

Piotr Sienkiewicz

Bezpieczeństwo cyberprzestrzeni państwa

Ekonomiczne Problemy Usług nr 88, 802-809

2012

Artykuł został opracowany do udostępnienia w internecie przez Muzeum Historii Polski w ramach prac podejmowanych na rzecz zapewnienia otwartego, powszechnego i trwałego dostępu do polskiego dorobku naukowego i kulturalnego. Artykuł jest umieszczony w kolekcji cyfrowej bazhum.muzhp.pl, gromadzącej zawartość polskich czasopism humanistycznych i społecznych.

Tekst jest udostępniony do wykorzystania w ramach dozwolonego użytku.

PIOTR SIENKIEWICZ

Wydział Bezpieczeństwa Narodowego Akademii Obrony Narodowej
Warszawska Wyższa Szkoła Informatyki

BEZPIECZEŃSTWO CYBERPRZESTRZENI PAŃSTWA

Internet jest globalną siecią komunikacyjną, lecz sposób jego wykorzystania i jego ewolucyjna natura są produktem ludzkiego działania w określonych warunkach historycznych.

Manuel Castells

Obecnie cybergospodarka jest prawdziwą gospodarką. Jeśli uszkodzicie sieci komputerowe, zdeorganizujecie życie narodu.

Condoleezza Rice (2011)

Wprowadzenie

Przełom wieków uświadomił, że świat współczesny cechuje zagęszczenie przestrzeni społecznej, przyspieszenie procesów zmiany, kumulacja efektów ubocznych działań społecznych oraz wzrost kosztów redukcji niepożądanych ich skutków itp. Globalizacja i rozwój społeczeństwa informacyjnego, które zdominowały myślenie o przyszłości, powstały dzięki kumulacji innowacji w dziedzinie technologii informacyjnych, przyniosły także немало rozczarowań. Globalizacja, wraz z dominującą doktryną neoliberalizmu, nie uchroniła przed „globalnym kryzysem gospodarczym”, załamaniem kapitalizmu finansowego. Społeczeństwo informacyjne, wbrew licznym wróżbom, nie przekształciło się w społeczeństwo wiedzy, a zwłaszcza w „społeczeństwo mądrości”. Nie wytworzyły się jakieś szczególne formy nie tyle regulacji, co choćby wczesnego ostrzegania przed zagrożeniami globalnego i lokalnego bezpieczeństwa. Tworzyła się nowa przestrzeń bezpieczeń-

stwa, którą cechowała kumulacja dobrze zidentyfikowanych zagrożeń oraz takich, jak zjawisko terroryzmu. Rozwój technologii informacyjnych (ICT) przyniósł jedną z najdonioślejszych innowacji cywilizacyjnych w postaci Internetu, ale również nieznanne wcześniej zjawiska cyberprzestępstw, w tym cyberterrorystyczne zagrożenia bezpieczeństwa narodowego.

Zasadniczym celem artykułu jest refleksja nad istotą nowego bytu – cyberprzestrzeni (*cyberspace*), jej miejscem w opisie współczesności wraz z konsekwencjami zagrożeń bezpieczeństwa.

1. Technologiczny determinizm

Obecna rewolucja informacyjna jest czwartą rewolucją tego typu w historii ludzkości. Pierwszą było wynalezienie druku (ok. 5000 lat temu w Mezopotamii), drugą zapoczątkowało wynalezienie książki (ok. roku 1300 p.n.e. w Chinach), trzecią zaś wynalezienie przez Gutenberga (1456) maszyny drukarskiej z ruchomymi czcionkami. Czwartą rewolucję wiąże się na ogół z wynalazkiem komputera i powstaniem systemów łączności wykorzystujących energię elektryczną. Aczkolwiek wynalazek komputera wiąże się przede wszystkim z maszynami liczącymi Konrada Zusego (1943) i powstaniem ENIACA (1946), to należy dostrzegać wcześniejsze dokonania, np. Pascala, Leibniza, Schickarda, Babbage'a czy Holleritha, a także prace teoretyczne Alana Turinga i Johna von Neumanna. Rozwój systemów łączności wyznaczały wynalazki Chappe'a (telegraf semaforowy), Morse'a (telegraf), Bella (telefon), Marconiego (radio), Farnswortha (telewizja), telekomunikacji satelitarnej (1961) i sieci komputerowej (1969) (rys. 1).

Za początek „ery informacji” można przyjąć zarówno rok 1969 (transmisja telewizyjna z lądowca na Księżycu i uruchomienie sieci ARPANET), jak i rok 1990 (Internet i WWW), albo rok 1948 (cybernetyka N. Wienera i teoria informacji C. Shannona, wynalazek tranzystora). Ostatnia dekada XX wieku upłynęła natomiast pod wpływem rozwoju technologii internetowych, telefonii komórkowej, systemu GPS i innych, zaś początek obecnego stulecia przyniósł np. Web.2.0.

Rozwój technologii informacyjnych spowodował istotne zmiany struktur społecznych i był jednym z głównych czynników kształtowania się społeczeństwa sieci, rozumianego jako wariant społeczeństwa informacyjnego. Należy jednak zauważyć, że ludzie od zarania dziejów cywilizacji tworzyli różne struktury sieciowe, począwszy od sieci dróg pozwalających sprawniej przemieszczać się na lądzie, potem na wodzie, w powietrzu, wreszcie w przestrzeni kosmicznej. Rozwojowi sieci komunikacyjnych towarzyszył między innymi rozwój sieci przesyłania informacji. Sieciowość można uznać za cechę cywilizacji, wyraz postępującej złożoności rzeczywistości kształtowanej przez procesy technologiczne.

2. Cyberprzestrzeń

Internet postrzegany bywa jako najważniejsza innowacja od czasów Gutenberga, choć np. dla Stanisława Lema stanowił odpowiedź na pytanie jeszcze niepostawione. Stanowi zjawisko, fenomen współczesności, który zawiera w sobie niejednoznaczność, dwoistość, cechy pozytywne i negatywne jednocześnie. Takim fenomenem współczesności jest przestrzeń cybernetyczna – pojęcie często używane i jeszcze częściej nadużywane.

Leibniz określał przestrzeń jako „porządek współlistniejących rzeczy w tym samym czasie”. Obecnie przestrzeń miejsc zastępuje przestrzeń dynamicznych przepływów rozpuszczająca czas przez dezintegrację sekwencji wydarzeń i natychmiastowe komunikowanie, sytuujące społeczeństwo w wiecznej ulotności, gdyż – jak zauważa M. Castells – przestrzeń jest ekspresją społeczeństwa¹.

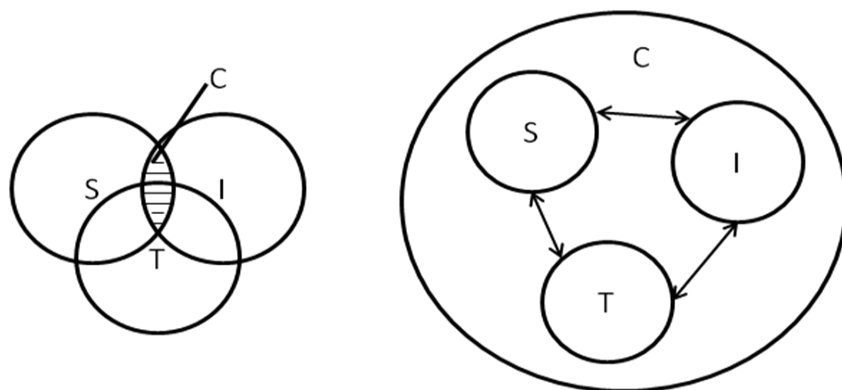
Tak rozumianą przestrzeń można określić mianem cybernetycznej, dostrzegając inspiracje wywodzące się z cybernetyki Wienera oraz prac Shannona, a to oznacza brak konieczności sięgania do postmodernistycznej literatury. Kojarzenie cyberprzestrzeni z Internetem to z pewnością najczęstsza i niepozabawiona racji, konstatacja. Jednakże, pomimo wszechobecności Internetu, jego natura, język i ograniczenia nie zostały dobrze poznane, z wyjątkiem kwestii ściśle technicznych.

Dążąc do uogólnień można przyjąć, że skumulowane na przełomie wieków innowacje technologiczne i organizacyjne przyniosły nową jakość w postaci konwergencji systemowych bytów, które można określić jako: socjosfera – infosfera – technosfera. Socjosfera to określona społeczność, która dzięki zaawansowanym technologicznie artefaktom (technosfera) wytwarza coraz większe zasoby informacyjne (infosfera) (rys. 1, tabela 1).

Zjawisko przedstawionej syntezy strukturalnej w skali globalnej przyniosło cyberprzestrzeń, czyli przestrzeń globalną, nieograniczoną czasem ani granicami geograficznymi czy politycznymi. Obecna technosfera utożsamiana jest z globalną siecią teleinformatyczną, czyli po prostu z Internetem.

Proponuje się przyjąć założenie o historycznej ewolucji cyberprzestrzeni (tabela 2): począwszy od wynalazku Gutenberga do obecnej dominującej roli Internetu. Z kolei do cech konstytutywnych cyberprzestrzeni należy zaliczyć sieciowość, zaś do cech potencjalnych – wirtualność.

¹ M. Castells, *Galaktyka Internetu*, Rebis, Poznań 2003.



Rys. 1. Dwa spojrzenia na cyberprzestrzeń (C) jako rezultat konwergencji socjosfery (S), infosfery (I) i technosfery (T)

Źródło: opracowanie własne.

Tabela 1

Ujęcia istoty cyberprzestrzeni (przykład)

PRZYKŁAD UJĘCIA	CHARAKTERYSTYKA
INTERNET	Teleinformatyczna sieć globalna tworzona przez zmienną w czasie liczbę sieci składowych (TCP/IP) o nieograniczonych otwartych zasobach i dostępnych usługach.
WIRTUALNA RZECZYWISTOŚĆ	System funkcjonujący w środowiskach wirtualnych i symulowanych światach. System, którego istotną cechą jest wirtualność.
MEGASIEĆ SPOŁECZNA	Globalna sieć tworzona przez systemy komunikowania społecznego funkcjonujące na globalnej platformie teleinformatycznej (Internet). Sieć złożona losowa.
EWOLUUJĄCY SYSTEM ZŁOŻONY	System o strukturze sieci złożonej o wieloelementowych i wielopoziomowych relacjach i wysokiej dynamice zmian liczby elementów i relacji.
REZULTAT SYSTEMOWEJ KONWERCENCJI	Wielki (globalny) system socjotechniczny, ukształtowany w procesie konwergencji systemów społecznych (socjosfera), systemów informacji (infosfera) i systemów teleinformatycznych (technosfera).

Źródło: opracowanie własne.

Natomiast, uwzględniając walory komunikacyjne współczesnych mediów, nie można pominąć takich cech jak: interaktywność, hipertekstowość i multimedialność. Jedną z przyczyn wyłonienia się tych cech była konwergencja systemów informatycznych, systemów telekomunikacyjnych i mediów elektronicznych.

Z punktu widzenia współczesnych badań systemowych istotne znaczenie mają cechy strukturalne i funkcjonalne systemu złożonego (*system of systems*) o strukturze „sieć sieci”, w której elementy (węzły sieci) oraz relacje (łuki sieci) powstają i znikają w procesie rozwoju systemu. Egzemplifikacją takiej sieci może być cyberprzestrzeń. Bardzo często eksponuje się związki cyberprzestrzeni z wirtualną rzeczywistością. Niekiedy dostrzega się w cyberprzestrzeni swoistą paradoksalność jej

obiektywnego i jednocześnie nieobiektywnego istnienia. Nie można jej odnieść do żadnego realnego miejsca, ale nie jest zupełnie nierealna, bowiem tworzą ją osoby, które komunikują się między sobą.

Można przyjąć, że cyberprzestrzeń jest obiektem wieloaspektowym wyrażającym jej złożoną i nie do końca rozpoznaną naturę (tabele 2 i 3).

Tabela 2

Model ewolucji cyberprzestrzeni (przykład)

FAZA ROZWOJU	OGÓLNA CHARAKTERYSTYKA
Cyberprzestrzeń – 0	„Galaktyka Gutenberga” (M. McLuhana) Rozwój drukowanego pisma oraz początki rozwoju telegrafii, telefonii, radia, telewizji.
Cyberprzestrzeń – 1	„Galaktyka Wienera” (P. Sienkiewicz) „Społeczeństwo informacyjne” (Masuda) Cybernetyczne koncepcje rozwoju systemów społecznych. Rozwój techniki cyfrowej, systemy komputerowe, łączność satelitarna (TELSTAR), sieć komputerowa (ARPANET), „boom PC” Sztuczna inteligencja
Cyberprzestrzeń – 2	„Galaktyka Internetu” (M. Castells) Internet (WWW). Gospodarka oparta na wiedzy. Globalizacja.
Cyberprzestrzeń – 3	„Galaktyka” (?) Internet (Web.2.0). Globalizacja sieci komunikowania społecznego. Nowe formy zachowań społecznych. „Społeczeństwo wiedzy” (?)

Źródło: opracowanie własne.

Tabela 3

Obszary specyficznych ograniczeń cyberprzestrzeni

OBSZAR	CHARAKTERYSTYKA
PRAWO (law)	prawo niejasne, niespójne niejasna odpowiedzialność za czyny i wykroczenia brak międzynarodowych (narodowych) kryteriów klasyfikacji i kwalifikacji nieprecyzyjne określenia aktów kryminalnych i aktów zagrożeń bezpieczeństwa narodowego
PRZESTRZEŃ (space)	brak granic przestrzennych brak granic politycznych brak granic geograficznych brak granic doraźnych
ZAGROŻENIA (threats)	prosta, ogólnie dostępna technologia anonimowość sprawcy wielość form cyberataków „efekt domina” jako skutek cechy „broni masowej dezorganizacji” niewielkie koszty ataków
BEZPIECZEŃSTWO (safety)	brak szybkich i skutecznych rozwiązań zabezpieczających mnogość obiektów zagrożeń (ataków) wysokie koszty zabezpieczeń zróżnicowana podatność obiektów nieprzewidywalność źródeł zagrożeń bardzo wysokie koszty

Źródło: opracowanie własne.

3. Bezpieczeństwo

Problem bezpieczeństwa informacyjnego obejmuje zarówno zabezpieczenia zasobów informacyjnych przed niedozwolonymi formami ingerencji obiektów (osób) niepożądanych, w tym ochronę informacji wrażliwych i danych osobowych, jak i różne formy zabezpieczenia systemów informatycznych (teleinformatycznych) przed rozpoznanymi destrukcyjnymi działaniami zewnętrznymi i wewnętrznymi obiektów.

O bezpieczeństwie cyberprzestrzeni można mówić, gdy istnieją niebezpieczeństwa, czyli zagrożenia, a więc sytuacje niepewne i ryzykowne, w których możliwa i prawdopodobna jest utrata wartościowych zasobów (informacyjnych, technicznych, programowych) częściowo lub w pełni, przez określonego ich dysponenta (właściciela, operatora, twórcę).

Można mówić o bezpieczeństwie cyberprzestrzeni na poziomie:

- społecznym (utrata określonych wartości w wyniku destrukcyjnych działań na określone zasoby infosfery i technosfery,
- informacyjnym (utrata wartościowych danych, informacji, wiedzy, bądź skutki niepożądanych destrukcyjnych działań na zasobach infosfery),
- technicznym (utrata bądź obniżenie niezawodności zasobów technologicznych i programowych tworzących technosferę).

Cyberprzestrzeń jest przestrzenią komunikowania społecznego, lecz nie tylko transinformowania (informowania wiernego), bowiem zachodzą tu procesy świadomego parainformowania, pseudoinformowania i dezinformowania².

Z punktu widzenia bezpieczeństwa można wyróżnić następujące rodzaje zagrożeń:

- naturalne (spowodowane przez „siły natury”),
- techniczne (będące następstwem zawodności systemów technicznych i programistycznych),
- społeczne, w tym:
 - nie będące aktem świadomej destrukcji,
 - będące aktem świadomej destrukcji z różnych pobudek (politycznych, ekonomicznych, emocjonalnych itp.).

Szczególne znaczenie ma ostatnia z wymienionych grup zagrożeń, gdyż ich przejawem są zjawiska, które mogą zakłócić ład społeczny, obniżając wartość systemu bezpieczeństwa narodowego, sprzyjając powstawaniu sytuacji konfliktowych i kryzysowych o różnej skali i intensywności (tabela 4).

Odrębnego znaczenia nabrały obecnie zagrożenia cyberprzestrzeni destrukcyjnie oddziałujące na poszczególne podsystemy (sektory) Krytycznej Infrastruktury

² M. Mazur, *Jakościowa teoria informacji*, WNT, Warszawa 1970.

ry Państwa, których efektywność działania w coraz większym zależy od efektywności teleinformatycznej infrastruktury, czyli technosfery cyberprzestrzeni.

Tabela 4

Podstawowe rodzaje cyberzagrożeń

ZJAWISKO	CECHY CHARAKTERYSTYCZNE
Cyberprzemoc	Wykorzystanie cyberprzestrzeni w celu wymuszania odbioru niepożądanych komunikatów zawierających informacje (dane, obrazy, treści) sprzeczne z wartościami adresata
Cyberprzestępstwo	Wykorzystanie cyberprzestrzeni w celu dokonania aktów kryminalnych pospolitych i zorganizowanych skierowanych na zasoby osób prywatnych i/lub organizacji (instytucji)
Cyberinwigilacja	Wykorzystanie cyberprzestrzeni w celu kontroli i/lub pozyskania informacji o zachowaniach i działaniach obywateli (społeczności, społeczeństwa) (efekt „Big Brother”)
Cyberterroryzm	Wykorzystanie cyberprzestrzeni w celu działań terrorystycznych (państwowych i pozapaństwowych)
Cyberdemokracja	Wykorzystanie cyberprzestrzeni w życiu politycznym państwa zgodnie z zasadami demokracji liberalnej (przeciwnieństwem – cyberterroryzm)
Cyberwojna	Wykorzystanie cyberprzestrzeni w celu realizacji działań politycznych realizowanych przez siły zbrojne (<i>cyberwarriors</i>) i skierowane na zasoby i struktury państwa przeciwnika (również w działaniach innych niż wojna)

Źródło: opracowanie własne.

Podsumowanie

Cyberprzestrzeń jest przestrzenią realizacji podstawowych wartości ludzkich we wszystkich sferach działań społecznych. Jest swoistą zapowiedzią nowej cywilizacji informacyjnej, której obecnym przejawem jest rozwój społeczeństwa informacyjnego. Jest także „ciemna strona” cyberprzestrzeni, jako źródła zagrożeń dla bezpieczeństwa międzynarodowego i narodowego. Musi być zatem przedmiotem racjonalnej polityki państwa, gdyż „cyberbezpieczeństwo” stanowi obecnie jeden z podstawowych filarów (segmentów) systemów bezpieczeństwa narodowego (regionalnego, globalnego). Istnieją bowiem systemy „cyberbroni” (*cyberweapons*), które w charakterze „broni” masowej dezorganizacji” mogą być efektywnym środkiem „cyberwojny” (*cyberwar, netwar*)³.

Istnieje jednakże pewnie szczególny aspekt myślenia o bezpiecznym, trwałym i zrównoważonym rozwoju państwa, a mianowicie wiążący się z bezpieczeństwem jego cyberprzestrzeni i dotyczący swoistości zmieniającej się socjosfery. Powstały społeczności, dla których cyberprzestrzeń jest realną przestrzenią realizacji życiowych szans, aspiracji, ale także gier i zabaw. Życie społeczne kolejny raz w historii ludzkości wyprzedza zasady i normy polityczne, prawne, obyczajowe. Nietrudno

³ Stowarzyszenie Euro-Atlantyckie (SEA) zorganizowało 7.10.2011 r. debatę nt. „Bezpieczeństwo cyberprzestrzeni RP”, którą prowadził autor artykułu.

przewidzieć powstanie nowej przestrzeni konfliktów i kryzysów społecznych, zagrożeń, ale również wyjątkowych szans.

Literatura

- 1 Ball P., *Masa krytyczna*, Insignis, Kraków 2007.
- 2 Castells M., *Spoleczeństwo sieci*, PWN, Warszawa 2010.
- 3 Castells M., Himanen P., *Spoleczeństwo informacyjne i państwo dobrobytu*, Wyd. Krytyki Politycznej, Warszawa 2009.
- 4 Goban-Klas T., Sienkiewicz P., *Spoleczeństwo informacyjne – szanse, zagrożenia, wyzwania*, Kraków 1999.
- 5 Sienkiewicz P., *Modele i metafory w badaniach społeczeństwa informacyjnego*, Zeszyty Naukowe nr 650, tom I, Uniwersytet Szczeciński, Szczecin 2011.
- 6 Dijk von J., *Spoleczne aspekty nowych mediów*, PWN, Warszawa 2010.
- 7 Świeboda H., *Zagrożenia bezpieczeństwa informacyjnego RP*, AON, Warszawa 2009.

STATE CYBERSPACE SECURITY

Summary

The author of the article proposes a model of cyberspace as a category of description of contemporary information society. Main threats of cyberspace security were discussed, e.g. cyberterrorism.

Translated by Magdalena Witecka