AKADEMIA LEONA KOŹMIŃSKIEGO

CBOS
Centrum Badania Opinii Społecznej

KOMUNIKAT Z BADAŃ

Warszawa, lipiec 2013

www.cbos.pl ● sekretariat@cbos.pl

BS/99/2013

OPINIE O BEZPIECZEŃSTWIE W INTERNECIE

Znak jakości przyznany CBOS przez Organizację Firm Badania Opinii i Rynku 11 stycznia 2013 roku

Fundacja Centrum Badania Opinii Społecznej
ul. Żurawia 4a, 00-503 Warszawa
e-mail: sekretariat@cbos.pl; info@cbos.pl
http://www.cbos.pl
(48 22) 629 35 69

Z roku na rok dostęp do internetu oraz innych usług telekomunikacyjnych staje się coraz bardziej powszechny. Dzieje się tak za sprawą wielu czynników – polityki rządu oraz regulacji prawnych, rozwoju technologicznego, konkurencji na wolnym rynku mediów, malejących cen itp. Posiadanie dostępu do sieci staje się wymogiem koniecznym dla dobrego funkcjonowania w życiu publicznym. Dotyczy to nie tylko osób prywatnych, a więc posiadaczy komputerów podłączonych do internetu, właścicieli telefonów komórkowych, smartfonów itp., ale również przedsiębiorstw oraz państwowych i społecznych instytucji, dających możliwość skorzystania z internetu w miejscu pracy. W tym kontekście mówi się także o ogólnej koncepcji e-urzędów, dzięki którym instytucje mogą łatwiej komunikować się między sobą, a petenci lub klienci uzyskują łatwiejszy kontakt z firmami oraz urzędami.

Za sprawą portali społecznościowych (możliwości utrzymywania kontaktów oraz nawiązywania nowych, komunikowania się, załatwiania spraw życia codziennego itp.) globalna sieć staje się ważną przestrzenią życia społecznego. Nietrudno jednak zauważyć, że internet ma również wiele oddziaływań negatywnych. Badacze podkreślają, że do sieci przenika wszystko to, co znamy z życia realnego, także zjawiska niepożądane. Należy więc wspomnieć o pedofilii, pornografii, złodziejstwie, różnego rodzaju przestępczości, terroryzmie itd. Biorąc pod uwagę coraz silniejszą zależność między światem realnym a wirtualnym oraz fakt, że w sieci stale zwiększa się ilość informacji, w tym mających kluczowe znaczenie dla bezpieczeństwa każdego z nas, właśnie do kwestii bezpieczeństwa przywiązywać trzeba coraz większą wagę.

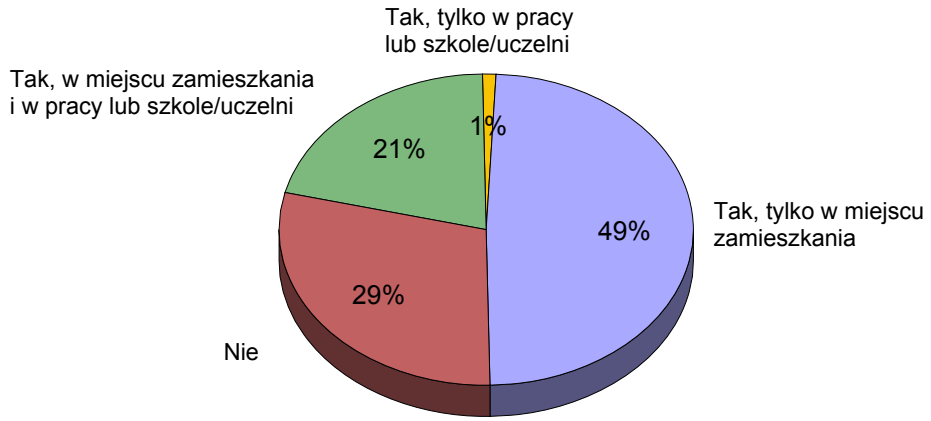
Celem naszego badania[1] było zbadanie postaw i opinii na temat realności zagrożeń takimi zjawiskami, jak: terroryzm, cyberterroryzm, hakerstwo, cyberwojna. Pytaliśmy o te sprawy w kontekście bezpieczeństwa państwa, firm, społeczeństwa oraz osób prywatnych.

[1] Badanie „Aktualne problemy i wydarzenia" (276) przeprowadzono w dniach 9–15 maja 2013 roku na liczącej 1101 osób reprezentatywnej próbie losowej dorosłych mieszkańców Polski. Prezentowany komunikat powstał jako rezultat umowy o współpracy między Fundacją CBOS a Akademią Leona Koźmińskiego. Umowa ta umożliwia studentom ALK systematyczny udział w badaniach opinii publicznej, realizowanych na reprezentatywnych próbach dorosłej ludności kraju. Studenci przygotowują projekty bloków pytań na wybrane przez siebie tematy, a następnie opracowują wyniki badania. Możliwość uczestnictwa w badaniach stanowi element studiów na ALK unikalny w skali nie tylko polskiej, ale i światowej. Niniejszy komunikat oraz badanie, na którym się opiera, zostały zaprojektowane i opracowane w ramach studiów socjologicznych na ALK, pod kierunkiem prof. dr. hab. Krzysztofa Zagórskiego.

Badani byli również proszeni m.in. o ocenę swoich umiejętności związanych z obsługą komputera i internetu. Prezentację wyników badania zaczynamy od kwestii dostępności sieci.

CBOS

RYS. 1. **CZY POSIADA PAN(I) STAŁY DOSTĘP DO INTERNETU?**

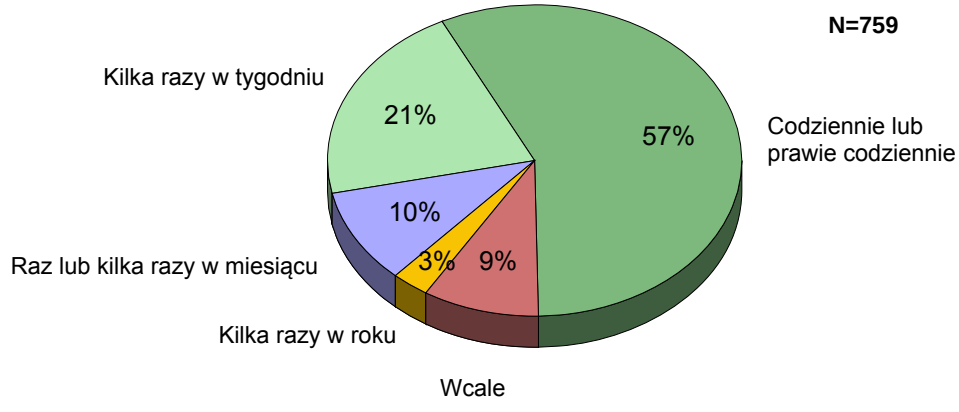


Blisko połowa dorosłych Polaków ma stały dostęp do internetu tylko w domu, a co piąty – zarówno w domu, jak i w pracy lub szkole. Możliwość korzystania z internetu wyłącznie w miejscu pracy lub w szkole ma 1% badanych. Można zatem powiedzieć, że stałym dostępem do sieci cieszy się 71% Polaków. Zbiorowość osób niemających w ogóle dostępu do internetu stanowi mniej niż jedną trzecią społeczeństwa (29%).

Kolejne pytania zadawaliśmy tylko tym osobom, które mają jakikolwiek dostęp do internetu. Najpierw ustaliliśmy częstość korzystania z sieci.

CBOS

RYS. 2. **JAK CZĘSTO (W PRZYBLIŻENIU) UŻYWAŁ(A) PAN(I) INTERNETU W CIĄGU OSTATNICH 12 MIESIĘCY?**



Ponad połowa respondentów mających dostęp do internetu (57%) korzysta z niego codziennie lub prawie codziennie, a ponad jedna piąta (21%) – kilka razy w tygodniu. Tak więc zdecydowana większość osób z omawianej grupy (78%) korzysta z internetu co najmniej kilka razy w tygodniu. Mniej więcej co ósmy badany mający dostęp do sieci (13%) korzysta z niej sporadycznie, a co jedenasty (9%) – w ogóle. Przypuszczalnie są to ci, którzy mają w domu dostęp do internetu, z którego korzystają inni członkowie rodziny.

Częstość korzystania z internetu wiąże się z oceną umiejętności posługiwania się nim.

Tabela 1

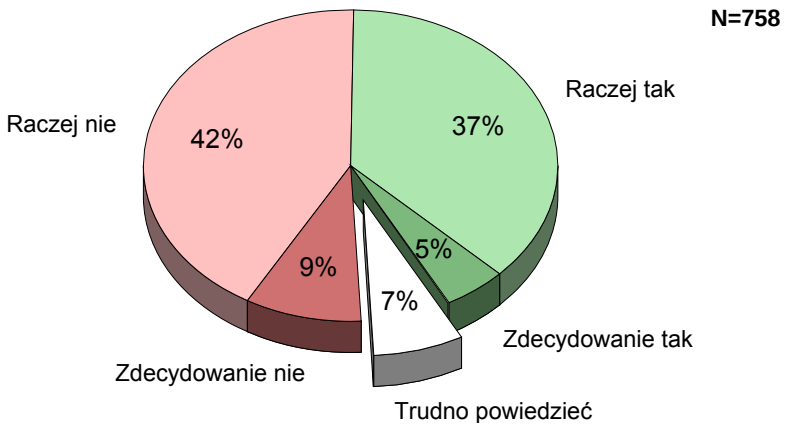
Proszę ocenić na skali od 1 do 5 swoje umiejętności wykorzystania poszczególnych usług i funkcji internetu	Bardzo źle	Źle	Tak sobie	Dobrze	Bardzo dobrze
	w procentach				
Gry komputerowe z innymi internautami	31	22	18	16	13
Obsługa programów komputerowych zabezpieczających komputer, np. przed wirusami (zapora sieciowa, antywirus)	24	13	24	22	17
Korzystanie z portali społecznościowych (np. Facebook)	20	12	19	23	26
Robienie zakupów przez internet (np. Allegro)	20	11	17	25	27
Korzystanie z baz danych	19	13	28	25	15
Rozmowy z transmisją obrazu i/lub dźwięku (np. Skype)	18	11	18	25	28
Prowadzenie korespondencji (np. e-mail)	15	9	16	27	33
Korzystanie z wyszukiwarki internetowej (np. Google)	9	3	23	31	33

Spośród aktywności związanych z internetem najgorzej wypada granie w gry komputerowe z innymi internautami. Prawie co trzeci badany ocenił swoje umiejętności bardzo źle, a ponad jedna piąta – źle. Być może dlatego, że niewielu polskich internautów gra poprzez sieć. Drugą w kolejności najgorzej ocenianą umiejętnością jest obsługa programów zabezpieczających komputer. Wachlarz dostępnych programów tego typu jest zróżnicowany i są one kluczowe z punktu widzenia bezpieczeństwa komputerów. Blisko jedna czwarta badanych bardzo źle oceniła swoje umiejętności w tym zakresie, a mniej więcej co ósmy – źle. Łącznie więc za niedostateczną w tej dziedzinie należy uznać wiedzę ponad jednej trzeciej internautów. Z kolei wśród najlepiej ocenianych umiejętności znalazło się korzystanie z wyszukiwarki internetowej (33% wskazań „bardzo dobrze", 31% „dobrze") oraz prowadzenie korespondencji e-mail (33% „bardzo dobrze", 27% „dobrze").

Opinie na temat tego, czy przesyłanie, wymiana informacji oraz korzystanie z nich w internecie jest bezpieczne, są podzielone. Przeważa jednak pogląd, że internet nie jest bezpieczny.

CBOS

RYS. 3. **CZY UWAŻA PAN(I), ŻE PRZESYŁANIE, WYMIANA I KORZYSTANIE Z INFORMACJI W INTERNECIE JEST BZPIECZNE?**

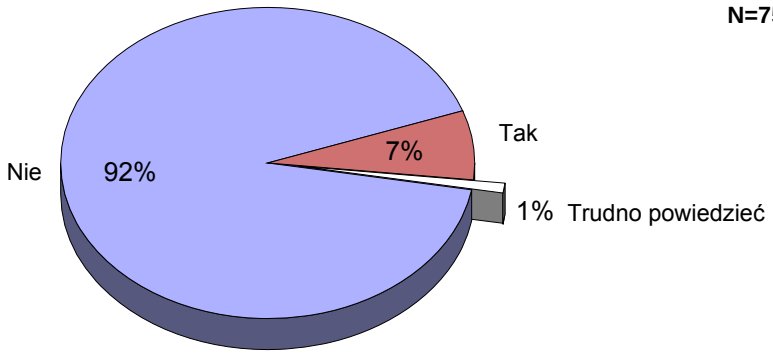


Połowa badanych (51%) twierdzi, że wykonywanie w internecie czynności związanych z wymianą informacji nie należy do bezpiecznych (w tym 42% uważa, iż jest to raczej niebezpieczne). Przeciwną opinię wyraża 42% respondentów (w tym 37% sądzi, że jest to raczej bezpieczne).

Mimo iż przeważa przekonanie o niebezpieczeństwach związanych z korzystaniem z sieci, 92% badanych deklaruje, że nigdy nie padło ofiarą przestępstwa internetowego (kradzieży, oszustwa, włamania do komputera itp.). Jedynie nieliczni (7%) twierdzą, że byli ofiarami któregoś z przestępstw. Nasuwa się więc pytanie, skąd tyle negatywnych opinii o bezpieczeństwie poruszania się w sieci.

CBOS

RYS. 4. . **CZY BYŁ(A) PAN(I) KIEDYŚ OFIARĄ PRZESTĘPSTWA INTERNETOWEGO, JAK KRADZIEŻY DANYCH, OSZUSTWA (NP. PRZY ZAKUPACH INTERNETOWYCH), WŁAMANIA DO KOMPUTERA ITP.?**



Interesująca jest zależność między przekonaniem o byciu ofiarą komputerowego przestępstwa a umiejętnością posługiwania się programami zabezpieczającymi.

Tabela 2

Czy był(a) Pan(i) kiedyś ofiarą przestępstwa internetowego, jak kradzieży danych, oszustwa (np. przy zakupach internetowych), włamania do komputera itp.?	Proszę ocenić na skali od 1 do 5 swoje umiejętności obsługi programów komputerowych zabezpieczających komputer, np. przed wirusami (zapora sieciowa, antywirus).				
	Bardzo źle	Źle	Tak sobie	Dobrze	Bardzo dobrze
	w procentach				
Tak	4	5	7	9	15
Nie	94	95	93	91	85
Nie wiem	2	0	0	0	0
Ogółem	100	100	100	100	100

Ci, którzy źle lub bardzo źle oceniają swoje umiejętności posługiwania się programami zabezpieczającymi komputer, na ogół twierdzą, że nigdy nie padli ofiarą przestępstw internetowych (94%–95%). Wśród osób dobrze lub bardzo dobrze oceniających swoje umiejętności w tym względzie odsetki te są niewiele mniejsze. Może to potwierdzać hipotezę, że osoby słabiej znające się na zabezpieczeniach komputera oraz zagrożeniach w sieci po prostu nie są świadome tego, że ich komputer może być zainfekowany, np. wirusem, który wykorzystuje go do rozsyłania spamu. Możliwe jest też, że ofiary przestępstwa uczą się później zapobiegania mu, a więc nabywają umiejętności w tym względzie. Stwierdzenie kierunku tej zależności wymagałoby dodatkowych badań.

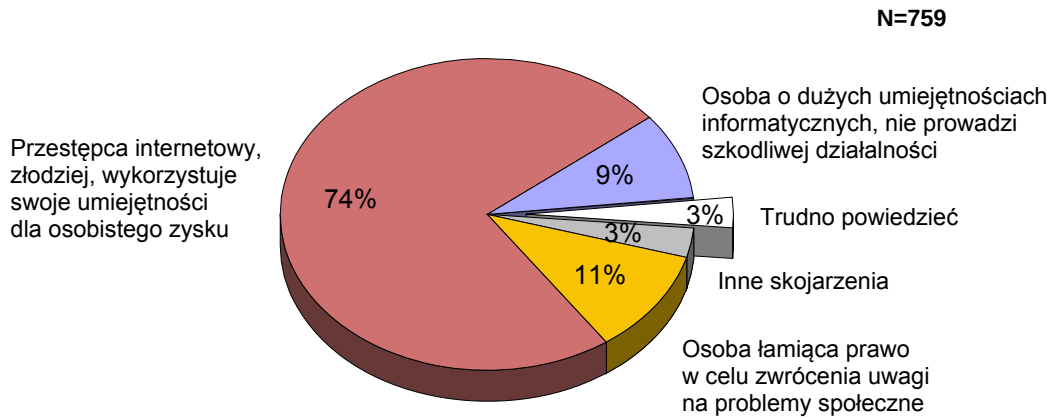
Pierwotnie określenie „haker" było zarezerwowane dla osób o bardzo wysokich kwalifikacjach i wszechstronnej wiedzy z zakresu informatyki. Haker potrafił znaleźć luki w systemie informatycznym, naprawić, stworzyć program, który będzie je łatał lub wykorzystywał. Znaczenie tego terminu było wówczas neutralne, a nawet pozytywne, gdyż hakerzy nie łamali prawa. W środowisku informatyków, hakerów lub po prostu tych, którzy interesują się informatyką, przyjęto, że osoby wykorzystujące swoje ponadprzeciętne umiejętności informatyczne do osiągania prywatnej korzyści (np. okradanie kont bankowych, wykradanie informacji itp.) określa się mianem krakerów, wandali lub *script kids*. Ten ostatni termin odnosi się przede wszystkim do osób nastoletnich, które często wykorzystują swoje umiejętności nieświadome odpowiedzialności za swoje czyny. Charakteryzują się one również brakiem przewidywalności, gdyż na ogół kieruje nimi ciekawość. Słowo „haker" nabrało pejoratywnego znaczenia, gdy elitarne umiejętności hakerów stawały się coraz bardziej powszechne wśród coraz młodszych użytkowników komputerów. Jednak równolegle

coraz powszechniejsze było podszywanie się internetowych przestępców pod hakerów. Obraz ten zaburzają również media, które na ogół mało precyzyjnie podchodzą do tego zjawiska, określając każde zdarzenie – atak, włamanie czy kradzież – jako dokonane przez hakerów.

Przeprowadzone badanie potwierdza stereotyp hakera, jaki utrwalił się w świadomości społecznej. Trzy czwarte respondentów (74%) uważa, że haker to, ogólnie mówiąc, przestępca internetowy, który wykorzystuje swoje umiejętności dla osobistego zysku. Co dziewiąty (11%) sądzi, że haker to osoba łamiąca prawo, ale motywem jej działania jest zwrócenie uwagi na problemy społeczne. Niewiele mniejsza grupa (9%) zgadza się ze stwierdzeniem, że haker to osoba o dużych umiejętnościach informatycznych, która nie prowadzi szkodliwej działalności.

CBOS

RYS. 5. **Z CZYM KOJARZY SIĘ PANU(I) SŁOWO HAKER?**



Zagrożenia płynące z internetu, w tym cyberterroryzm, przeważnie uważane są za realne. Co jednak ciekawe, internauci częściej dostrzegają zagrożenia dla firm, dużych korporacji i instytucji państwowych niż dla społeczeństwa lub osób prywatnych.

Tabela 3

Czy uważa Pan(i) przestępstwa internetowe, w tym cyberterroryzm, za realne zagrożenie dla:	Tak	Nie	Trudno powiedzieć
	w procentach		
– firm i dużych korporacji	89	7	4
– państwa, instytucji państwowych	84	12	4
– społeczeństwa	78	16	5
– pojedynczych osób	74	21	5

Prawie 90% badanych mających dostęp do sieci uważa, iż przestępstwa internetowe stanowią realne zagrożenie dla różnego rodzaju przedsiębiorstw oraz instytucji państwowych, tylko nieznacznie mniej dostrzega takie zagrożenia dla społeczeństwa i osób prywatnych. Poczucie zagrożenia jest więc duże. Wynik ten jest o tyle ciekawy, iż w tym samym badaniu 92% internautów zadeklarowało, że nie było ofiarą internetowych przestępstw. Wpływ na odpowiedzi mogły mieć jednak doniesienia medialne, które w ostatnich latach często przynoszą informacje o atakach internetowych przestępców, „hakerów" itp., także na arenie międzynarodowej. Szczególnie głośno jest o hakerach (trzymając się terminologii mediów) z Chin. Według licznych specjalistów oraz naukowców z zakresu informatyki, obronności czy bezpieczeństwa, cyberterroryzm na razie obecny jest głównie w internetowej komunikacji i propagandzie, a mało jest rzeczywistych ataków cybernetycznych. Nie oznacza to, że zagrożenia nie ma. Podkreśla się fakt, iż coraz bardziej powszechna wiedza oraz nowe technologie stają się dostępne również dla terrorystów.

Czy dzięki prowadzonej polityce bezpieczeństwa i stosowanym technologiom nasz kraj i jego obywatele są dobrze chronieni przed zagrożeniem cyberwojną, cyberterroryzmem oraz ogólnie terroryzmem? Badani zdecydowanie najgorzej oceniają zabezpieczenie przed cyberterroryzmem i cyberwojną, natomiast lepiej – bezpieczeństwo w kontekście zwykłego terroryzmu.

Tabela 4

Czy uważa Pan(i), że dzięki prowadzonej polityce bezpieczeństwa i stosowanym technologiom nasz kraj i jego obywatele są dobrze chronieni przed:	Tak	Nie	Trudno powiedzieć
	w procentach		
– cyberwojną	25	45	30
– cyberterroryzmem	29	51	20
– terroryzmem ogólnie	43	45	13

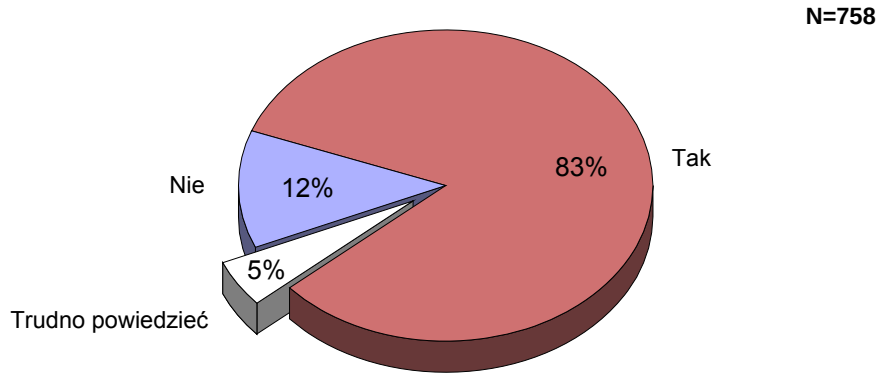
Jak widać, stopień bezpieczeństwa dla wyżej wymienionych zagrożeń oceniany jest nie najlepiej. Może to być spowodowane kilkoma czynnikami. Trudno przy tym mówić o wpływie przykrych doświadczeń z ostatnich lat, gdyż żadne z omawianych zjawisk nie miało miejsca w Polsce. Jednym z prawdopodobnych wyjaśnień może być znikoma aktywność instytucji oraz służb odpowiedzialnych za zapewnienie bezpieczeństwa w sferze informacyjnej. Poza informacjami podawanymi na stronach internetowych tych instytucji (np. ABW, CERT) raczej trudno jest dowiedzieć się czegokolwiek z przekazów medialnych, zwłaszcza z telewizji. Instytucje te nie są skore do informowania na bieżąco opinii publicznej o prowadzonych działaniach, których celem byłoby podnoszenie poziomu bezpieczeństwa

państwa oraz jego obywateli. Polacy nie mają zatem łatwo dostępnych informacji o tym, czy mogą czuć się bezpiecznie.

Zdecydowana większość badanych mających dostęp do internetu (83%) uważa, że zagrożenia występujące w sieci mogą mieć realne skutki w życiu codziennym.

CBOS

RYS. 6. **CZY UWAŻA PAN(I), ŻE ZAGROŻENIA ZWIĄZANE Z INTERNETEM MOGĄ MIEĆ REALNE SKUTKI W ŻYCIU CODZIENNYM?**



★

★ ★

Podsumowując można powiedzieć, że cyberzagrożenia, w tym cyberterroryzm oraz cyberwojna, uznawane są przez internautów za realne zagrożenie, a przede wszystkim za powód do obaw o bezpieczeństwo państwa oraz firm i korporacji. Opinie co do poziomu prewencyjnych działań państwa są podzielone, dominuje jednak ocena negatywna. Polscy internauci niezbyt dobrze oceniają swoje umiejętności związane z obsługą programów zabezpieczających komputery, ale są przekonani, że nie padli ofiarą przestępstw w sieci. Niezależnie od tego, korzystanie z internetu jest przez nich uznawane za niebezpieczne. Co więcej, dominuje wśród nich opinia, że zagrożenia występujące w sieci mogą się przekładać na codzienne życie w realnym świecie.

Opracował

Jakub FRYŁOW