**NAUKA** 4/2010 • 31-42

**RYSZARD TADEUSIEWICZ**

# Zagrożenia w cyberprzestrzeni

## 1. Postawienie problemu

O tym, że mamy na przełomie XX i XXI wieku do czynienia z rewolucją informatyczną, wie każde dziecko. Wszechobecne komputery, towarzyszące nam praktycznie na wszystkich stanowiskach pracy, w szkołach, w szpitalach, w samochodach i na lotniskach, w domach, w miejscach rozrywki (na przykład jako „serca" automatów do gier albo systemy sterujące światłami w operze), a nawet chodzące z nami krok w krok w postaci procesorów wbudowanych w telefony komórkowe – są owocem tej właśnie rewolucji. Informatyka decyduje dziś o tym, jak pracujemy i jak odpoczywamy, a jej rola we wszystkich dziedzinach, w których jest stosowana, ustawicznie rośnie. W szczególności Internet jest czymś więcej, niż po prostu jeszcze jednym środkiem komunikacji czy też (jak to się często formułuje) – nowym medium informacyjnym. W sposób całkiem bezprecedensowy już w dziesięć lat po powszechnym udostępnieniu [1] stał się on stosem pacierzowym nowej formacji społeczno-ekonomicznej, zwanej społeczeństwem informacyjnym. Żadne inne narzędzie techniczne w dziejach nie miało tak doniosłych konsekwencji społecznych!

Oczywiście są konkretne przyczyny tego stanu rzeczy. Komputery usprawniają i ułatwiają wykonywanie dowolnych prac, a Internet oferuje nieprzebrane bogactwo informacji na praktycznie każdy temat oraz łączy ludzi w sposób, którego nie zapewniał żaden wcześniej stosowany środek komunikacji. Z pomocą Internetu mogą wymieniać myśli i poglądy osoby o różnym poziomie wykształcenia i statusie społecznym, często należące do różnych kultur, używające różnych języków i przywiązane do różnych religii. Internet jest ważnym obiektem w rzeczywistości XXI wieku, gdyż jego powstanie zdynamizowało trwające od blisko dwustu lat procesy społeczno-ekonomiczne, których cechą było stałe zwiększanie się znaczenia zadań tworzenia i przetwarzania **informacji**, przy malejącym zaangażowaniu ludzi w realizację zadań **produkcji** rolnej i przemysłowej. Procesy te mają charakter trwały, ponieważ postępy wiedzy

* Prof. dr hab. Ryszard Tadeusiewicz, członek korespondent PAN, Akademia Górniczo-Hutnicza, Kraków

[1] Wcześniej sieć, której bezpośrednim „spadkobiercą" jest Internet, była wykorzystywana do celów wojskowych (jako tak zwany Arpanet), a potem jako sieć komputerowa udostępniona wyłącznie do zastosowań akademickich.

agrobiologicznej oraz rosnąca mechanizacja rolnictwa umożliwiają bardzo wydajne produkowanie żywności nawet dla szybko wzrastających populacji przy minimalnym zapotrzebowaniu na pracę związanych z tym zawodem ludzi, zaś rozwijająca się automatyzacja przemysłu pozwala na zaspokajanie rosnących potrzeb materialnych całego społeczeństwa, również przez coraz mniejszy odsetek ludzi zatrudnionych bezpośrednio w proces wytwarzania dóbr. Usługi niezwiązane z informacją rozwijały się w okresach wzrostu gospodarczego, zaś zatrudnienie w tym sektorze malało w czasie trudnym dla gospodarki. Natomiast sektor związany z produkcją, przetwarzaniem, gromadzeniem i przesyłaniem informacji na przestrzeni ostatnich dziesiątków lat stale i silnie rośnie.

Wskazane procesy skutkują między innymi tym, że szeroko rozumiana cyberprzestrzeń[2] staje się nie tylko miejscem, gdzie ludzie pracują, zdobywają wiedzę, komunikują się ze sobą, a także poszukują rozrywki – ale również stała się miejscem, w którym ludzie są wystawieni na różne zagrożenia. Zagrożenia te dotyczą możliwości kradzieży informacji (co naraża okradaną stronę na straty), możliwości celowego i nielegalnego zmieniania informacji (co zaburza tę sferę aktywności zawodowej lub prywatnej, która jest uzależniona od prawdziwości i aktualności informacji, które zostały zmienione), możliwość ograniczania dostępu do informacji aż do całkowitej blokady włącznie (co może sparaliżować pewne sfery działania z katastrofalnymi niekiedy skutkami) itp. Kolekcja zagrożeń, na jakie może być wystawiony każdy użytkownik cyberprzestrzeni, jest bardzo duża, a skala ich szkodliwości ustawicznie rośnie w związku ze zjawiskiem narastającej migracji do cyberprzestrzeni, zatem żeby nadać dalszym rozważaniom bardziej konkretny wymiar, dokonamy krótkiej oceny skali tej migracji.

## 2. Skala migracji do cyberprzestrzeni – ujęcie globalne

Procesy informacyjne są więc obecnie – bez wątpienia będą także w ciągu najbliższych lat – głównym motorem gospodarki XXI wieku, a Internet, który je napędza, jest najważniejszym narzędziem, jakie stworzono w całym okresie rozwoju cywilizacji. Warto przyjrzeć się statystyce pokazującej liczbę oraz procentowy udział ludzi korzystających z Internetu w różnych regionach świata oraz prezentującej dynamikę wzrostu w tym zakresie (tabela na podstawie www.internetworldstats.com/stats.htm), żeby zdać sobie sprawę ze skali społecznej procesu migracji ludzi do cyberprzestrzeni oraz z rozkładu geograficznego tego zjawiska.

[2] Tym terminem określa się zwykle ogół narzędzi sprzętowych i programowych związanych z technikami gromadzenia, przetwarzania, przesyłania i udostępniania informacji, wykorzystywanych przez ludzi do pozyskiwania wiedzy oraz do komunikacji z innymi ludźmi. Najważniejszym, chociaż nie jedynym, składnikiem cyberprzestrzeni jest obecnie Internet.

Tabela 1. Udział użytkowników Internetu w populacji poszczególnych regionów świata

| Regiony świata | Populacja (2009) | Liczba użytkowników Internetu (2009) | Odsetek internautów w społeczeństwie | Użytkownicy z danego regionu jako część światowej populacji internautów |
|---|---|---|---|---|
| Europa | 803 850 858 | 425 773 571 | 53,0% | 23,6% |
| Ameryka Północna | 340 831 831 | 259 561 000 | 76,2% | 14,4% |
| Afryka | 991 002 342 | 86 217 900 | 8,7% | 4,8% |
| Azja | 3 808 070 503 | 764 435 900 | 20,1% | 42,4% |
| Środkowy Wschód | 202 687 005 | 58 309 546 | 28,8% | 3,2% |
| Ameryka Łacińska | 586 662 468 | 186 922 050 | 31,9% | 10,4% |
| Australia i Oceania | 34 700 201 | 21 110 490 | 60,8% | 1,2% |
| ŚWIAT OGÓŁEM | 6 767 805 208 | 1 802 330 457 | 26,6% | 100,0% |

Odnotujmy kilka znamiennych zjawisk. Europa jest dobrze umiejscowiona w cyberprzestrzeni, ale jest wciąż słabiej nasycona dostępem do Internetu niż Ameryka Północna (53% internautów w Europie w stosunku do 76% w Ameryce). Co więcej, ustępujemy pod tym względem także mieszkańcom Australii i Oceanii (prawie 61%)! Tempo migracji do cyberprzestrzeni w ostatniej dekadzie było w Europie dość duże (ponad 300% wzrostu liczby internautów w stosunku do 140% w Ameryce), ale i tak jest odległe od tempa osiąganego przez Afrykę czy Środkowy Wschód (ponad półtora tysiąca procent!). Nasz kontynent zamieszkuje prawie 24% internautów świata, ale to niewiele w stosunku do ponad 40% wywodzących się z Azji. Ciekawych spostrzeżeń i wniosków z tej tabeli można by było wyciągnąć więcej, ale nie taki jest cel tego referatu. Tezą, którą usiłuję wykazać, jest stwierdzenie, że migracja ludzi do cyberprzestrzeni ma charakter autentycznie masowy, a to powoduje, że zagrożenia (opisane dalej), jakie na tych ludzi czekają w kontekście używania systemów teleinformatycznych, nie są błahe.

## 3. Sytuacja w Polsce

Rozwój Internetu i związanego z nim społeczeństwa informacyjnego w Polsce biegnie podobnie jak w pozostałych krajach Europy, chociaż ze względu na początkowe zacofanie polskiej infrastruktury telekomunikacyjnej stan społecznego nasycenia technikami teleinformatycznymi pozostawia jeszcze wiele do życzenia. Niemniej dane analogiczne do zgromadzonych w tabeli 1 odniesione do Polski wyglądają następująco (dane z http://www.internetstats.pl/index.php/baza-wskaznikow/liczba-internautow/):

Tabela 2. Udział polskich użytkowników Internetu w populacji kraju i świata

| Populacja (2009) | Liczba użytkowników Internetu (2009) | Odsetek internautów w społeczeństwie | Użytkownicy z Polski jako część internautów świata |
|---|---|---|---|
| 38 155 000 | 17 300 000 | 45,3% | 0,9% |

Jak wynika z podanego zestawienia, odsetek osób, których dotyczą problemy związane z zagrożeniami powstającymi w cyberprzestrzeni, jest w Polsce nieco mniejszy niż przeciętna europejska, ale blisko dwa razy większy niż średnia dla całego świata. Dodatkowe światło na rozważany problem rzuca raport ABW dotyczący zdarzających się w Polsce ataków hakerów. Na początku bieżącego roku prasę polską obiegły artykuły pod znamiennymi tytułami: *Polska jest w światowej czołówce krajów nękanych przez hakerów.* Pisał o tym w „Dzienniku Zachodnim" Agaton Koziński (20.01.2010), pisali także inni autorzy w innych periodykach, powołując się na raport ABW. Do samego raportu nie udało się dotrzeć, ale z omówień wynika, że liczba ataków (zwłaszcza mających formę tak zwanego *phishingu*, czyli wyłudzanie tajnych informacji osobistych) na prywatne adresy e-mail w Polsce w ostatnich miesiącach tak się nasiliła, że stawia nas to w tym zakresie na jednym z czołowych miejsc na świecie (z niektórych oszacowań wynika, że mamy w tej niechlubnej konkurencji miejsce trzecie).

## 4. Czy zagrożenia w cyberprzestrzeni mają duże znaczenie?

Rozważając problem zagrożeń wiążących się z powszechnym używaniem komputerów, możemy się spotkać z opiniami, że nie są to zagrożenia szczególnie ważne, gdyż w przypadku systemów cywilnych nikt nie może być fizycznie poszkodowany i doznać uszczerbku na życiu i zdrowiu na skutek ataku hakera czy przechwycenia jakichś informacji. Nie jest to trafna argumentacja, ponieważ ataki hakerów na niektóre cywilne systemy informatyczne **mogą** sprowadzić bezpośrednie zagrożenie dla życia i zdrowia ludzi – by wspomnieć tylko o systemach szpitalnych sterujących na przykład przebiegiem operacji telechirurgicznych albo o systemach sterowania ruchem lotniczym.

Jednak nie trzeba odwoływać się do aż tak krańcowych przykładów, by stwierdzić, że żadnych zagrożeń występujących w cyberprzestrzeni nie powinno się lekceważyć. Jest tak, ponieważ przy ocenianiu skutków tych zagrożeń trzeba brać pod uwagę efekt skali, który multiplikuje szkodliwość nawet tych na pozór mało groźnych zagrożeń. W celu uzasadnienia tej tezy weźmy pod uwagę pozornie niewinny problem tak zwanych spamów. Jak pewnie wszyscy wiedzą, ta dziwna nazwa obejmuje wszelkie wiadomości tekstowe (a ostatnio także obrazowe), które otrzymujemy jako listy email albo jako wiadomości z naszych elektronicznych komunikatorów, chociaż ich wcale nie chcemy. Takich niepotrzebnych i niechcianych wiadomości krążą w Internecie

miliony, coraz częściej spamy pojawiają się także niechcianych wiadomości jako SMS-y w komórkach.

Zjawisko spamów bierze się stąd, że w systemach informatycznych każda wiadomość jest łatwa do powielania, więc z równą łatwością wysyła się list do jednej osoby, jak i do setek czy tysięcy ludzi. No więc skoro można, to ludzie wysyłają takie masowe paczki listów. Jedni to robią z głupoty (nie zdając sobie sprawy ze szkodliwości tego działania), inni z chęci zysku (reklamy i różne oszukańcze ogłoszenia), jeszcze inni – z czystej złośliwości. I spam rośnie.

Jest to – powtórzmy – bez wątpienia najmniej uciążliwe spośród licznych cyberprzestrzennych zagrożeń. A jednak przy uwzględnieniu skali można pokazać, że nawet te pozornie mało groźne spamy są bardziej szkodliwe niż morderczy huragan. Na pozór stwierdzenie przytoczone wyżej wydaje się grubą przesadą. Jednak przyjrzyjmy się sprawie dokładniej. Każda taka niepotrzebnie (a czasem złośliwie) szeroko rozesłana wiadomość jest źródłem kłopotów dla tych odbiorców, którzy jej nie chcą i nie potrzebują. Każdy taki elektroniczny śmieć trzeba najpierw obejrzeć, zanim się go wyrzuci – a to **zajmuje czas**. Są wprawdzie programy, które automatycznie filtrują nadchodzące wiadomości, usiłując zgadnąć, które są przydatne dla użytkownika, a które są spamami, ale wszystkie te programy mają wspólną wadę: sporo SPAM-ów jednak przepuszczają, za to czasem „wytną" jakąś potrzebną wiadomość, co potem rodzi kłopoty, gdy nadawca czeka na odpowiedź, a odbiorca listu nie przeczytał z powodu nadgorliwości filtru antyspam.

## 5. Inspirujące porównanie

Szacuje się, że przynajmniej 70% krążących w Internecie wiadomości to spamy. Zatykają one łącza, powodują niepotrzebne straty energii, ale głównie – okradają odbiorców z czasu. Jak bardzo jest to szkodliwe, może unaocznić pewne wyliczenie, które wymyślił nasz rodak, prof. Koczkodaj z Kanady.

Otóż porównał on utratę czasu, na jaką spamy narażają miliony internautów na całym świecie – z utratą czasu (życia) spowodowaną przez huragan Katrina, który nawiedził USA w 2005 roku. Huragan ten zabił 1836 osób. Zabił, to znaczy pozbawił tego czasu, który mogliby przeżyć, gdyby nie ten kataklizm. Biorąc pod uwagę znaną ze statystyk średnią długość życia (większą dla kobiet i krótszą dla mężczyzn) i znając wiek ofiar, można wyliczyć, ile czasu ukradł im huragan. Wykonano odpowiednie obliczenia i okazało się, że było to 71 145 lat. Liczba ta staje się jeszcze bardziej przerażająca, gdy się ją wyrazi w sekundach: morderczy żywioł zabrał 2 245 165 452 000 sekund ludzkiego życia.

Jeśli jednak tę liczbę podzielić przez liczbę ludzi, którym na całym świecie kradną czas spamy (jak wynika z tabeli 1 pod koniec 2009 było tych ludzi dokładnie

1 802 330 457), to okazuje się, że na jednego internautę przypada zaledwie około 20 minut. Zaledwie! A przecież przeciętny odbiorca poczty elektronicznej traci co tydzień więcej niż pół godziny na walkę ze spamami. Traci ten czas bezpowrotnie, podczas gdy jego chwile na tym świecie są policzone. Więc patrząc na skutki, możemy powiedzieć, że co tydzień przez światową sieć informatyczną przetacza się huragan o sile porównywalnej z Katriną, okradając ludzi z ich czasu.

## 6. Przyczyny zagrożeń i możliwości ich eliminacji

### 6.1. Zagrożenia techniczne

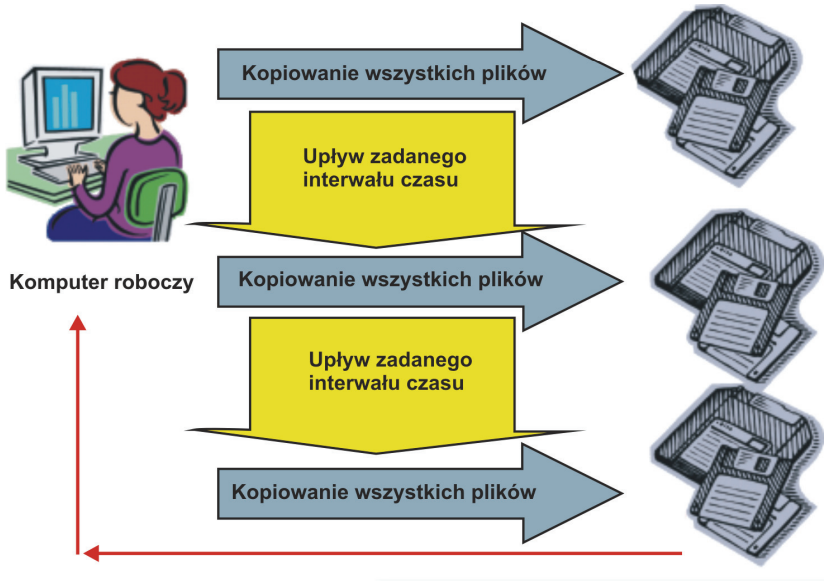
Ustaliwszy, że problemu zagrożeń w cyberprzestrzeni nie powinno się ignorować, możemy teraz spróbować przeanalizować przyczyny tych zagrożeń. Generalnie źródłem zagrożeń występujących w cyberprzestrzeni może być technika albo ludzie. Zagrożenia leżące po stronie techniki są oczywiście poważne, gdyż awaria komputera może unieruchomić działalność ważnej instytucji (na przykład banku), pozbawiając ją spodziewanych zysków i prestiżu – ale nie jest to najpoważniejszy problem, bowiem w dobrze zbudowanym systemie informatycznym zasadnicze elementy powinny być zdublowane. Awaria komputera roboczego powoduje, że pracę przejmuje komputer zapasowy, więc ciągłość działania jest niezagrożona, co najwyżej można mówić o spadku wydajności przetwarzania danych (komputer zapasowy ma często mniejszą moc obliczeniową niż ten podstawowy). Przykładem systemu mającego od strony technicznej bardzo wysoki poziom zabezpieczenia przed skutkami awarii jest komputer Tandem S70006 zawierający 6 procesorów, zwany komputerem „produkcyjnym", będący „sercem" systemu WARSET obsługującego warszawską Giełdę Papierów Wartościowych. Jego pracę dubluje komputer Tandem S70004 zawierający 4 procesory, zwany komputerem „zapasowym". Taka architektura systemu z dwoma niezależnymi jednostkami (powtarzaną architekturą „bezpieczeństwa"), z dublującymi się wszystkimi danymi gwarantuje niezawodność bliską 100%, przejawiającą się w odporności zarówno na błędy sprzętowe, jak i związane z oprogramowaniem. Oczywiście nie zawsze i nie wszędzie konieczne jest stosowanie aż tak wysokiego poziomu zabezpieczeń, ale ważna jest świadomość, że jeśli zachodzi potrzeba, to można uzyskać dowolnie wysoki poziom bezpieczeństwa technicznego systemu informatycznego.

Odrębnym zagadnieniem jest kwestia bezpieczeństwa danych. W każdym systemie informatycznym po krótkim nawet czasie jego eksploatacji wytwarza się sytuacja polegająca na tym, że dane zgromadzone w pamięci komputera są warte znacznie więcej niż komputer jako taki. Tymczasem te dane mogą zostać utracone na skutek awarii technicznej (fizyczne uszkodzenie dysku), na skutek wadliwego oprogramowania albo na skutek błędnego działania ludzi obsługujących system. Przed fizycznymi

uszkodzeniami nośnika danych można się chronić stosując zamiast pojedynczego dysku macierz dyskową tupu RAID. Jednak nie chroni to przed innymi przyczynami, które mogą spowodować utratę cennych danych. Dlatego dla zabezpieczenia danych stosować trzeba metody tworzenia kopii bezpieczeństwa (backup). Nie rozwijając tego tematu, warto wskazać, że kopie zapasowe można podzielić ze względu na strategie dodawania plików do tworzonej kopii na:

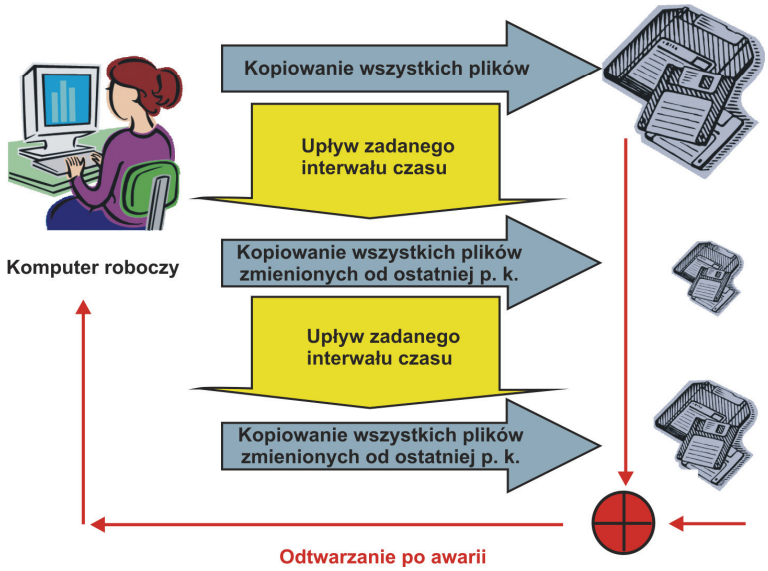
- kopie pełne (rys. 1);
- kopie przyrostowe (rys. 2);
- kopie różnicowe (rys. 3).

Kopie pełne są najbardziej kłopotliwe w sporządzaniu, ale dają możliwość najszybszego odzyskania sprawności systemu po awarii, natomiast pozostałe strategie charakteryzują się tym, że w coraz mniejszym stopniu obciążają administratorów systemu dodatkową pracą związaną z tworzeniem tych kopii, ale też coraz bardziej kłopotliwe jest odzyskanie danych, gdy już (niestety) nastąpi awaria.

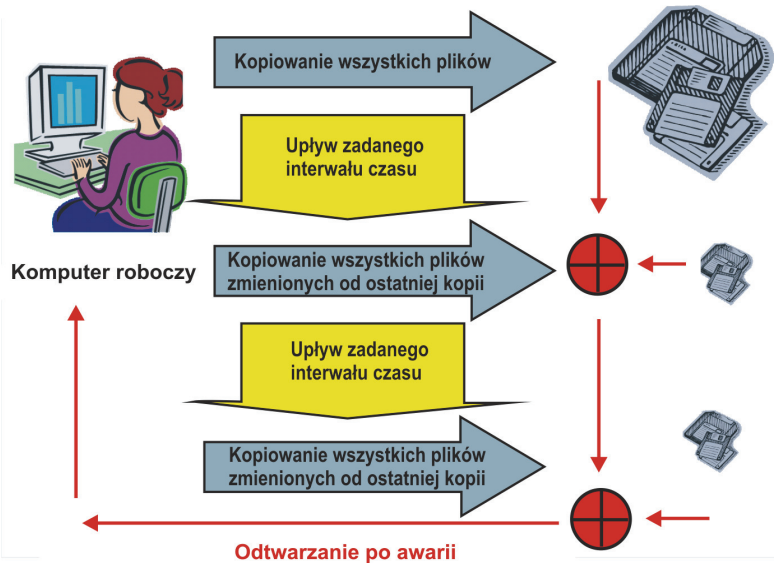



Rys. 1. Tworzenie i wykorzystanie kopii pełnej

Do sfery zagrożeń technicznych należą także zagrożenia związane z możliwością utraty zasilania. Uważa się za zasadę, że ważne systemy informatyczne muszą być niezależne od awarii sieci energetycznej i muszą mieć awaryjne zasilanie w postaci układów UPS lub generatora spalinowego napędzającego prądnicę, pozwalającego na dłuższy czas pracy autonomicznej.



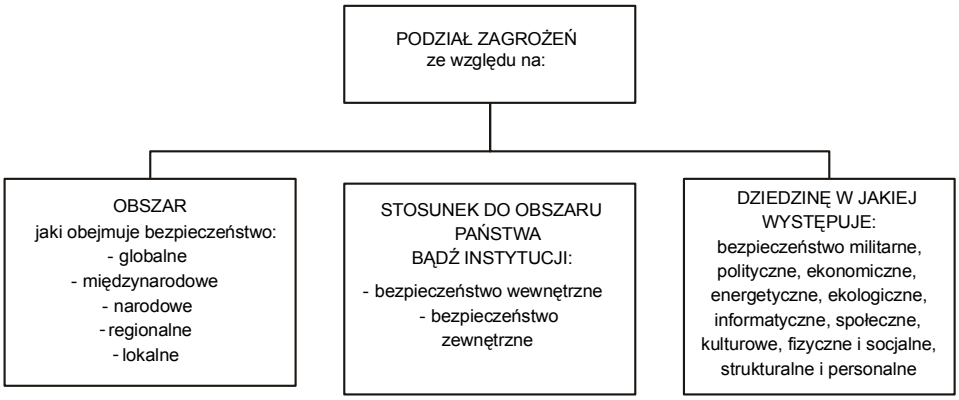

Rys. 2. Tworzenie i wykorzystanie kopii przyrostowej




Rys. 3. Tworzenie i wykorzystanie kopii różnicowej

### 6.2. Zagrożenia związane z ludźmi

Opisane wyżej zagrożenia, których źródłem jest strona techniczna cyberprzestrzeni, są niczym w zestawieniu z zagrożeniami, jakich źródłem mogą być ludzie. Klasyfikację tych zagrożeń przedstawia rysunek 4.



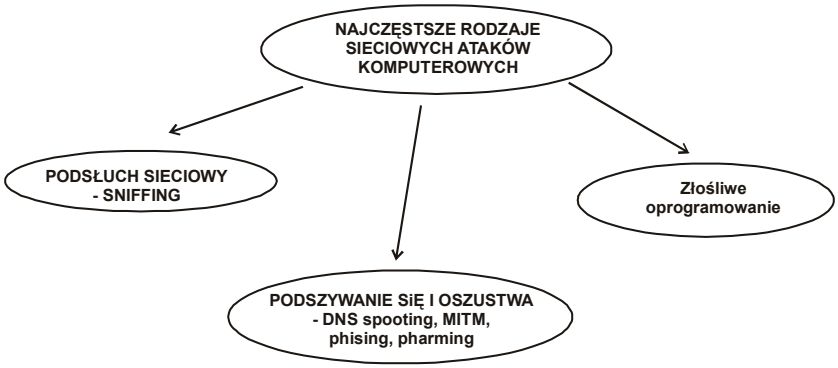

Rys. 4. Podział zagrożeń ze względu na wybrane kryteria

Szkody i zagrożenia w cyberprzestrzeni generowane przez ludzi powstają z różnych pobudek. Niektóre z nich zebrano (przykładowo) w tabeli 3.

Tabela 3. Przykładowe motywacje osób stwarzających zagrożenie w cyberprzestrzeni

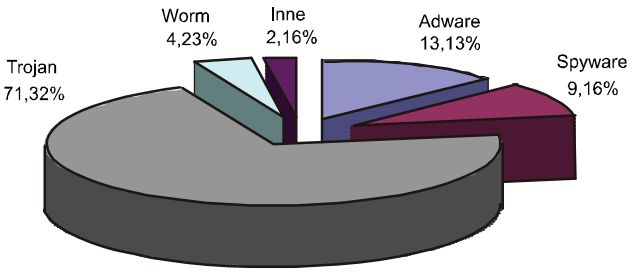
| Atakujący | Zamierzenie |
|---|---|
| Student | Odczytywanie cudzych listów dla zabawy |
| Kraker | Testowanie bezpieczeństwa obcych systemów, kradzież informacji |
| Przedstawiciel handlowy | Chęć poprawy własnego wizerunku i prestiżu |
| Biznesmen | Poznanie strategicznych tajemnic konkurentów |
| Były pracownik | Zemsta za zwolnienie z pracy |
| Księgowy | Defraudacja firmowych pieniędzy |
| Makler giełdowy | Wycofanie się z obietnicy złożonej klientowi drogą elektroniczną |
| Oszust | Przechwycenie numerów kart kredytowych |
| Szpieg | Zapoznanie się z wojskowymi i przemysłowymi tajemnicami |
| Terrorysta | Dokonanie zniszczeń, które przyniosą szkodę zaatakowanemu |

Formy, jakie przybierają ataki w cyberprzestrzeni, pokazano na rysunku 5.




Rys. 5. Najczęstsze rodzaje sieciowych ataków komputerowych

Z kolei na rycinie 6 (zaczerpniętej ze strony http://www.interaktywnie.com) pokazano rodzaje zagrożeń (złośliwych programów szpiegujących) oraz ich procentowe występowanie.




Rys. 6. Klasyfikacja zagrożeń związanych ze złośliwym oprogramowaniem

## 7. Podsumowanie i wnioski

Przedstawiony w artykule przegląd jest zaledwie wstępnym rzutem oka na niezwykle rozległą i ważną dziedzinę, jaką jest problem zagrożeń w cyberprzestrzeni. Mimo tej skrótowej formy artykuł może być użyteczny, ponieważ zwraca uwagę na fakt, że ludzie XXI wieku wprawdzie nadal fizycznie przebywają w świecie przedmiotów realnych i tam eksponowani są na zagrożenia ze strony przedmiotów realnych (czynniki zakaźne, klęski żywiołowe, zanieczyszczenie środowiska, terroryzm itp.), ale wiele form działania ludzi przenosi się systematycznie ze sfery bytów realnych do sfery bytów wirtualnych. W świecie bytów wirtualnych, określonym umownie w tym artykule jako cyberprzestrzeń, obok licznych udogodnień istnieją też zagrożenia. Celem artykułu było zwrócenie uwagi na istnienie tych zagrożeń i na konieczność ich zwalczania.

## Wybrane pozycje literatury

Babiy V., Bigelow B., Grewal R.S. et al.: *Internet Contamination as a Global Harm and a Social Problem*, Journal of Applied Computer Science, Vol. 16, No. 2, 2008, pp. 43-53.

Bigelow B., Janicki R., Kakiashvili T. et al.: *A Case of Web Cancer*, Pro-Dialog, Nr 23, 2007, pp. 59-62.

Grewal R.S., Janicki R., Kakiashvili T. et al.: *Attacking the web cancer with the automatic understanding approach*, Chapter in book: Wegrzyn-Wolska K.M., Szczepaniak P.S. (Eds.): *Advances in Intelligent Web Mastering, Advances in Soft Computing*, vol. 43, Springer-Verlag, Berlin – Heidelberg – New York, 2007, pp. 136-141.

Mak S.: Ethical Values for E-Society: *Information, Security and Privacy. Ethics and Policy of Biometrics. Third International Conference on Ethics and Policy of Biometrics and International Data Sharing*, ICEB 2010. Revised Papers. 2010, pp. 96-101.

Ponelis S., Britz J.: *The Elephant in the Server Room: Confronting the Need for an Ethics Officer in the IT Function*. Proceedings of the International Conference on Information Management and Evaluation. 2010, pp. 232-239.

Rezaul K.M., Rahman M.M., Hossain A.: *Information Security and Threats: A study on E-commerce*. Proceedings of the 2009 International Conference on Security & Management. SAM. 2009, pp. 22-27.

Solanas A., Domingo Ferrer J., Castella Roca J.: *Digital Identity and Privacy in some New-Generation Information and Communication Technologies*. The European Journal for the Informatics Professional. Feb. 2010, 11(1), pp. 67-72.

Tadeusiewicz R.: *Człowiek w Społeczeństwie Informacyjnym*. Rozdział w książce: Gielarowski A., Homa T., Urban M. (red.): *Odczarowania – Człowiek w społeczeństwie*. Humanitas – Studia Kulturoznawcze, Ignatianum, Kraków, 2008, s. 145-156.

Tadeusiewicz R.: *E-administracja jako narzędzie formowania społeczeństwa informacyjnego*. V Forum Informatyki w Administracji, Centrum Promocji Informatyki, Warszawa 2005, s. 7-42.

Tadeusiewicz R.: *Nowe technologie dowodowe dla przestępstw popełnianych w obszarze społeczeństwa informacyjnego*. Rozdział w książce: Gardocki L., Godyń J., Hudzik M., Paprzycki L.K. (red.): *Nowe technologie dowodowe a proces karny*. Sąd Najwyższy, Warszawa 2007, s. 19-20.

Tadeusiewicz R.: *O potrzebie naukowej refleksji nad rozwojem społeczeństwa informacyjnego*. Rozdział w książce: Bliźniuk G., Nowak J.S.: *Społeczeństwo informacyjne 2005*, PTI Oddział Górnośląski, Katowice 2005, s. 11-38.

Tadeusiewicz R.: *Problem formowania e-administracji jako składnika społeczeństwa informacyjnego*, Rozdział w książce Siwik A. (red.): *Od społeczeństwa industrialnego do społeczeństwa informacyjnego*, UWND AGH, Kraków 2007, s. 391-404.

Tadeusiewicz R.: *Rewolucja społeczeństwa informacyjnego na tle wcześniejszych rewolucji cywilizacyjnych*. Rozdział w książce: Haber L., Niezgoda M. (red.): Społeczeństwo informacyjne – aspekty funkcjonalne i dysfunkcjonalne, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków, 2006, s. 31-45.

Tadeusiewicz R.: *Rola technologii cyfrowych w bibliotekach XXI wieku*. Rozdział w pracy zbiorowej: Próchnicka M., Korycińska-Huras A. (red.): *Między przeszłością a przyszłością. Książka, biblioteka, informacja naukowa – funkcje społeczne na przestrzeni wieków*. Wydawnictwo UJ, Kraków 2007, s. 303-314.

Tadeusiewicz R.: *Technologie cyfrowe a społeczeństwo informacyjne*, W materiałach konferencji: V Ogólnopolskie Sympozjum Rola INSPIRE w rozwoju społeczeństwa informacyjnego, Urząd Miasta Krakowa 2009, s. 33-34.

Tadeusiewicz R.: *Telemedycyna jako ważny, ale trudny składnik społeczeństwa informacyjnego*, Rozdział w książce: Bliźniuk G., Nowak J.S. (red.): *Społeczeństwo informacyjne – doświadczenie i przyszłość*, PTI, Katowice, 2006, s. 99-123.

## Threats in cyberspace

Development of Information and Communication Technology (ICT) is very fast. Moreover scale of social impact of such technology, which can be evaluated on the base of calculation of number of people connected to Internet, is also huge and increasing. Thinking about social impact of ICT we must also take into account role played by this technology in many

people's activities. In many professions we cannot work regular without computers, Internet and other elements of information technology. Social impact of ICT is nowadays expressed by talking about so called information society. This new form of social and economical organization presents many advantages. But there are also the dark side. Opening for people huge space for communication, reach in (between others) valuable information, such technology, called often cyberspace, lead also to new kinds of threats. There are completely new threats, which was even not forecasted few years ago. In paper some of such threats are presented and discussed with stress located on their increasing nature. Moreover such threats concern increasing number of people around the world. For emphasize scale of problem the analogy between consequences of threats in cyberspace and hurricane Katrina is presented in numerical form.

**Key words:** civilization threats, cyberspace, spam, information society, haker