

Cyberterroryzm jako element zagrożenia współczesnej cywilizacji

Jerzy KISIELNICKI

Prof. zw. dr hab. Uniwersytet Warszawski Wydział Zarządzania, Katedra Systemów informacyjnych zarządzania

Streszczenie

Artykuł poświęcony jest problematyce nowego zagrożenia współczesnej cywilizacji jakim jest cyberterroryzm. Przedstawiono w nim formy działalności cyberterrorystycznej i niebezpieczeństwa które nosi ono dla społeczeństwa. Uzasadniono w nim również konieczność przeznaczenia odpowiednich środków na walkę z tym zjawiskiem

Wprowadzenie

Jeżeli nasze społeczeństwo jest świadome możliwości jakie daje zastosowanie systemów informatycznych zarządzania umie je wykorzystać dla wzbogacenia się i łatwości podejmowania decyzji to na pewno będzie szczęśliwe (w potocznym słowa tego rozumieniu). Jednak współczesna cywilizacja, która często bywa nazywana cywilizacją informacyjną to nie tylko pozytywy to także nowe zagrożenia.

Zmienia się świat a wraz z nim zmienia się największa plaga jaką jest terroryzm. To nie brodaty anarchista z bombą ale wykształcony siedzący/a przy komputerze osoba potrafi wywołać panikę i przerażenie świata.

Revolucja informacyjna i jej społeczne reperkusje

W nowym społeczeństwie na plan pierwszy wysuwa się informacja. Człowiek staje się wolnym, ponieważ posiada informacje i wiedze, które to zasoby pozwalają mu na decydowanie o swoim losie. Rewolucja informacyjna, w którą wchodzi rozwinięty świat stwarza niezwykle szanse dla jednostki i społeczeństwa. [L. Zacher 1999]. Wynika to z faktu, iż zwiększając znacząco możliwości przekazu informacji, stwarza się całkowicie nowe warunki dla komunikowania się i współdziałania. Obdarzony ogromną wyobraźnią futurolog A. Toffler [1991] pisze o konieczności rozwiązania różnorodnych problemów takich jak elektroniczna autostrada, powstanie monopolu informacyjnych, totalna wojna informacyjna.

Według L. Groff [1997] „cały świat – w różny sposób i różnymi sposobami-ulega restrukturyzacji oraz wpływowi rewolucji informacyjnej.” Polska również ulega tym przekształceniom.

Pragniemy też przedstawić hipotezę, że Polska jako nowy członek Unii Europejskiej dążąc do zacieśnienia współpracy gospodarczej, kulturalnej, turystycznej z krajami starej Unii Europejskiej, musi jak najszybciej przystąpić do budowy wspólnej przestrzeni informacyjnej. Przestrzeń informacyjna obejmuje między innymi bazy: danych, wiedzy, modeli, obrazów, dźwięku, wraz odpowiednim oprogramowaniem i środkami technicznymi, które umożliwiają użytkownikom korzystanie z tych zasobów w sposób bezpieczny i zgodny z przeznaczeniem. Dla osiągnięcia tych celów musimy wydatkować odpowiednie kwoty na TI.

Jak wielkie powinny być te kwoty? Na pewno powinny one proporcjonalnie odpowiadać kwotom wydatkowym w tych krajach, których poziom życia pragniemy osiągnąć. Oczywiście nakłady na współczesną infrastrukturę zarządzania pokrywane są w większości przez prywatnych przedsiębiorców. Ale od państwa polskiego zależy czy dla tego celu zostaną stworzone odpowiednie warunki makroekonomiczne. Jednak wydaje się, iż polityka gospodarcza nie zawsze jest skoordynowana z działaniami zarówno Unii Europejskiej, jak i naszych bezpośrednich sąsiadów. Przeprowadzone badania pod kierunkiem W. Cellarego [2002] wykazały, że Polska jest w grupie krajów o najniższym poziomie informatycznej infrastruktury. Sytuacja się nie poprawiła a wręcz przeciwnie. Jak pisze się w Gazecie Wyborczej „Polska to technologiczny zaścianek Europy” [G.W. z 2008.04.09]. Według Global Information Technology Polska w roku 2007 spadła z 58 miejsca w roku 2006 na 62. Na marginesie to w roku 2003 byliśmy na 47 pozycji. Natomiast jeżeli wziąć pod uwagę samo wykorzystanie TI w administracji państwowej i samorządowej to jesteśmy na 103 miejscu wśród wszystkich 130 ujętych w raporcie państw. Z analizy zamieszczonych w opracowaniach danych statystycznych, European Information Technology Observatory [roczniki 2000 - 2008] wynika, że, mimo, iż dynamika wydatków na TI w Polsce i krajach byłego bloku RWPG (kraje Europy Środkowo – Wschodniej) jest wysoka to jednak bezwzględna ich wysokość jest o wiele niższa niż w rozwiniętych krajach Unii Europejskiej . I tak mimo, że w Polsce w ciągu ostatnich 10 lat wydatkowano znaczne środki na TI to jednak jest to wiele mniej niż w większości krajów Unii Europejskiej. Polska należy w Europie do krajów najbardziej opóźnionych w zakresie wydatków na TI ale dynamika odrabiania tych strat jest bardzo duża.

Konsekwencją posiadania przestarzałej TI jest powstanie nowego typu barier związanych z brakiem informacji o możliwościach rozwoju poszczególnych branż i przedsiębiorstw. Efekty negatywne takiej informacyjnej bariery to między innymi spadek konkurencyjności firm polskich w stosunku do firm pochodzących z tych krajów, które taką nowoczesną TI posiadają. Problematyka ta jest przedmiotem obrad między innymi w Information Society Forum (ISF). Forum to powołane w 1995 roku jako niezależne ciało doradcze Komisji Europejskiej, którego zadaniem jest wyciąganie wniosków i formułowanie zaleceń dla wszystkich instytucji Europejskich. Według prac Komisji i opracowanego przez nią raportu wydatki na TI są niezbędne dla realizacji Europejskiej Drogi do Społeczeństwa Informatycznego. Europejska Droga to stawianie na silny rynek, nieustanną innowacyjność oraz wolny przepływ informacji i wiedzy. Wolny przepływ to również pole do nadużyć.

Tworzenie przestrzeni informacyjnej jako podstawowego elementu gospodarki informacyjnej wymaga przeznaczenia dość znacznych środków na budowę bezpiecznej infrastruktury zarządzania a więc na technologię informacyjną.

W warunkach Polski możliwości jakie niesie ze sobą TI są dużą szansą dla rozwoju przedsiębiorczości i przyspieszenia procesu gospodarczej integracji krajów Unii Europejskiej.

Globalne strategie organizacji mogą być w pełniejszy i łatwiejszy sposób realizowane dzięki gospodarce elektronicznej. Polska i inne kraje Europy środkowo – wschodniej korzystając z gospodarki elektronicznej mają większe możliwości stania się

konkurencyjnymi i kreatywnymi, niż w przypadku dotychczasowej tradycyjnej gospodarki rynkowej. Powstanie gospodarki elektronicznej jest wynikiem rozwoju informacyjnej technologii. Dzięki gospodarce elektronicznej organizacje pochodzące z krajów Europy środkowo-wschodniej mają możliwości funkcjonowania zarówno w wymiarze lokalnym jak i globalnym. Rozwój gospodarki elektronicznej to szansa wzrostu konkurencyjności tak małych, jak i dużych organizacji na rynku globalnym.

Jednak czy takie organizacje nie będą łatwiej wystawione na atak terrorystyczny? Szansa taka nie jest związana z lokalizacją organizacji. Jednak obok szans pojawiają się też nowe zagrożenia. Jak stwierdza G.Yip [1996] „umiejętność opracowania i realizacja strategii globalnej jest prawdziwym testem sprawności zarządzania organizacją”. Na całym świecie poszczególne organizacje dążą w stronę globalizacji rozumianej jako ekspansja na rynki zagraniczne. Problematyka ta jest tym bardziej aktualna, że, niezależnie od tego, czy poszczególne osoby chcą globalizacji czy też są jej przeciwnie, jest to naturalna droga rozwoju niemal wszystkich działów i gałęzi gospodarki narodowej.

Spośród wszystkich decyzji dotyczących tworzenia społeczeństwa informacyjnego oraz unowocześnienia funkcjonowania organizacji, właśnie decyzje dotyczące komputeryzacji systemów informacyjnych, czyli zastosowania systemów informatycznych zarządzania (MIS), wzbudzają największe kontrowersje.

Zagrożenie budowy społeczeństwa informacyjnego cyberterroryzm

Jak już wspomniano budowa społeczeństwa informacyjnego niesie różnego rodzaju niebezpieczeństwa. Ze względu na ograniczoną prezentację wybrano jeden o z nich ale bardzo silnie związanych z TI i jej rozwojem w kontekście budowy społeczeństwa informacyjnego. Jest to cyberterroryzm, którego powstanie łączy się z kluczowymi zagrożeniami bezpieczeństwa państwa jego obywateli. Analizując tzw. piramidę Masłowa [J. Kisielnicki 2008] widzimy, że dla ludzi zaraz po zaspokojeniu potrzeb fizjologicznych najważniejsze jest zaspokojenie potrzeb obronnych.

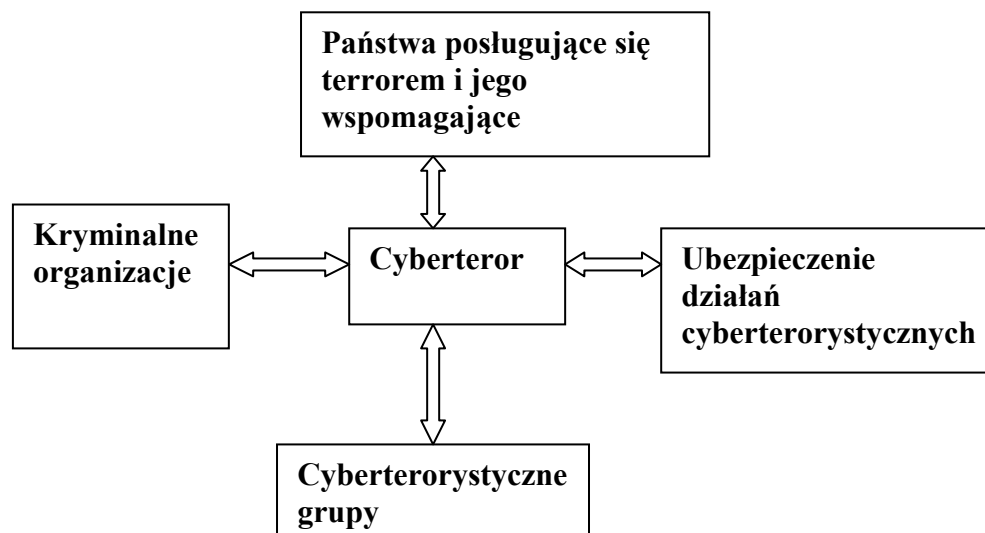
Dzięki rozwojowi TI z terroryzmu powstał cyberterroryzm.

Według eksperta w dziedzinie bezpieczeństwa cyberprzestrzeni i nowych technologii -na Uniwersytecie Georgetown w Waszyngtonie D.E. Denning [2000 i 2002], "Cyberterroryzm jest konwergencją cyberprzestrzeni i terroryzmu. Dotyczy nielegalnych ataków i gróźb ataków przeciwko komputerom, sieciom komputerowym i informacjom przechowywanych w nich by zastraszyć lub wymusić na rządzie lub społeczeństwie polityczne lub społeczne cele. By zakwalifikować atak jako cyberterroryzm powinien skutkować przemocą przeciwko ludziom lub mieniu lub przynajmniej wyrządzić wystarczająco szkody by stwarzać strach". W wikipedii pod tym hasłem można znaleźć następujące stwierdzenie:

Cyberterroryzm - spotykane w mediach oraz literaturze określenie opisujące posługiwanie się zdobyciami [technologii informacyjnej](#) w celu wyrządzenia szkody z pobudek politycznych lub ideologicznych, zwłaszcza w odniesieniu do infrastruktury o istotnym znaczeniu dla gospodarki lub obronności atakowanego kraju. W szerszym, ogólnym znaczeniu jest to [terroryzm](#). A. Bógdał-Brzezińska, M.F. Gawrych i [2003], piszą, że cyberterroryzm jest najbardziej nieprzewidywalnym sposobem oddziaływania

zorganizowanych grup na funkcjonowanie i stabilność struktur państwowych. Telekomunikacja, system energetyczny, system bankowy i finansowy, produkcja, magazynowanie oraz transport gazu ziemnego i ropy naftowej, transport, system zaopatrzenia w wodę, służby ratownicze itp systemy są często nazywane krytyczną infrastrukturą. Jej zniszczenie lub uszkodzenie może osłabić zdolność obronną oraz bezpieczeństwo ekonomiczne państwa, przerwać ciągłość funkcjonowania władzy i służb publicznych. Systemy te w nomenklaturze anglosaskiej są określane jako SCADA (Supervisory Control And Data Acquisition). Jak pisze L. Janczewski i A Colarik [2007] system należące do SCADA są znakomitym celem ataków cyberterrorystów ze względu na rolę jaką pełnią, ale nie tylko dlatego. Systemy SCADA są pochodną automatycznych systemów sterowania obiektami przemysłowymi. Te dawniejsze systemy funkcjonowały całkowicie autonomicznie. Fizyczny dostęp do nich był utrudniony (np sterowanie elektrownią wodą ze stanowiska kontrolnego umieszczonego na szczycie tamy). Wysiłek ich konstruktorów był ukierunkowany głównie na ich niezawodne działanie. Zastosowanie komputerów i telekomunikacji spowodowało, że funkcje sterownicze są realizowane zdalnie z wykorzystaniem ogólnodostępnych łączy i komputerów. Nie opracowano do tej pory właściwego zabezpieczenia systemów SCADA od zagrożeń zewnętrznych (np hackerów) i to stanowi ich zasadniczą wadę, czyli atrakcyjność dla cyberterrorystów.

K Kumalski [2009] zwraca uwagę na fakt, że wielu ludzi nie widzi różnicy pomiędzy terroryzmem [u nas cyberterroryzmem] a innymi formami zbrodni.. Różnica jest ogromna . Powoduje on bowiem reperkusje psychologiczne nie tylko u bezpośredniej ofiary. Przy pomocy rozgłosu zdobytego w wyniku przemocy dążą oni do zdobycia wpływów i władzy. Jest to akt kryminalny ale jego skutki najczęściej znacznie wykraczają poza granice klasycznego przestępstwa kryminalnego. Posługując się typologią podaną przez T Mockatis [2008] możemy głównych aktorów działań cyberterrorystycznych przedstawić jak na rysunku 1.



Rys 1 Aktorzy działalności terrorystycznej

Źródło: por T Mockatis [2008]

Wiele krajów powołały specjalne ośrodki zajmujące się ochroną systemów krytycznych (jak: USA, Anglia, Australia, Norwegia, Nowa Zelandia). Ośrodki te nie tylko są aktywne wewnątrz krajów, w jakich działają, ale bardzo ściśle ze sobą współpracują. Np w marcu 2008 miały miejsce międzynarodowe ćwiczenia obejmujące w/w kraje i mające na celu zbadanie wspólnych zdolności tych krajów do zwalczania ataków ukierunkowanych na systemy krytyczne. Ćwiczenia te nie są typu „sztuka dla sztuki”. Przykładem rzeczywistych zagrożeń mogą być wydarzenia z Estonii, z maja 2007. W wyniku konfliktowej decyzji władz estońskich przesunięcia pomnika upamiętniającego żołnierzy radzieckich poległych na tych terenach w czasie drugiej wojny światowej nastąpił zmasowany atak cybernetyczny na sieć informatyczna tego kraju. Szereg centralnych urzędów Estonii, wliczając ministerstwa i bank centralny było odciętych od świata przez wiele godzin. Atak ten był przeprowadzony spoza granic Estonii przez elementy pro-rosyjskie, przeciwne rządowi tego państwa. Nie ma do tej pory oficjalnych dowodów udziału rządu rosyjskiego w tych wydarzeniach. W wyniku tych wydarzeń na terenie Estonii powołano ośrodek NATO-wski zajmujący się cyberterroryzmem i wojnami cybernetycznymi. W Polsce funkcjonuje między innymi Centrum Badań nad Terroryzmem Collegium Civitas.

Terrorystyci z Al Kaidy w wydanym oświadczeniu wzięli odpowiedzialność za podjęte w roku 2003 działania, w konsekwencji których nastąpiła przerwa w dostawie zasilania w północnych częściach Stanów Zjednoczonych i południowych Kanady

(władze amerykańskie zaprzeczają udziałowi Al Kaidy w tych zakłóceniach) a także za dokonaną w tym samym roku (nie skuteczną zresztą) "Elektryczną blokadę Wielkiej Brytanii". Jak uspakajają w internecie takie organizacje jak CIA i FBI, infrastruktura obronna Stanów Zjednoczonych -broń atomowa i inne systemy wojskowe a także systemy informatyczne FBI i CIA są izolowane od Internetu, co czyni je niedostępnymi dla działających z "zewnątrz" hakerów czy cyberterrorystów. Działania hackerów lub innych osób posługujących się tzw narzędziami szpiegującymi ma na celu przygotowanie ataku cyberterrorystycznego. Te uzasadnienia są dosyć wątpliwego znaczenia ponieważ statystyka ataków na systemy informacyjne pokazuje, że praktycznie połowa tych ataków jest inicjowana wewnętrznie [L. Janczewski, A. Colarik 2005]. Warto dodać, że wiele „tradycyjnych” konfliktów ma swoje odpowiedniki cybernetyczne, np w czasie nasilenie konfliktów takich jak palestyński, indyjsko-pakistański, bałkański, itp odnotowuje się nasilenie ataków cybernetycznych (z obu stron).

O czyhającym na nas niebezpieczeństwie napisano wiele powieści pojawiło się wiele filmów, Mimo przytoczonych powyżej faktów nasuwa się pytanie: Czy osoby wskazujące na cyberterrorystyczny, jako realne zagrożenie dla bezpieczeństwa narodowego i międzynarodowego wkładają tylko swoją cegiełkę do „histerii terrorystycznej”, jaka ma miejsce po 11 września 2001 roku ? A może jednak cyberterrorystyczny w niedługim czasie ma szansę stać się jednym z największych wyzwań współczesnego świata? Pytania to możemy postawić, każdemu członkowi społeczności. Zabezpieczenie przed takim rodzajem ataku jest bardzo kosztowne i ogranicza naszą ‘wolność’ w budowie społeczeństwa informacyjnego. Jednak bardzo często jest one konieczne .

Wynika to z faktu, iż w przypadku takiego ataku skutki mogą mieć niewyobrażalne konsekwencje. Od 11 września 2001 roku wszyscy żyjemy w obawie następnych ataków. I jak musimy zdejmować buty przed bramkami kontroli na lotnisku nie buntujemy się. Obawiamy się Fatwe czyli wypowiedzenia świętej wojny, przez Osamy bin Ladena Ekstremiści nie tylko muzułmańscy są rozproszeni po całym niemal świecie, a ich przesłania to zachęcanie do przyłączenia się do wspólnej walki, Internet może być, efektywną drogą do realizacji tych celów . Dostępu do dowolnego punktu na świecie z każdego miejsca pozwala w konsekwencji na możliwość łatwego ,szybkiego, przesyłania nieograniczonej ilości propagandy pomaga ekstremistom jednoczyć i motywować się wzajemnie.

Sprawa nie jest taka prosta. B. Schneier opublikował w 2007 roku bardzo interesujący artykuł na ten temat. Jego myślą przewodnią było to, że uczucie zagrożenia bardzo często nie jest związane z rzeczywistym zagrożeniem. Jak to napisano powyżej transport lotniczy wydał wiele miliardów dolarów na ochronę pasażerów. Nastąpiło to w wyniku śmierci około 3 tysięcy ludzi w wypadkach lotniczych w ostatnim 10 leciu. Z drugiej strony od zatruc żywością umiera rocznie w USA około 5 tysięcy ludzi ale roczne wydatki agencji zajmującej się tymi sprawami liczy się tylko w dziesiątkach milionów dolarów. Uczucie zagrożenia jest złym motywem działania. Dodatkowo dużą negatywną rolę spełniają mass media nagłaśniające jakiegokolwiek działania terrorystyczne a pomijające trywialną (z ich punkty widzenia rzeczywistość). Terrorystyczny jest zbudowany na strachu a doniesienia prasowe na temat ataków terrorystycznych stanowią znakomite paliwo do podsycania tego uczucia. Informatyczna infrastruktura

tworzona w budowie społeczeństwa informacyjnego nie jest uodporniona na ataki z zewnątrz. W konsekwencji, cyberterrorysta ma szansę dostępu do celów z dowolnego punktu na ziemi, czy też z przestrzeni. Charakteryzując zagrożenia cyberterrorystyczne należy zwrócić uwagę na sieciową organizację działań i bezterytorialność.

Zależność społeczeństwa od TI tworzyła nowy rodzaj zagrożenia, którego świadomość zwróciła uwagę mass mediów, naukowców i informatyków. W warunkach Polski zagadnienie zabezpieczeń jest tym bardziej trudne, że informatyczna kultura nie jest zbyt wysoka.

Istnieje już wiele publikacji przestrzegających społeczeństwo przed cyberterroryzmem i zwracających uwagę na konieczność podejmowania działań ochronnych. I tak w jednym z nich cyberterrorystyczny atak na system komputerowy kontrolujący elektrownię, prowadzi do katastrofy skażenia radioaktywnego, w efekcie prowadząc do śmierci wielu niewinnych ludzi. W innym scenariuszu cyberterrorysty włamują się do systemu kierowania przestrzenią powietrzną i powodują kolizję cywilnych samolotów. Powstaje więc pytanie, czy zagrożenie przestrzeni cybernetycznej działalnością cyber-terrorystów czy też cyber-wojskowych jest realne czy też nie? Naszym zdaniem sytuacja jest prawie identyczna z pojawieniem się słynnego wirusa. milenijny czyli Y2K Bug. Wirus ten pojawił się w na przełomie roku 1999 i 2000. Zagrożenie było realne w skali światowej i wiele wysiłków zostało dokonanych, by ten wirus nie uaktywnił się na szerszą skalę. I rzeczywiście, z wybiciem zegara Nowego Milenium NIC SIĘ NIE STAŁO. Niektórzy nawet odczuwali zawód z tego powodu. Pewni obywatele USA, którzy w przewidywaniu chaosu socjalnego z tego powodu kupowali żywność (i, oczywiście, broń) i wypełniali nimi zaparkowane przed ich domami kontenery. Jednak nie ulega wątpliwości, że bez tych środków zapobiegawczych nie odnotowano większych zakłóceń. Podobne zagrożenie istnieje ze strony ataków cyberterrorystów ich zasięg może mieć szeroki zasięg, jeżeli nie podejmie się środków zapobiegawczych. Takie działania są już coraz częściej podejmowane w skali światowej i prawdopodobieństwo skutecznych ataków cyberterrorystów nie rośnie.

W wielu scenariuszach filmowych szczególnie w filmach o ataku na elektrownie atomowe, cyberterrorysty włamują się do systemu bankowego i kontrolują międzynarodowe transakcje finansowe i giełdy papierów wartościowych. System ekonomiczny załamuje się a społeczeństwo traci zaufanie do państwa i cel cyberterrorystów destabilizacja zostaje osiągnięta.

Zagrożenie cyberterroryzmem może się wielu wydawać wyolbrzymione, nie powinniśmy jednak je .go istnienia zaprzeczać czy ignorować

Uwagi końcowe

Budowa społeczeństwa informacyjnego jest faktem. Polska musi wejść do tego pociągu jeżeli ma ambicje bycia liczącym się krajem w Unii Europejskiej. Innych dróg nie ma dla zostania państwa demokratycznego i nowoczesnego. Musimy zdawać sobie jednak sprawę z konieczności poniesienie na ten cel znacznych nakładów i konieczności przeprowadzenia zmian w mentalności dość dużej grupie naszego społeczeństwa. Polska w zakresie TI nie należy do liderów, ale bez odpowiedniej

infrastruktury informatycznej będziemy na pewno pomijani przez zagranicznych inwestorów. Równocześnie należy zdawać sobie sprawę z pojawiających się nowych zagrożeń. Z nich jednym z najbardziej istotnych jest cyberterrorizm w różnych postaciach. Przeznaczając coraz to większe środki na TI i tworzenie społeczeństwa informacyjnego winniśmy również pamiętać przeznaczeniu części ich na działania anty cyberterrorystyczne.

Literatura

- Abramowicz W. Filtrowanie informacji, Wyd Akademia Ekonomiczna Poznań 2008
- Adamski A., Cyberterrorizm, [w:] materiały z Konferencji n/t terroryzmu 11.04.2002 r. Wydział Prawa UMK Toruń, Toruń 2002.
- Bangeman M. Raport Europa a globalne społeczeństwo informacyjne , Zalecenia dla Komisji Europejskiej . <http://kbn/icm/edu.pl/gsi/raport>
- Batorski D., Marody M., Nowak A. (red.), Społeczna przestrzeń Internetu, Wyd Akademia Warszawa 2006.
- Bell D., The Coming of Post-Industrial Society. A Venture in Social Forecasting, New York 1973.
- Bógdał-Brzezińska A., Gawrycki M.F., Cyberterrorizm i problemy bezpieczeństwa informacyjnego we współczesnym świecie, Fundacja Studiów Międzynarodowych, Warszawa, Oficyna wydawnicza ASPRA-JR, Warszawa 2003.
- Bógdał-Brzezińska A., Cyberterrorizm i problemy bezpieczeństwa informacyjnego we współczesnym świecie, Fundacja Studiów Międzynarodowych, Warszawa, Oficyna wydawnicza ASPRA-JR, Warszawa 2007
- Castells M., Galaktyka Internetu, Wyd Rebis seria Nowe Horyzonty Poznań 2003.
- Casey M. „Europejska polityka informacyjna, Międzynarodowe Centrum Zarządzania informacją, UMK, Toruń 2001
- Cellary W. (red.) Polska w drodze do globalnego społeczeństwa informacyjnego, UNDP, Warszawa 2002
- Czapiński J, Panek T, (red), Diagnoza społeczna , Wyd Wizja Warszawa 2007
- Colarik A, Cyber Terrorism: Political and Economic Implications , Idea Group, 2006
- Denning, D.E. Wojna informacyjna i bezpieczeństwo informacji Wydawnictwa Naukowo-Techniczne / Warszawa 2002
- Gawrycki M. F., Globalizacja w służbie antyglobalistów - "zapatyści" i rewolucja informacyjna, (w:) I. Łęcka (red.) Społeczne skutki globalizacji – globalizacja a bezpieczeństwo i zdrowie publiczne, Warszawa 2006;
- Goban-Klas, T. Edukacja wobec pokolenia SMSu, [w:] W. Strykowski, W. Skrzydlewski (red.), Media i edukacja w dobie integracji, EMPI2, Poznań 2002.

Globan-Klass T., Sienkiewicz P., Polska w drodze do globalnego społeczeństwa informacyjnego, Kraków 1999.

Kubicek, H. Möglichkeiten und Gefahren der "Informationsgesellschaft", 1999, <http://www.fgtk.informatik.uni-bremen.de/ig/WS99-00/studienbrief/index.html>

Janczewski, L., Colarik A., Cyber Warfare and Cyber Terrorism, New York, NY, USA, Information Science Reference, . 2007.

Janczewski L., Colarik A , Managerial Guide to Handling Cyber-Terrorism & Information Warfare, Hershey, PA, USA, IDEA Group Publishing, 300p, 2005

Kisielnicki, J; Informacyjna infrastruktura zarządzania, PWN, Warszawa.1994

Kisielnicki, J Zarządzanie , PWE, Warszawa 2008

Kumalski K. Problemy definicyjne pojęcia terroryzmu, , www.psz.pl 2008

Mockatis T. , The New Terrorism : Myths and Realists, Stanford University Press 2008

Oleński J, Informacyjna infrastruktura państwa w globalnej gospodarce, Wyd UW Warszawa 2006

Papińska – Kacperek, J, (red) Społeczeństwo informacyjne , PWN, Warszawa 2008

Schneier, B. The Psychology of security – draft, CRYPTO-GRAM, February 28, 2007

Wallace P., Psychologia Internetu, Poznań 2004.

Yip G.S., Strategia globalna, Światowa przewaga globalna

Zacher L. (red.), Społeczeństwo Informacyjne. Aspekty techniczne, społeczne i polityczne, Lublin–Warszawa 1992.

Zacher L.W Transformacje społeczeństw od informacji do wiedzy, C.H Beck Warszawa 2007