłamstwo obiegło już świat dwa razy- prawda zakłada dopiero buty.*

FORMY AGRESJI ELEKTRONICZNEJ

- przesyłanie **wrogich komunikatów** bezpośrednio do ofiary (np. wysłanie nieprzyjemnego komunikatu **SMS)**
- ataki, które w ogóle nie zawierają elementu komunikacji z ofiarą (np. upublicznienie online, czyichś tajemnic).
- **zdjęcia lub filmy** odbierane przez ofiary jako bardzo dotkliwe (Slonje&Smith, 2009; Wojtasik, 2009).
- **wiadomości przez komunikator** (np. gadu-gadu), które obraziły/ośmieszyły kogoś.
- **komentowanie wypowiedzi na forum internetowym** w taki sposób, że sprawiają przykrość, straszą.
- **złośliwe komentowanie profilu** w portalu typu nasza-klasa.pl; fotka.pl lub blogów,.
- **obrażanie/wyzywanie** w grach online (np. Tibia, World of Warcraft, Counter Strike).

FORMY AGRESJI ELEKTRONICZNEJ

- wysyłanie wbrew woli materiałów [np. linki do materiałów z nieprzyjemnymi treściami].
- wysłanie materiału zawierającego wirus komputerowy.
- rozsyłanie, bez zgody właściciela telefonu/konta pocztowego/komunikatora, nieprzyjemnych informacji do innych osób.
- zamieszczanie w Internecie [rozesłanie innym osobom] zdjęć zrobionych w nieprzyjemnej, dla konkretnej osoby, sytuacji.
- włamania do poczty internetowej/komunikatora, ujawnianie tajemnic.

FORMY AGRESJI ELEKTRONICZNEJ

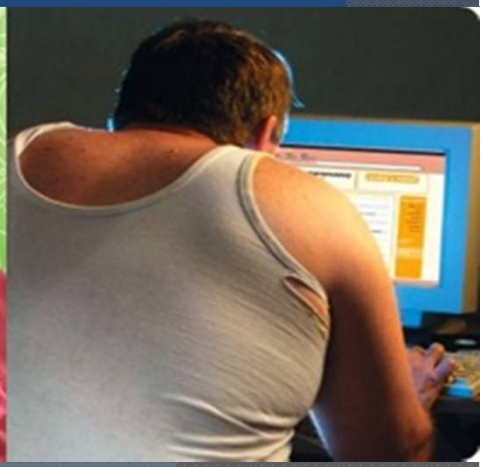
- prowokowanie do dziwnego zachowania, a potem umieszczanie w Internecie filmów lub zdjęć,
- zakładanie fałszywego konta na portalu typu nasza-klasa. pl; fotka.pl lub podobnym,
- wykonanie montażu/przetwarzanie i umieszczanie w Internecie zdjęć o obraźliwej treści,
- zakładanie stron internetowych przedstawiających osobę w nieprzyjemny sposób,
- wysyłanie na portal randkowy/towarzyski fałszywych ogłoszeń matrymonialnych.

RODZAJE AGRESJI ELEKTRONICZNEJ

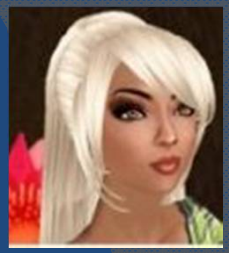
- Agresja słowna na forach, komunikatorach (*flaming*)
- Prześladowanie (*harassment*)
- Kradzież tożsamości
- Upublicznianie tajemnic (*outing*)
- Śledzenie (*cyberstalking*)
- Prowokowanie (*happy slapping*)
- Poniżenie (*denigration*)
- Wykluczenie (*exclusion*)
- Agresja „techniczna”

PROMOWANIE TREŚCI NIEBEZPIECZNYCH

- PRO-ANA
- SPONSORING
- PORNOGRAFIA Z UDZIAŁEM DZIECI
- RASIZM
- ZACHĘCANIE DO STOSOWANIA UŻYWEK
- WUODZENIE DZIECI



OSZUSTWA INTERNETOWE



- Phishing polega na tworzeniu fałszywych strony i wysyłaniu różnych ofert do użytkowników
- Kradzież tożsamości w grze i w realu
- Plagiaty internetowe
- Fałszywe sklepy internetowe
- Wirtualne kradzieże

NETOHOLIZM

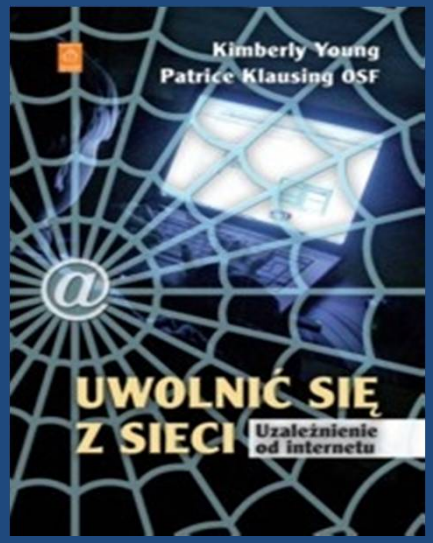
Dla określenia zjawiska kompulsywnego i nałogowego przebywania w sieci powstało wiele nazw:

- siecioholizm,
- infoholizm,
- netomania,
- datoholizm,
- Internet Addiction Disorder (IAD) - zespół uzależnienia od Internetu. Zaburzenie to ma podobny mechanizm powstawania, jaki obserwuje się przy uzależnieniu od środków psychoaktywnych (Pluciński, 2005).

Opierając się o kryteria diagnostyczne DSM IV z 1994 zespół uzależnienia od Internetu (IAD) można rozpatrywać jako nieprawidłowy sposób korzystania z sieci, prowadzący do istotnego zakłócenia czynności psychicznych i zaburzenia zachowania się, przejawiających się w okresie minionych 12 miesięcy, co najmniej trzema spośród następujących przejawów:

- zapotrzebowanie na kontakt
- koszty
- zespół odstawienny [Woronowicz, 2001. s. 192].

FAZY ROZWOJU KONTAKTÓW Z INTERNETEM



ZAANGAŻOWANIE

ZASTĘPOWANIE

UCIECZKA

PREFEROWANE TYPY KONTAKTÓW INTERNETOWYCH

- **Preferowanie cyberseksu** (uzależnienie od cybernetycznej pornografii albo chat roomów). Niekontrolowane oglądanie stron porno bywa formą ucieczki- od partner nieakceptowanej rzeczywistości lub siebie.
- **Uzależnienie od cybernetycznych relacji** (znajomości zawarte on-line poprzez ICQ, IRC, MUDDY, chat roomy, grupy dyskusyjne albo kawiarenki internetowe).
- **Kompulsje sieciowe** (obsesyjne robienie zakupów on- line, kompulsywny hazard on-line, uzależnienie od wirtualnych akcji).
- **Cyberkomunikacja**(posługiwanie się slangiem komputerowym).
- **Przeładowanie informacyjne** (kompulsyjne, nałogowe przeglądanie stron oraz przeszukiwanie danych).

GRY KOMPUTEROWE

- Symulatory
- Tekstowe
- Sportowe
- Strategiczne
- Zręcznościowe
- Logiczne
- Przygodowe

* RPG

ODDZIAŁYWANIE GIER KOMUTEROWYCH NA PSYCHIKĘ ODBIORCY

- **Podawanie wzorów**; to przedstawienie dziecku wzorców postępowania, które pobudzają go do naśladowania, czyli upodobania się wyglądem, sposobem wyrażania się, zachowaniem do modela.
- **Nadawanie znaczeń**, to wiązanie określonych emocji ze zdarzeniami.
- **Trening,** to powtarzanie czynności czego wynikiem jest wyuczenie się ich oraz przyzwyczajenie w ich wykonywaniu.
- **Prowokacja sytuacyjna,** to stworzenie sytuacji, które wymagają od gracza samodzielnego rozwiązanie problemu i aktywności.

DLACZEGO GRY FASCYNUJĄ ?

Dobrowolność- gracz ma swobodę w podejmowaniu decyzji, czy ma ochotę na grę, czy nie;

Bezinteresowność- gry nie służą do zaspakajania życiowych konieczności;

Ograniczoność w czasie oraz przestrzeni a także odrębność;

Intensywność; powtarzalność akcji;

Podporządkowanie ograniczającym regułom;

Rywalizacyjny charakter;

Świadomość nierealności akcji.

PRZEJAWY AGRESJI TECHNICZNEJ

- POZYSKIWANIE DANYCH OSOBOWYCH bez wiedzy użytkownika, np. podczas wypełniania formularzy rejestracyjnych, formularzy zamówienia w sklepach internetowych;
- ZAGROŻENIA, gdy wchodzimy na niektóre strony internetowe, poprzez tzw. **cookies,** czyli pliki, które zapisywane są automatycznie na dysku twardym i gromadzące podstawowe dane o użytkowniku;
- PROGRAMY TYPU **SPYWARE** mające na celu śledzenie najważniejszych działań użytkownika;

PRZEJAWY AGRESJI TECHNICZNEJ

- **PHISHING** tzn. podszywanie się pod firmy, instytucje godne zaufania i wysyłanie wiadomości do użytkowników z prośbą o podanie pewnych pilnych danych. Często można spotkać się z tego typu praktyką w kontekście banków. Oszuści podszywają się pod nie i proszą o podanie hasła dostępu do konta w celu „weryfikacji rachunku" albo zmian systemowych (technicznych, programowych);
- wysyłanie niezamówionych informacji handlowych tzn. **spamów;**
- programy, które dokonują przełączenia modemowego użytkownika sieci bez jego wiedzy ze standardowego połączenia na droższe. Celem jest oczywiście zmuszenie konsumenta do płacenia wyższych rachunków telefonicznych. Cel ten osiąga przy pomocy tzw. **dialerów internetowych;**
- podejmowanie transakcji finansowych (zakupy on-line) przez dzieci;

PRZECIWDZIAŁANIE

- W celu przeciwdziałania problemowi cyberprzemocy i innym zagrożeniom związanym z korzystaniem przez dzieci z mediów elektronicznych w lutym 2007 roku w ramach kampanii „Dziecko w Sieci” powołany został:
- **Projekt** Helpline.org.pl. Pod adresem www.helpline.org.pl
- **bezpłatny numer telefonu 0 800 100 100** - mogą uzyskać pomoc zarówno najmłodsi i dorośli [rodzice oraz profesjonaliści].

ZABEZPIECZENIA TECHNICZNE

- Na polskim rynku istnieje szereg programów umożliwiających filtrowanie nielegalnych i szkodliwych treści w Internecie. Do najpopularniejszych zaliczymy: Benjamin, Cenzor, Motyl, Weblock, X-Guard II.
- Blokowanie stron niepożądanych (tzw. Czarna Lista) - osoba administrująca programem może stworzyć listę stron WWW, które uważa za niewłaściwe do oglądania przez młodszych użytkowników.
- Stworzenie tzw. Białej Listy czyli listy stron dozwolonych.
- Blokowanie komunikatorów (gg, skype, tlen i inne).

ZABEZPIECZENIA TECHNICZNE

- Blokowanie plików wykonywalnych EXE i plików MP3, które często są nośnikiem niewłaściwych treści.
- Blokowanie pobierania dokumentów.
- Blokowanie list dyskusyjnych.
- Blokowanie dostępu do poczty elektronicznej (POP3 i SMTP).
- Możliwość ustawienia limitu czasu na korzystanie z Internetu.
- Blokowanie wyszukiwarki grafiki.
- Blokowanie bramek SMS.

10 ZASAD KAŻDEGO INTERNAUTY

cz. 1

- 1. Aktualizować **system operacyjny** komputera (najlepiej automatycznie).
- 2. Zainstalować program antywirusowy i aktualizować go.
- 3. Włączyć **firewalla** i nie zmieniać bez potrzeby jego ustawień.
- 4. Nie otwierać listów od **nieznanych nadawców** i podejrzanych załączników.
- 5. Używać **haseł** trudnych do odszyfrowania (kombinacje dużych i małych liter, cyfr i znaków specjalnych).

10 ZASAD KAŻDEGO INTERNAUTY cz.2

- 6. Nigdy nie wysyłać haseł **drogą mailową**.
- 7. Przed dokonaniem **transakcji** w Internecie, upewnić się, że jesteśmy na właściwej stronie (szyfrowane strony zaczynają się od https: w adresie, certyfikat jest ważny, a przeglądarka wyświetla zamkniętą kłódkę - to znak, że połączenie jest bezpieczne).
- 8. Nie używać **poufnych danych** w kawiarenkach internetowych.
- 9. Nie wchodzić na **podejrzane strony** (można zainstalować bezpłatny program do oceny stron www).
- 10. Zachować zdrowy **rozsądek**.

ZALECENIA DLA PROFILAKTYKI WPŁYWÓW MEDIALNYCH

Działania skierowane do młodzieży:

- Doskonalenie umiejętności zarządzania czasem.
- Nauka samokontroli w korzystaniu z Internetu.
- Kształcenie umiejętności racjonalnego, selektywnego i refleksyjnego korzystania z mediów elektronicznych oraz nauka samodyscypliny w roli ich użytkownika.
- Kształtowanie świadomej, krytycznej i selektywnej postawy względem mediów.
- Dostarczenie wiedzy na temat zagrożeń wynikających z korzystania z sieci.
- Poznanie zasad kodeksu etycznego internauty.
- Nauka pokonywania nawyku biernego korzystania z Internetu(oglądactwo).

ZALECENIA DLA PROFILAKTYKI WPŁYWÓW MEDIALNYCH

Działania skierowane do młodzieży:

- Nauka, że Internet sam w sobie nie jest ani zły ani dobry. Jest narzędziem poznawania świata i uprzyjemniania i ułatwia życia, ale narzędzie dobrze służy tylko temu, kto wie w jakich okolicznościach i w jaki sposób należy się nim posługiwać.
- Nauka właściwego sposobu korzystania z for internetowych i serwisów społecznościowych.
- Ukazanie wartości typu: prywatność TAK, anonimowość NIE - indywidualne konta sieciowe.
- Uświadomienie, że uczniom, że każda aktywność jest monitorowana, że może być szybko i skutecznie zidentyfikowana, co eliminuje zakusy polegające na świadomym czy nieświadomym wyrządzeniu przykrości i stosowaniu cyberprzemocy.
- Edukacja medialna – przedmiot przyszłości.

ZALECENIA DLA PROFILAKTYKI WPŁYWÓW MEDIALNYCH

Działania skierowane do rodziców i nauczycieli:

- Nauka przestrzegania zasad dotyczących interakcji dziecko-media.
- Przekonanie rodziców i nauczycieli że korzystanie z komputera powinno odbywać się przy pełnym zachowaniu zasad higieny i z uwzględnieniem właściwości psychiki młodych ludzi.
- Dostarczanie wiedzy na temat wpływu mediów na kształtowanie się osobowości i zachowania młodzieży.
- Zachęcanie do refleksji nad medialnym stylem życia współczesnego człowieka.
- Przestrzeganie zasady wychowawczej, zgodnie z którą *wygra ten, kto połączy znajomość najnowszych technologii ze światem tradycyjnych wartości* (J. Santorski).

CO WARTO PRZECZYTAĆ?

- *Edukacja medialna w społeczeństwie informacyjnym* / pod red. Stanisława Juszczyka. Toruń : Wydaw. Adam Marszałek, 2002. (Multimedialna Biblioteka Pedagogiczna).
- *Media i edukacja w dobie integracji* / pod red. Wacława Strykowskiego, Wojciecha Skrzydlewskiego. Poznań : eMPi^2, 2002.
- *Media- przyjaciel czy wróg dziecka* ? / pod red. Wioletty Tuszyńskiej-Boguckiej . Poznań: wyd. eMPi2, 2006.