

„Wolność to bardzo piękna rzecz, ale  
wtedy, gdy nie jest okupiona  
samotnością”  
Bertrand Russel

## BEZPIECZEŃSTWO I WOLNOŚĆ W GLOBALNYM SPOŁECZEŃSTWIE INFORMACYJNYM

Piotr SIENKIEWICZ<sup>1</sup>

### 1. Wprowadzenie

O globalnym społeczeństwie informacyjnym XXI wieku mówi się, że rozwija się w klimacie niepewności i ryzyka. Klimat ten dostrzega się nie tylko w skali globalnej, lecz także lokalnej oraz w wymiarze jednostkowym jako cechę egzystencji współczesnego człowieka. Nader często pojawiają się iście kasandryczne wieszczona, eksponujące nowe zagrożenia cywilizacyjne i przywołujące Orwellovskiego Wielkiego Brata, panoptikon Benthama i Foucaulta, społeczeństwo nadzoru Lyona czy społeczeństwa ryzyka Becka. „*Społeczeństwo ryzyka jest społeczeństwem katastrof. Zagraża mu to, że stany wyjątkowe stają się stanami normalnym*” Wiek XX, zwany niekiedy wiekiem skrajności, to okres dwóch wojen światowych, powstania i upadku totalitaryzmów, trudnych do opisania wojen i konfliktów lokalnych oraz licznych kataklizmów różnorodnej natury, lecz to także złoty wiek nauki, techniki i sztuki. To historia świata, który utracił punkty oparcia i został opanowany przez niepewność oraz kryzys. Obok „zwyčajnych” kryzysów w życiu współczesnych społeczeństw, których „oswajanie” odbywa się kosztem ich wyjątkowości i niezwykłości, pojawiły się wyjątkowe wydarzenia takie, jak: WTC, Pentagon, Kursk, Concorde, Enron i Worldcom, Musical Nord-Ost w teatrze na Dubrowce, Bali, Intifada, Tankowiec Prestige czy epidemia SARS. Z tego obrazu wyłania się świat kryzysów, czyli świat niedoboru bezpieczeństwa.

Na szczęście nie brak i optymistycznych sądów. Optymiści idealizują sieci w przekonaniu, że „zepchną” one w cień reżimy sterowania oparte na hierarchii. Optymistyczny nurt diagnoz i prognoz społecznych, rujnujący epokę globalizacji i Internetu, wpisuje się w paradygmat refleksyjności, rozwoju osobowości i ewolucji struktur społecznych. Zapewne w tym nurcie mieszczą się, w różnym stopniu, zarówno Toffler, Giddens, także Beck i Castells. Jeśli z jakiejś możliwej syntezy tych propozycji wyłania się pewna wizja optymistycznego „kresu” formującego się globalnego społeczeństwa informacyjnego i, jeśli nawet uznamy ją za kolejną utopię, to warto wyrazić nadzieję, że - jak powiadał Pierre Lery – jest to „utopia osiągalna” (*une utopie realisable*).

### 2. Globalna przestrzeń bezpieczeństwa

Przełom wieków to okres globalizacji i społeczeństwa informacyjnego, czyli tworzenia się globalnego społeczeństwa informacyjnego - nowego dynamicznego i nieliniowego systemu. Ten zaś możemy postrzegać zarówno jako system cybernetyczny i jako globalne społeczeństwo ryzyka. Każdy system ma własną racjonalność, wyrazem której może być jego główny cel: zachowanie równowagi i (lub) maksymalizacja dóbr (zysku) i

---

<sup>1</sup>plk prof. dr hab. inż. Piotr Sienkiewicz, Akademia Obrony Narodowej.

(lub) maksymalizacja władzy (dominacji). Dążenie do osiągnięcia tych celów może, choć nie musi sprzyjać powstawaniu sytuacji konfliktowych i kryzysowych, zagrażających bezpieczeństwu w skali globalnej i lokalnej. W złożonym, dynamicznym i nieliniowym systemie – dla pewnych warunków początkowych - zakłócenia na poziomie jego elementów (podsystemów) mogą wywołać nieprzewidywalne skutki globalne. W systemach tych stała jest zmiana, zaś nie ma czegoś takiego, jak izolowany człowiek lub sytuacja. Istnieje tylko relacja między człowiekiem i środowiskiem, a relacją tą jest zagrożenie. Powoduje to, że we współczesnym świecie kryzys stał się zjawiskiem „normalnym” (tabela 1).

**Tab. 1.** Istota zjawiska kryzysu

DZIEDZINA	PRZYKŁADOWE WYJAŚNIENIE POJĘCIA KRYZYS	WYBRANE KONCEPCJE ROZWAŻANE PROBLEMY
NAUKA (HISTORIA NAUKI)	Postępujące trudności z obowiązującym paradygmatem, który nie wystarcza do opisu i analizy zjawisk.	Koncepcja T. Kuhna dotycząca rewolucji naukowych. Paradygmaty naukowe. Postęp w nauce.
POLITYKA	Załamania na scenie politycznej przejawiające się w niestabilności, zmianie układu władzy.	Kryzysy rządowe. Zaufanie do państwa.
GOSPODARKA	Najczęściej: załamanie procesu wzrostu gospodarczego.	Cykle koniunkturalne. Symptomy i wskaźniki kryzysu. Krachy giełdowe, kryzysy finansowe.
SPOŁECZEŃSTWO, CYWILIZACJA, KULTURA	Załamanie systemu wartości podstawowego dla danego społeczeństwa.	Rozwój i powstanie cywilizacji. Modernizacja. Zmiany wartości kulturowych, trauma kulturowa.
PRAWO	Nadzwyczajne, nie dające się przewidzieć zakłócenie istniejącego stanu rzeczy (np. porządku prawnego, jednolitości politycznej).	Regulacje prawne dotyczące kryzysu i stanów kryzysowych; stan wyjątkowy
PRZYRODA	Zdarzenia powodujące przejście pomiędzy istniejącymi w przyrodzie gatunkami (formacjami, płaszczynami).	Ewolucja, wymieranie gatunków a także: kataklizmy, równowaga ekologiczna.
MEDYCYNA	Nagle, gwałtowne przesilenie się choroby, przełom.	Diagnozowanie i prognozowanie rozstrzygnięć.

Źródło: J.N.Rosenau, (1990) *Turbulenc In World Politics. A theory of Change and Continuity*, Princeton.

Analiza systemowa bezpieczeństwa ma racjonalny sens, gdy dokonuje się identyfikacji niebezpieczeństwa, czyli zagrożeń mogących spowodować bądź zakłócenia funkcjonowania (egzystencji, rozwoju) badanych obiektów, bądź możliwość utraty przez nie określonych wartości. Bezpieczeństwo jest pojęciem wieloznacznym, odnoszącym się do: (1) braku zagrożenia, (2) systemu instytucjonalnych i pozainstytucjonalnych gwarancji likwidacji

lub minimalizacji zagrożeń, (3) utraty jednej z istotnych wartości egzystencjalnych, wiążących się z poczuciem stabilności, trwałości korzystnego stanu rzeczy, odczuciem stanu zagrożenia, wrażeniem pewności itp. W badaniach nad bezpieczeństwem narodowym (międzynarodowym) stosowane są zarówno kryteria zasięgu (np. bezpieczeństwo regionalne, globalne), jak i kryterium przedmiotowe (np. bezpieczeństwo: militarne, ekonomiczne, ekologiczne, technologiczne, kulturowe, informacyjne).

Na przełomie wieków kształtował się „nowy (ponowoczesny) ład światowy”, czyli określona „globalna przestrzeń bezpieczeństwa”. Wymiarami tej przestrzeni są: (1) możliwe i prawdopodobne zagrożenia, (2) prawdopodobieństwo wystąpienia tych zagrożeń, (3) przewidywane negatywne skutki zagrożeń (w skali globalnej i lokalnej), (4) możliwości zapobieżenia zagrożeniom lub likwidacji ich skutków, (5) strategie zapobiegania zagrożeniom (ich skutkom w postaci kryzysów i konfliktów). Można dostrzec alternatywne modele „państwocentrycznego” i „policentrycznego” globalnego systemu politycznego (tabela 2).

**Tab. 2.** Model państwocentrycznego i policentrycznego świata polityki.

	ŚWIAT PAŃSTWOCENTRYCZNY	ŚWIAT POLICENTRYCZNY
Liczba aktorów	Określona na ok. 200 państw.	Nieokreślona: aktorzy państwowi i niepaństwowi.
Podstawowa wartość	Bezpieczeństwo, potęga, racja stanu.	Autonomia, dobrobyt państw i społeczności międzynarodowej, solidaryzm.
Główne cele	Integralność terytorialna, suwerenność, potęga/siła.	Globalizacja i liberalizacja handlu, integracja subsystemów, solidaryzm i zanik egizmów państwowych.
Środki	Militarne.	Dyplomatyczne i sytuacyjne.
Formy współpracy	Formalne sojusze.	Czasowe koalicje.
Skala współpracy	Zredukowana do zapewnienia bezpieczeństwa.	Nieograniczona.
Wyznaczniki pozycji	Potencjał militarny.	Ekonomiczna, potencjał techniczny i cywilizacyjny.
Struktura systemu	Sztywna, wyznaczana przez wielkie mocarstwa.	Labilna, wyznaczana przez aktorów z potencjałem ekonomicznym.
Rodzaje oddziaływań	Symetryczne.	Asymetryczne.
Umiejscowienie władzy	Wielkie mocarstwa.	Aktorzy dysponujący różnymi formami wpływów.
Zdolność do zmian	Ograniczona.	Nieograniczona.
Ośrodki kontroli	Skoncentrowane w rękach supermocarstw.	Zdekoncentrowane i przeniesione na podmioty niepaństwowe.
Źródła władzy	Prawo, autorytet formalny.	Różne źródła autorytetu i władzy (skuteczne przywództwo).

Źródło: J.N.Rosenau, 1990 *Turbulenc In World Politics. A theory of Change and Continuity*, Princeton.

Nowe środowisko bezpieczeństwa globalnego systemu określają takie zjawiska, jak:

- postępująca globalizacja polityczna, gospodarcza, finansowa, kulturowa, informacyjna;
- procesy integracyjne związane z rozwojem organizacji międzynarodowych („oddanie części suwerenności”);
- kryzys państwowości;
- asymetria ekonomiczna, technologiczna, społeczna (luka rozwojowa między Północą i Południem);
- słabość istniejących struktur bezpieczeństwa (ONZ, NATO, UE, OBWE, UA);
- niedostatki prawa międzynarodowego (brak jednolitych regulacji wobec nowych negatywnych zjawisk);
- jednobiegowość w sferze militarnej (dominacja USA);
- rewolucja technologiczna w siłach zbrojnych (rewolucja teleinformatyczna, sieciocentryczne pole walki);
- zróżnicowanie koncepcji bezpieczeństwa – nowa rola sił zbrojnych (prewencja oraz „soft power”);
- trudności w adaptacji organizacji międzynarodowych do nowych warunków (zagrożenia asymetryczne, ograniczona przewidywalność, nieokreśloność doktryn i struktur, myślenie w kategoriach kryzysu).

Nowe, globalne środowisko społeczne sprzyja powstawaniu nowych zagrożeń, a także rozwojowi dawnych, wyniesionych niejako z „ery industrialnej”. Do nich należy zaliczyć:

- zorganizowany terroryzm międzynarodowy;
- proliferację broni masowego rażenia;
- nowe rodzaje przestępczości związane z rozwojem technologii informacyjnych (infoterroryzm, cyberterroryzm);
- niekontrolowane operacje finansowe (zwłaszcza w e-bankowości);
- wrażliwość krytycznej infrastruktury państwa (zwłaszcza na cyberataki);
- wrażliwość globalnego systemu gospodarczego;
- zagrożenia ekologiczne (degradacja ekosfery);
- zagrożenia informacyjne (degradacja infosfery);
- wzrost zasięgu społeczności „odrzuconych”, marginalizowanych (trudności w asymilacji i integracji);
- wzrost bezrobocia (w tym strukturalnego);
- wymuszone masowe migracje;
- przestępczość transgraniczną;
- nowe choroby zakaźne;
- rozwój zasięgu fundamentalizmów.

Różna jest waga i skala wyróżnionych zagrożeń, jedne są bezpośrednim skutkiem globalizacji, inne zaś – rozwoju technologii informacyjnych. Wyznaczają one w znacznym stopniu „obszary niepewności” w systemie globalnym (tabela 3).

**Tab. 3.** Obszary niepewności

WZGLĘDNA PEWNOŚĆ	KLUCZOWE NIEPEWNOŚCI
Globalizacja praktycznie nieodwracalna, będzie stawać się coraz mniej „zachodnia”.	Czy globalizacja spowoduje rozwój zacofanych gospodarek; w jakim stopni kraje azjatyckie określą nowe reguły gry?
Gospodarka światowa znacznie większa.	Zwiększenie się przepaści między państwami bogatymi i biednymi, załamywanie się kruchych demokracji, rozwiązywanie

	kryzysów finansowych.
Rosnąca liczba przedsiębiorstw globalnych ułatwia rozszerzanie się technologii.	Zakres wyzwań dla rządów, wynikających z ponadpaństwowych powiązań gospodarczych.
Wzrost znaczenia krajów Azji i pojawienie się nowych państw – „gospodarczej wagi średniej”.	Czy wzrost gospodarczy Chin i Indii będzie odbywać się bez konfliktów?
Starzenie się ludności w najpotężniejszych dzisiaj państwach.	Jakie są zdolności Unii Europejskiej i Japonii do adaptacji siły roboczej, systemów socjalnych i do integracji ludności napływowej; czy Unia zostanie supermocarstwem?
Stan zasobów energetycznych w złożach wystarczający do pokrycia światowego zapotrzebowania.	Niestabilność polityczna w krajach – dostawcach paliw, zakłócenia w dostawach.
Rosnąca siła i znaczenie innych niż państwa uczestników światowej gry.	Chęć i zdolność państw oraz instytucji międzynarodowych do współpracy z tymi czynnikami.
Islam politycznie pozostanie potężną siłą.	Wpływ religijności na jedność państw i potencjalne konflikty z tym związane; rozwój ideologii dżihadu.
Zwiększono możliwości stosowania broni masowej zagłady przez niektóre państwa.	Więcej czy mniej państw nuklearnych; zdolności terrorystów do uzyskania broni biologicznej, chemicznej, radioaktywnej lub jądrowej.
Łuk niestabilności rozciągający się od Afryki przez Bliski Wschód do Azji.	Przyspieszanie wydarzeń prowadzących do obalania rządów.
Mało prawdopodobny konflikt między wielkimi mocarstwami, przekształcający się w wojnę totalitarną.	Zdolność do rozładowywania punktów zapalnych i hamowania walki o surowce.
Coraz silniej postrzegane problemy etyczne i środowiska naturalnego.	Zakres, w którym nowe technologie tworzą lub rozwiązują dylematy etyczne.
USA pozostaną najpotężniejszym uczestnikiem gry światowej – ekonomicznie, technicznie, i wojskowo.	Pytanie, czy inne kraje będą mogły bardziej otwarcie rzucać wyzwanie Waszyngtonowi; czy USA stracą swoją przewagę w nauce i technice?

Źródło: Raport NIC (National Intelligence Council), (2004)

W pierwszej dekadzie XXI wieku szczególnego znaczenia nabiera walka z ponadnarodowymi, niezlokalizowanymi organizacjami (wirtualnymi?), których członkowie nie tylko akceptują samobójstwo, lecz żarliwie go pragną.

Dialektyka wojny i pokoju to w istocie dialektyka strachu. W globalnym społeczeństwie informacyjnym „wielki strach” (przed atomową zagładą) ustępuje miejsca wielu mniejszym lękom i ich niejako kumulacjom, wiążącym się z ryzykiem - zagrożeniami dla zdrowia, środowiska, bezpiecznego rozwoju itp.

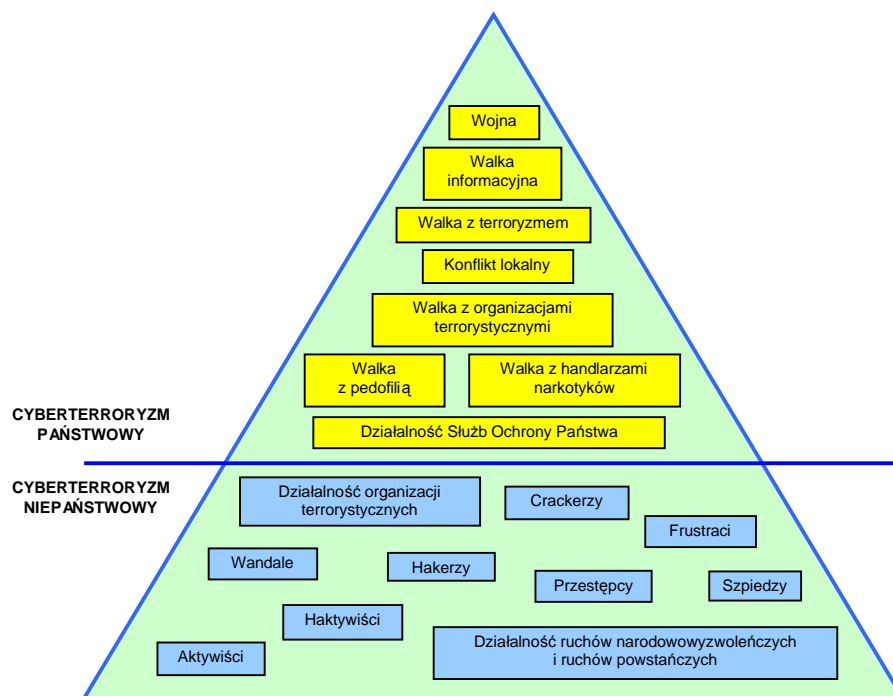
### 3. Niebezpieczna przestrzeń cybernetyczna

Po raz pierwszy termin „cyberterroryzm” pojawił się w raporcie o zagrożeniach komputerowych w Szwecji, w 1979 r. Obejmował on wszelką działalność z użyciem komputerów mającą na celu niszczenie systemów teleinformatycznych, systemów nadzoru i kontroli, programów, danych itp., a w konsekwencji zastraszanie rządów i społeczeństw, wywieranie presji psychologicznej, doprowadzenie do zagrożenia życia lub powstania znacznych strat materialnych.

Jednakże powszechnie za twórcę pojęcia cyberterroryzm uznaje się B. Collina, pracownika Institute for Security and Intelligence w Kalifornii, który w latach 80. ubiegłego wieku użył go dla określenia połączenia cyberprzestrzeni i terroryzmu. Według Bógdał-Brzezińskiej, cyberterroryzm: *to świadome wykorzystanie systemu informacyjnego, sieci komputerowej lub jej części składowych w celu wsparcia lub ułatwienia terrorystycznej akcji.*

W amerykańskim Departamencie Obrony próbuje się połączyć zarówno aspekt „konwencjonalny” jak i „cybernetyczny”, a wtedy cyberterroryzm to zdeterminowane i świadome użycie środków walki informacyjnej przez aktorów niepaństwowych lub grupy sponsorowane przez państwa, motywowane politycznie, społecznie, ekonomicznie lub religijnie, w celu zastraszania, wzbudzenia niepokoju i paniki wśród atakowanej ludności oraz doprowadzenia do zniszczenia wojskowych i cywilnych celów. Atak cyberterrorystyczny to każde działanie wymierzone w systemy informacyjne, bez względu na to, czy jest on dokonany za pomocą komputera, czy też nie (rys.1).

**Rys.1.** Cyberterroryzm państwowy i niepaństwowy



Źródło: opracowanie własne.

Definicja uznawana przez FBI, określa cyberterroryzm jako *politycznie umotywowana, przemyślana działalność grup narodowych lub innych wrogich sił wymierzona przeciw informacji, systemom komputerowym, programom i danym, która powoduje straty cywilne*

W latach 80. terminem cyberterroryzm posługiwano się w amerykańskich służbach specjalnych, wskazując na możliwości przeprowadzenia ataków elektronicznych przez wrogów Stanów Zjednoczonych. W 1998 r. w Centrali FBI utworzono Centrum Ochrony

Infrastruktury Narodowej (NIPC), którego zadaniem jest koordynowanie działań w zakresie gromadzenia informacji o zagrożeniach, reagowanie na zagrożenia informacyjne lub zamachy na elementy krytycznej infrastruktury państwa.

Istnieje sześć głównych powodów przemawiających za wykorzystaniem cyberterroryzmu dla osiągnięcia konkretnych celów:

- niskie koszty takiej działalności, zwłaszcza w porównaniu z kosztami regularnych działań zbrojnych (do ataku cyberterrorystycznego wystarczy przeciętny sprzęt komputerowy, dostęp do Internetu i trochę umiejętności);
- zanikanie wszelkich granic - państwa tracą część swojej suwerenności - zacierają się granice między tym co prywatne a państwowe, wojskowe a komercyjne itd. Konsekwencją zanikania wszelkich barier jest prawdopodobieństwo, że zaatakowane państwo nie będzie sobie z tego zdawało sprawy (zacieranie się granic między wojną a pokojem);
- możliwość dokonywania nagłych i nieprzewidywalnych akcji - ofiary są, całkowicie nieświadome i nieprzygotowane do ich odparcia;
- całkowita anonimowość - powoduje to możliwość manipulowania informacją, utrudnia państwom odparcie ataku i budowanie koalicji;
- minimalne ryzyko wykrycia przygotowywanego ataku;
- zamiast uderzać w niewinnych ludzi można sparaliżować system wrogiego państwa - większy efekt propagandowy i uznanie opinii publicznej.

Istnieje jeszcze kilka powodów, dla których terroryści mogą przenieść swoją działalność do cyberprzestrzeni. Po pierwsze, konwencjonalne metody działalności terrorystycznej są niebezpieczne dla samych terrorystów. Cyberprzestrzeń pozwala dokonywać ataków bez narażania własnego życia. Po drugie, nie trzeba wielkich umiejętności przeprowadzając tego typu akcję. Po trzecie, walka z cyberterroryzmem wymaga o wiele większej koordynacji niż w przypadku innych działań. Po czwarte, państwa dysponują bardzo małymi możliwościami zastosowania sankcji. Po piąte, umasowienie dostępu do komputerów sprawia, że stają się one coraz prostsze w obsłudze - nie potrzeba specjalnych umiejętności, aby obsługiwać programy komputerowe i podobnie jest z narzędziami niezbędnymi do przeprowadzania cyberataków - w Internecie można znaleźć bardzo wiele programów, które umożliwiają odszyfrowanie kodu dostępu do komputera lub bazy danych, czy włamanie się do systemu. Wraz ze zmniejszaniem się potrzebnych umiejętności do przeprowadzenia cyberataku, zwiększa się skuteczność i jakość programów mających to ułatwić. W konsekwencji każdy może zostać cyberterrorystą.

Aktualna klasyfikacja ataków cyberterrorystycznych jest następująca:

- 1) metody polegające na uzyskaniu haseł dostępu do sieci (*stealing passwords*);
- 2) wykorzystanie niekompetencji osób, które mają dostęp do systemu (*social engineering*);
- 3) korzystanie z systemu bez specjalnych zezwoleń lub używanie oprogramowania z nielegalnych źródeł (*bugs and backdoors*);
- 4) zniszczenie mechanizmu używanego do autoryzacji (*authentication failures*);
- 5) wykorzystanie luk w zbiorze reguł sterujących wymianą informacji pomiędzy dwoma lub wieloma niezależnymi urządzeniami lub procesami (*protocol failures*);
- 6) atakujący zdobywa informacje dostępne tylko dla administratora, niezbędne do poprawnego funkcjonowania sieci (*information leakage*);
- 7) uniemożliwienie użytkownikom korzystania z ich systemu (*denial of service*).

Po wydarzeniach z 11 września 2001 r. zwrócono uwagę na możliwość podobnych ataków terrorystycznych na całym świecie, w tym na możliwe i prawdopodobne zmasowane „cyberataki” na systemy teleinformatyczne USA i sprzymierźców, wykorzystywane w walce ze światowym terroryzmem. Wówczas, w amerykańskiej ustawie antyterrorystycznej rozszerzono definicję terroru o cyberterroryzm i sankcje prawne (np. hackerska penetracja

systemów informacyjnych o dużym znaczeniu dla bezpieczeństwa narodowego zagrożona jest w USA nawet karą dożywotniego więzienia).

Można stwierdzić, że w znaczeniu wąskim cyberterroryzm to działalność terrorystyczna w systemach teleinformatycznych ukierunkowana na zniszczenie lub modyfikację danych w tych systemach, skutkująca ofiarami śmiertelnymi lub zniszczeniem mienia w znacznych rozmiarach (zazwyczaj celem jest jedno i drugie). W szerszym znaczeniu jest to wszelka działalność terrorystyczna związana z cyberprzestrzenią (systemami teleinformatycznymi), włączając w to fizyczne ataki na systemy oraz aktywność propagandową. Działalność taka może na przykład przyczynić się do pozyskiwania informacji przydatnych do realizacji bardziej klasycznych akcji terrorystycznych, na przykład zamachów bombowych.

Liczne przykłady funkcjonowania stron www poświęconych terroryzmowi (szacuje się, że stron poświęconych tylko dżihadowi jest w sieci 150 – 200) potwierdzają efektywne i często efektowne narzędzie propagandy terrorystów. W sieci można przeczytać o organizacjach i ich celach. Niektóre z nich oferują sprzedaż „gadżetów”, takich jak koszulki, plakaty, kasety video itp.; inne werbują za pomocą Internetu ochotników do walki ze swoimi przeciwnikami, oferują informacje typu jak dokonać zamachu terrorystycznego, skonstruować bombę, na niektórych wreszcie są informacje jak dofinansować przedsięwzięcia o charakterze przestępczym.

**Rys. 2.** Typologia zagrożeń dla bezpieczeństwa systemów informacyjnych



Źródło: Opracowanie własne.

#### 4. Ucieczka od (do?) wolności

Zaufanie i bezpieczeństwo, ryzyko i zagrożenie, kryzys i konflikt pojawiają się w różnych historycznie specyficznych skojarzeniach, służą do opisu globalnej nowoczesności. *Nowoczesność to kultura ryzyka. Nowoczesność zmniejsza ogólną ryzykowność pewnych sfer i sposobów życia, ale jednocześnie wprowadza nowe, prawie lub całkiem nieznanie wcześniejszym epokom parametry ryzyka*” Nie oznacza to, że świat zmierza ku katastrofie, lecz że niesie nieznaną dotąd formę ryzyka ograniczającą swobodę decyzyjną i poczucie bezpieczeństwa. *Lęk nie ogranicza się do konkretnej sytuacji ryzyka i zagrożenia. Należy go raczej kojarzyć z całościowym systemem bezpieczeństwa, który wykształca jednostkę*” W

świecie jaki znamy *dochodzi do spotkania dwóch różnych wartości: wolności i bezpieczeństwa - na równi pożądanym, bo na równi niezbędnym dla godnego i szczęśliwego życia. Pragnienie bezpieczeństwa i pragnienie wolności nie dają się ze sobą pogodzić. (...) Brak wolności objawia się z kolei w postaci nadmiaru obezwładniającego i zniewalającego bezpieczeństwa (określanego mianem „zależności”). (...) kiedy brakuje poczucia bezpieczeństwa, wolne jednostki tracą pewność siebie, bez której trudno korzystać z wolności.*

Globalne społeczeństwo informacyjne stwarza nowy typ sytuacji decyzyjnych dla wielu ludzi, gdy mają „wolność do wyboru”, ale zarazem napotykają na ograniczenia uniemożliwiające podjęcie racjonalnych decyzji. Wzrost zasobów informacyjnych i rosnące możliwości techniczne korzystania z nich zwiększają możliwości dokonywania racjonalnych wyborów, bowiem to informacje stanowią główną determinantę pomyślnego rozwiązywania sytuacji decyzyjnych. Ale nadmiar informacji wraz z ograniczonymi możliwościami ich selekcji, w połączeniu z „tyraniem chwili” stanowi przyczynę powstawania sytuacji typu „wolność od wyboru”. Być może sposobem wyjścia z takich sytuacji jest swoisty eskapizm, „ucieczka od wolności”. Większą możliwość wyboru ogranicza wolność.

„Wolność od wyboru” cechowała człowieka w systemach totalitarnych. Tak działo się w świecie antyutopii Orwella („1984”), gdzie o wszystkim decydował „Wielki Brat” (*Big Brother is watching you!*), a w realnych totalitaryzmach onnipotentne „Centrum”. „Wolność do wyboru” ma stanowić cechę systemu demokratycznego, społeczeństwa obywatelskiego. Państwo jednak ponosi instytucjonalną odpowiedzialność za bezpieczeństwo obywateli, co nieuchronnie musi doprowadzić do ograniczenia ich swobody decyzyjnej („wolności do wyboru”). Należy przy tym odróżnić obiektywną wolność jednostki od poczucia wolności, czyli „bycia wolnym” (*being free*) od „czucia się wolnym” (*feeling free*). Podobnie, jak należy rozróżniać bezpieczeństwo fizyczne czy techniczne (*safety*) i bezpieczeństwo społeczne (*security*). *Poczucie swobody może nie odpowiadać rzeczywistej dowolności podejmowania decyzji (...), dobrze znane są przypadki, że człowiek żyjący w systemie autorytarnym lub terytorialnym czuje się bardziej wolnym niż jednostka włączona w tradycyjne struktury demokratyczne.* Godząc się na udostępnienie danych osobowych lub np. na coraz powszechniejszy monitoring wizyjny zarówno w różnych miejscach w mieście, jaki i w budynkach (w szczególności tzw. budynkach inteligentnych), akceptujemy kolejne ograniczenia, gdyż zwiększają bezpieczeństwo obywateli, choć z drugiej strony ograniczają poczucie wolności. Przedsięwzięcia typu monitoring wizyjny, monitorowanie ruchu w sieciach teleinformatycznych, mniej lub bardziej ukryte formy inwigilacji lub cenzurowania np. treści komunikatów internetowych stają się elementem globalnego społeczeństwa informacyjnego.

Internet przestał być systemem wspomagającym różnorodne działania i służącym zaspokajaniu potrzeb poznawczych (dostępu do zasobów informacji i wiedzy). Warto przypomnieć, że ARPANet - pierwsza sieć komputerowa uruchomiona w 1969 r. - była elementem amerykańskiego systemu bezpieczeństwa narodowego. Następnie przekształciła się w sieć akademicką, by stać się w końcu globalnym systemem komercyjnym - megasiecią w postaci Internetu. Obecnie znaczna część wielomilionowej „społeczności Internetu” podejmuje działania autoteliczne, zaś wiele z nich z trudem poddaje się racjonalnej ocenie. Nie brak wśród nich działań niegodziwych, należących do licznego repertuaru przestępstw komputerowych. Można przyjąć, że częste, także uzależniające, korzystanie z zasobów i usług Internetu stanowi efekt pokusy „zanurzenia się” w rzeczywistości wirtualnej, o której pisano niegdyś, że może stanowić LSD XXI wieku. Uzależnienie od rzeczywistości wirtualnej jest zapewne formą eskapizmu, ucieczki nie tyle od wolności, co od rzeczywistości. Przyczyną tego zjawiska może być dążenie do zaspokojenia potrzeb autotelicznych (*homo ludens ery informacyjnej*), ale także poczucie samotności, alienacji w realnym środowisku społecznym. Niepewność pracy, „tyrania czasu”, uczestnictwo w „wyścigu szczurów”, osłabienie więzi

rodziny i towarzyskich, „syndrom konsumpcyjny” itp., to zapewne niektóre z przyczyn skłaniających do szukania swoistej rekompensaty w cyberprzestrzeni. Konsekwencją tej formy eskapizmu może być „samotność w sieci”, gdyż wirtualne związki są tylko substytutem zaspokojenia naturalnej potrzeby przyjaźni i miłości.

Uważa się, że częściej niż inni i z większą łatwością przywiązują się do cyberprzestrzeni osoby odczuwające osamotnienie, o rysach introwertycznych, charakteryzujące się zaniżoną samooceną itp. To może tłumaczyć poziom i styl zamieszczanych w Internecie wypowiedzi na dowolny temat, jest on bowiem często żenujący, zarówno ze względu na sens (brak sensu), jak i formę. Można im z pewnością przypisać, poza agresywnością i arogancją, jakąś formę ekshibicjonizmu, a raczej zaniku staroświeckiego „poczucia wstydu”. Być może jest to przejaw beznadziejnego zmagania się z samotnością, prowadzącą do eskapizmu.

## 5. Zakończenie

Internet jest odpowiedzią na pytanie, które nie zostało jeszcze postawione - twierdził Stanisław Lem. On też przestrzegał: *Kolejnym problemem, kto wie czy nie najfatalniejszym, jest fakt, że Internet otwiera wrota - jako ziemia opleciona siecią elektroniczną wyzbyta kontroli i centrów zwiadowczych - wszelkiej działalności - a zatem i takiej, która jest występna, a nawet zbrodnicza. Mafie, camorry, gangi, gangsterzy, oszuści i „imposterzy” wszelkiej maści uzyskują wstęp na arenę informacji na równi z potencjalnymi Einsteinami*

Technologie informacyjne zmieniły, niekiedy w ten sposób radykalny, styl życia, pracy, edukacji i rozrywki. Ale człowiek zawsze będzie pytać o sens życia, sens cierpienia i umierania. Na te pytania trudno znaleźć odpowiedź w przestrzeni cybernetycznej. Być może dlatego właśnie: *Z braku komfortu psychicznego zadowolamy się dzisiaj bezpieczeństwem albo pozorem bezpieczeństwa*

## Literatura

1. Balcerowicz B., 2002: Pokój i nie-pokój, Warszawa
2. Bauman Z. 2007: Płynne życie. Kraków.
3. Beck U. 2002: Społeczeństwo ryzyka. Warszawa.
4. Verton D. 2004: Black Ice. Niewidzialna groźba cyberterrorizmu. Gliwice
5. Castells M. 2003: Galaktyka Internetu. Poznań.
6. Chmielewski P., 2003: Semantyka kryzysu, [w:] Problemy zarządzania, Nr 2 Warszawa
7. Eriksen T. H. 2003: Tyrania chwili. Warszawa.
8. Fromm E. 1978: Ucieczka od wolności. Warszawa
9. Giddens A. 2001: Nowoczesność i tożsamość. Warszawa.
10. Goban- Klas T., Sienkiewicz P., 1999: Spdeczeństwo informacyjne- szanse, zagrożenia, wyzwania. Kraków.
11. Haber L.H., Niezgodna M. 2006: Społeczeństwo informacyjne. Aspekty funkcjonalne i dysfunkcjonalne. Kraków.
12. Kozielecki J. 2001: Psychotransgresja. Warszawa
13. Lem S. 2004: Krótkie zwanie. Kraków.
14. Sienkiewicz P. 2007: Konflikty i kryzysy w społeczeństwie informacyjnym. Szczecin.
15. Sienkiewicz P. 2006: Społeczeństwo informacyjne jako społeczeństwo ryzyka. Kraków.
16. Sienkiewicz P. 2005: Ucieczka od wolności w globalnym społeczeństwie informacyjnym. Szczecin.
17. Sienkiewicz P., Świeboda H. 2006: Niebezpieczna przestrzeń cybernetyczna. „Transformacje”, nr 1-4 (47-50) Warszawa.
18. Bógdoł-Brzezińska A., Gawrycki M., 2003: Cyberterrorizm i problemy bezpieczeństwa informacyjnego we współczesnym świecie. Warszawa

19. Zacher L. 2003: Spór o globalizację. Warszawa.