Zeszyty Naukowe AON nr 2(99) 2015
ISSN 2299-6753

POTĘGA CYBERNETYCZNA PAŃSTW – POMIAR I ZASTOSOWANIE

dr Robert BIAŁOSKÓRSKI
Wydział Humanistyczny Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach

Streszczenie

Artykuł porusza problem pomiaru potęgi cybernetycznej państw na przykładzie dwóch modeli badawczych: modelu Cyber Power Index (CPI) oraz modelu A.M. Gomeza. Obie metody oparte są na analizie wskaźników, przy czym pierwszy model szacuje wyłącznie defensywną potęgę cybernetyczną, natomiast drugi zarówno jej wymiar defensywny, jak i ofensywny. Oba te wymiary cyberpotęgi stanowią obecnie główne determinanty kierunków poszukiwań rozwiązania ww. problemu badawczego. Ponadto model drugi służy do szacowania strategii państw w cyberprzestrzeni, spośród trzech wyróżnionych: – utrzymania potęgi cybernetycznej; – osiągania równowagi; – demonstrowania potęgi cybernetycznej. Prezentowane wyniki badań obu modeli różnią się dość znacznie, co potwierdza złożoność problematyki już w fazie koncepcyjnej i konieczność dalszych poszukiwań.

Słowa kluczowe: cyberprzestrzeń, potęga cybernetyczna, pomiar, model

Wstęp

Współczesna rewolucja informacyjna oparta jest na globalnej zależności od technologii informacyjno-komunikacyjnej (ang. *Information and Communication Technology*, ICT). Kształtujące się społeczeństwo informacyjne dysponuje coraz większymi zdolnościami i możliwościami oddziaływania w cyberprzestrzeni, stwarzającymi zarówno szanse, jak i zagrożenia. Dotyczy to wszystkich podmiotów systemu międzynarodowego, zarówno rządowych jak i pozarządowych. Każdy podmiot może być zarówno sprawcą, jak i ofiarą cyberzagrożeń, takich jak: cyberwojna, cyberszpiegostwo, cyberterroryzm i cyberprzestępczość[1], których identyfikacja stanowi jeden z głównych problemów cyberbezpieczeństwa[2]. W tej sytuacji problem pomiaru potęgi cybernetycznej stanowi jeden z kolejnych czynników istotnych przy szacowaniu potęgi państw. W artykule podjęto problematykę definiowania potęgi cybernetycznej państwa oraz metod jej pomiaru. Inspiracją do podjęcia badań był ich nowatorski charakter, brak opracowań w polskim piśmiennictwie naukowym oraz zakres zgodny z głównym kierunkiem zainteresowań naukowych autora problematyką zapobiegania konfliktom zbrojnym (ang. *conflict prevention*, CP) definiowanym jako: proces wczesnego ostrzegania i reagowania prewencyjnego, polegający na stałym monitorowaniu i analizowaniu rozwoju zdarzeń w rejonach ryzyka konfliktu zbrojnego (wczesne ostrzeganie) oraz bieżącym wypracowywaniu i podejmowaniu akcji prewencyjnych (reagowanie prewencyjne) w celu zapobiegania konfliktom zbrojnym[3]. Z uwagi na złożoność podjętej problematyki artykuł przedstawia jedynie zarys problemu badawczego, który wymaga pogłębionych studiów teoretycznych oraz badań empirycznych.

[1] Zob. R. Białoskórski, *Cyberzagrożenia w sìrodowisku bezpieczeniìstwa XXI wieku,* Wyd. WSCiL, Warszawa 2011.

[2] Autor zaproponował konceptualną analizę cyberzagrożeń opartą na analizie czterech czynników: podmiotu atakującego, podmiotu atakowanego, celów oraz motywacji. Zob. R. Białoskórski, *Cyberthreats in the Security Environment of the 21st Century,* „Journal of Security and Sustainability Issues" 2012*,* nr 4, s. 255–258.

[3] R. Białoskórski, *Modelowanie konfliktów zbrojnych z wykorzystaniem procesu analizy hierarchicznej – kazus syryjski* [w:] M. Sułek (red.), *Potęgometria*, t. II, Wyd. Europejskie Centrum Analiz Geopolitycznych, Warszawa 2015, s. 52.

Pojęcie potęgi cybernetycznej

Definicja „potęgi cybernetycznej" jest ściśle związana z pojęciem „cyberprzestrzeni". Mattiolli Rossella uważa, iż trudno jest określić granice pomiędzy cyberprzestrzenią i cyberbezpieczeństwem, głównie ze względu na dynamiczny charakter cyberprzestrzeni i brak klasycznie pojmowanych atrybutów terytorialności[4]. Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej definiuje bezpieczeństwo cyberprzestrzeni jako: (…) zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mający na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni"[5]. W literaturze przedmiotu cyberprzestrzeń jest w zasadzie definiowana, jako: 1) *globalna przestrzeń informacyjna*, rozumiana jako „przestrzeń wirtualna, w której odbywa się komunikacja między komputerami połączonymi w sieć internetową"[6] lub „przestrzeń otwartego komunikowania się za pośrednictwem połączonych komputerów i powiązań informatycznych pracujących na całym świecie z uwzględnieniem wszystkich systemów komunikacji elektronicznej (w tym również klasycznej sieci telefonicznej), które przesyłają informacje pochodzące ze źródeł numerycznych lub przeznaczone do numeracji"[7] oraz 2) *strategiczny element systemu bezpieczeństwa państwa*, jako: „wrażliwy system – system kontroli państwa… składający się z setek tysięcy sprzężonych ze sobą komputerów, serwerów, przełączników i kabli światłowodowych, wprawiających w działanie infrastrukturę krytyczną"[8] lub „niezależna sieć infrastruktury technologii informacyjnej, obejmująca Internet, sieci telekomunikacyjne, systemy komputerowe oraz wbudowane procesory i kontrolery działające w krytycznej infrastrukturze przemysłowej"[9] lub „militarna przestrzeń operacyjna (obok: lądowej, powietrznej, morskiej i kosmicznej)"[10]. Biorąc powyższe pod uwagę, można wprost skonkludować, że *cyberprzestrzeń to globalna przestrzeń informacyjna, stanowiąca strategiczny element systemu bezpieczeństwa państwa*, i taką też definicję cyberprzestrzeni przyjmuje autor w ramach konwencji terminologicznej badanego problemu[11]. Nie należy jednak przy tym zapominać o rosnącym znaczeniu pozapaństwowych podmiotów transnarodowych, które także coraz aktywniej wykorzystują cyberprzestrzeń dla swoich celów, nie zawsze zbieżnych z celami państw, na terytorium których operują[12]. Autor w konwencji terminologicznej artykułu przyjął koncepcję realizmu z teorii stosunków międzynarodowych, zakładającą państwo unitarne jako jedyny podmiot stosunków międzynarodowych o anarchicznym charakterze, zwracając jednocześnie uwagę na nurt liberalny, zgodnie z którym w systemie międzynarodowym m.in. wzrasta znaczenie podmiotów niepaństwowych, takich jak: międzynarodowe organizacje pozarządowe (ang. *International Non-Governmental Organizations*, INGOs) oraz jednoznacznie negatywne podmioty transnarodowe, do których autor zaliczył – międzynarodowe organizacje terrorystyczne (ang. *International Terrorist Organizations*, ITOs) i międzynarodowe grupy przestępcze (ang. *International Criminal Groups*, ICGs). W najbliższym czasie należy oczekiwać eksplozji ich aktywności w cyberprzestrzeni, zwłaszcza ITOs, które dotychczas wykorzystują ją głównie dla celów medialnych, werbunkowych i łączności operacyjnej. Decyduje o tym przede wszystkim stosunkowo niewielki koszt dostępu do cyberbroni, przy jednoczesnych olbrzymich możliwościach jej destrukcyjnego oddziaływania,

[4] R. Mattioli, *The «State(s)» of Cybersecurity* [w:] G. Giacomello (red.), *Security in Cyberspace*, New York, London, New Delhi, Sydney, Bloomsbury, 2014, s. 27.

[5] *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, 25 czerwiec 2013, http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html (dostęp: 27.01.2015).

[6] *Słownik Języka Polskiego*, http://sjp.pwn.pl/sjp/cyberprzestrzeń;2553915 (dostęp: 27.01.2015).

[7] *Słownik komputerowy i encyklopedia informatyczna*, http://www.i-slownik.pl/323,cyberprzestrzen (dostęp: 27.01.2015).

[8] *The National Strategy to Secure Cyberspace*, The White House Washington, luty 2003, p. vii, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (dostęp: 27.01.2015).

[9] *National Security Presidential Directive/NSPD-54 Homeland Security Presidential Directive/HSPD-23*, 8 styczeń 2008, p. 7g, https://epic.org/privacy/cybersecurity/EPIC-FOIA-NSPD54.pdf (dostęp: 27.01.2015).

[10] *Department of Defense Strategy for Operating in Cyberspace*, lipiec 2011, http://www.defense.gov/news/d20110714cyber.pdf (dostęp: 27.01.2015).

[11] Konwencja terminologiczna jest umową pomiędzy autorem i czytelnikami odnośnie do definicji terminów, obowiązujących autora w całej publikacji, M. Mazur, *Cybernetyka i charakter*, wyd. 2, Wyd. AULA, Podkowa Leśna 1996, s. 27–28.

[12] Zob. E. Panas, *Potęga transnarodowych organizacji społeczeństwa obywatelskiego* [w:] M. Sułek (red.), *Potęgometria*, tom I, Wyd. Europejskie Centrum Analiz Geopolitycznych, Warszawa 2013, s. 78–94.

porównywanych niekiedy do skutków broni masowego rażenia. Zagadnienie szacowania potęgi cybernetycznej podmiotów niepaństwowych jest równie istotne jak państwowych i wymaga podjęcia wnikliwych studiów, tym bardziej, że problematyka ta w literaturze przedmiotu praktycznie nie występuje[13]. Niezależnie więc od silnych i słabych stron konkretnych definicji cyberprzestrzeni, takie jej postrzeganie plasuje ją w sferze bezpieczeństwa państwa (także w wymiarze międzynarodowym), w sferze ochrony i bezpieczeństwa rządowych sieci informacyjnych i infrastruktury krytycznej państwa[14]. W wymiarze operacyjnej przestrzeni bezpieczeństwa[15] cyberprzestrzeń wyróżnia m.in. fakt, iż jej użytkownicy (indywidualni i zorganizowani) są jednocześnie jej kreatorami oraz jej odmienna fizyczna charakterystyka (tworzenie, gromadzenie, przekształcanie, wymiana i wykorzystywanie przepływu informacji drogą elektroniczną), która silnie oddziałuje na wszystkie pozostałe przestrzenie operacyjne (lądową, powietrzną, morską i kosmiczną) tradycyjnie pojmowane w sensie przestrzeni geograficznych. Cyberprzestrzeń jest od nich nie tylko o wiele bardziej dynamiczna i nieprzewidywalna, ale można ją też po prostu włączyć lub wyłączyć[16].

Daniel T. Kuehl, definiując potęgę cybernetyczną państwa, szukał inspiracji w analogii do pionierskich pojęć potęg morskiej i powietrznej, których główną ideą jest zdolność do użycia i wykorzystania danego środowiska dla określonych celów. To doprowadziło go do konstatacji, że *potęga cybernetyczna to zdolność do użycia cyberprzestrzeni w celu wywarcia wpływu na zdarzenia we wszystkich przestrzeniach operacyjnych oraz uzyskania przewagi we wszystkich tworzących cyberpotęgę czynnikach*[17]. Pomiar potęgi cybernetycznej odnosi się więc wprost do pomiaru własności tego środowiska. Do jego głównych wskaźników badacz ten zaliczył: 1) wskaźnik zdolności technologicznych (stale zmienny i różny w dyspozycji różnych użytkowników – państwowych i niepaństwowych) oraz 2) wskaźnik zdolności organizacyjnych.

Joseph S. Nye definiuje z kolei potęgę cybernetyczną jako: zdolność do osiągania zakładanych celów za pomocą sprzężonych w cyberprzestrzeni elektronicznych zasobów informacyjnych[18]. Badacz ten rozpatruje cyberpotęgę w wymiarach wewnętrznych i zewnętrznych oddziaływań informacyjnych (wirtualnych) i fizycznych generujących cybernetyczną siłę miękką (ang. *soft power*) oraz twardą (ang. *intra cyberspace hard power*)[19]. Przykładowo – w wymiarze wewnętrznych oddziaływań informacyjnych możemy mieć do czynienia z miękką siłą cybernetyczną w postaci systemu norm i standardów oraz z twardą siłą w postaci cyberataków[20] typu DoS/DDoS (tabela 1).

Tabela 1

Wirtualny i fizyczny wymiar potęgi cybernetycznej

	Wewnętrzna potęga cybernetyczna	Zewnętrzna potęga cybernetyczna
Instrumenty informacyjne	Twarda: ataki typu DoS (ang. *Denial of Service*)/DDoS (ang. *Distributed Denial of Service*)[1] Miękka: system norm i standardów	Twarda: ataki na systemy SCADA (ang. *Supervisory Control And Data Acquisition*)[2] Miękka: działania dyplomatyczne wpływające na opinię publiczną
Instrumenty fizyczne	Twarda: rządowa kontrola przedsiębiorstw Miękka: działania wspierające ruchy obrońców praw człowieka	Twarda: ataki na routery lub magistrale sieciowe Miękka: działania szkalujące cyber-dostawców

[1] Atak DoS polega na zmasowanym wysyłaniu do atakowanego systemu komputerowego tak dużej ilości danych, że nie jest on w stanie ich obsłużyć, co spowalnia lub paraliżuje jego działanie. W ataku rozproszonym DDoS bierze udział duża liczba komputerów atakujących, nad którymi

[13] R. Białoskórski, Cyberthreats…, op. cit., s. 252–253. Zob. E. Panas, *Potęga transnarodowych organizacji społeczeństwa obywatelskiego* [w:] M. Sułek (red.), *Potęgometria*, tom I, Wyd. Europejskie Centrum Analiz Geopolitycznych, Warszawa 2013, s. 78–94.

[14] D.T. Kuehl, *From Cyberspace to Cyberpower: Defining the Problem* [w:] D. Kramer, H. Stuart, L.K. Wentz, *Cyberpower and National Security Policy*, National Defense University, Potomac Books, Inc., 2009, http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf (dostęp: 27.01.2015), s. 2.

[15] Pojęcie operacyjności oznacza w tym przypadku praktyczne działanie w danym miejscu i czasie (Ibidem, przyp. 13).

[16] Zob. G.J. Rattray, *An Environmental Approach to Understanding Cyberpower*, 13 styczeń 2015, http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-10.pdf (dostęp: 27.01.2015).

[17] D.T. Kuehl, *From Cyberspace…*, s. 12.

[18] J.S. Nye, *Cyber Power*, Cambridge: Harvard Kennedy School, 2010), http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf (dostęp: 27.01.2015), s. 3–4.

[19] Ibidem, s. 3.

[20] Cyberatak (atak cybernetyczny) to najogólniej celowe zakłócenie prawidłowego funkcjonowania cyberprzestrzeni, *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, s. 6. W artykule pojęcie to dotyczy szerszych działań w ramach operacji informacyjnych.

przejęto wcześniej kontrolę (np. zombie). R. Białoskórski, *Bezpieczeństwo informacji. Słownik pojęć i skrótów*, Wyd. Ubezpieczeń, Warszawa 2010, s. 47–48.

[2] SCADA jest systemem nadzorującym przebieg procesu technologicznego lub produkcyjnego, polegający na zbieraniu aktualnych danych (pomiary), ich wizualizacji, sterowaniu procesem, alarmowaniu oraz archiwizacji danych, http://pl.wikipedia.org/wiki/SCADA (dostęp: 27.01.2015).

Źródło: J.S. Nye, op. cit., s. 3.

Badacz ten proponuje również trzy warianty potęgi cybernetycznej[21], a mianowicie:

Wariant 1: (A zmienia strategię B, której B początkowo nie planowało)

Twarda siła: ataki DoS, złośliwe oprogramowanie (ang. *malware*), ataki na systemy sterujące procesami przemysłowymi SCADA, aresztowania blogerów;

Miękka siła: kampanie informacyjne ukierunkowane na zmianę preferencji hakerów, rekrutowanie członków organizacji terrorystycznych.

Wariant 2: (Agenda sterująca: A zmienia podjętą przez B strategię)

Twarda siła: zapory sieciowe (ang. *firewalls*), filtry, naciski na firmy;

Miękka siła: dostawcy usług internetowych (ang. *Internet Service Providers*, ISPs), Internetowa Korporacja ds. Nadanych Nazw i Numerów (ang. *The Internet Corporation for Assigned Names and Numbers*, ICAAN), ogólnie akceptowane standardy oprogramowania.

Wariant 3: (A wpływa prewencyjnie na strategię B, w taki sposób, że B nie rozpatruje niekorzystnych dla A decyzji)

Twarda siła: ściganie blogerów łamiących prawo;

Miękka siła: informowanie preferencyjne (np. stymulujące nacjonalizm i „patriotyczne hakerstwo"), normy budzące odrazę (np. pornografia dziecięca).

Brak powszechnie uznanych definicji potęgi cybernetycznej oznacza, że badacze zajmujący się problemem jej pomiaru powinni każdorazowo przyjmować własną konwencję terminologiczną, stosownie do przyjętej metody badawczej.

Pomiar potęgi cybernetycznej państw

Potęga cybernetyczna może być rozpatrywania w sensie defensywnym i wówczas mamy do czynienia z defensywną potęgą cybernetyczną (ang. *defensive cyber power*, DCP) oraz w sensie ofensywnym w postaci – ofensywnej potęgi cybernetycznej (ang. *offensive cyber power*, OCP). Powyższy czynnik m.in. determinuje kierunki koncepcji metod pomiaru potęgi cybernetycznej, nawet jeśli nie jest on wyrażony *expressis verbis*, jak to ma miejsce w omówionym przykładowo modelu CPI.

Model CPI

Koncepcja modelu pomiaru potęgi cybernetycznej CPI (ang. *Cyber Power Index*) opracowana została przez zespół wywiadu ekonomicznego (ang. *The Economist Intelligence Unit*, EIU) renomowanego czasopisma „The Economist" we współpracy z konsorcjum Booz Allen Hamilton. Jego celem jest tworzenie rankingów zdolności cybernetycznej państw grupy G20 w zakresie zapobiegania i przeciwdziałania atakom cybernetycznym oraz promowanie problematyki cyberbezpieczeństwa w środowisku międzynarodowym. Jest to więc *de facto* model pomiaru defensywnej potęgi cybernetycznej (DCP).

Polega on na obliczaniu wskaźników potęgi cybernetycznej państw. W tym celu opracowano matrycę 39 ilościowych i jakościowych wskaźników pogrupowanych w 4 kategorie oraz 19 podkategorii z uwzględnieniem ich średnich wag (tabela 2). Matryca została opracowana w maju 2011 roku metodą ocen ekspertów[22]. Każdy ze wskaźników otrzymuje przyznane przez ekspertów wartości w skali rosnącej od 0 do 100, gdzie 100 oznacza największą wartość potęgi cybernetycznej. Repozytoria danych stanowią narodowe i międzynarodowe źródła statystyczne, w tym: The Economist Intelligence Unit (EIU); The UN Educational, Scientific and Cultural Organization (UNESCO); The International Telecommunications Union (ITU); The World Bank (WB).

[21] J. Nye, op. cit., s. 7.

[22] Metoda ocen ekspertów wymaga przede wszystkim starannego doboru ekspertów, najczęściej na podstawie kryteriów formalnych (stopień naukowy, doświadczenie zawodowe, dorobek naukowy, nagrody) lub społeczno-moralnych (dobra opinia współpracowników, rzetelność, uczciwość, bezkompromisowość). W opracowaniu uśrednionej oceny grupowej należy uwzględnić różnice w ocenach ekspertów indywidualnych (większa swoboda wypowiadania się i prezentowania wyników) i grupowych (możliwe psychologiczne zahamowania) oraz aspekty etyczne. Zob. M. Sułek, *Metody i techniki badań stosunków międzynarodowych*, Oficyna Wyd. ASPRA-JR, Warszawa 2004, s. 167–174.

Tabela 2

Matryca wskaźników i wag potęgi cybernetycznej modelu CPI[1]

Kategoria wskaźników	Waga [%]	Podkategoria wskaźników	Waga [%]	Wskaźniki
I. Wskaźniki prawno-regulacyjne	26,3	I.1. Wskaźniki rządowych zdolności cybernetycznych	27,1	1. Wskaźnik narodowych programów cybernetycznych
				2. Wskaźnik publiczno-prywatnego cyberpartnerstwa
		I.2. Wskaźniki polityki cyberbezpieczeństwa	24	3. Wskaźnik organów wykonawczych
				4. Wskaźnik regulacji prawnych
				5. Wskaźników zdolności zwalczania cyberprzestępczości
				6. Wskaźnik zobowiązań prawnomiędzynarodowych
				7. Wskaźnik planów cyberbezpieczeństwa
		I.3. Wskaźnik cybercenzury	15,5	8. Wskaźnik cybercenzury
		I.4. Wskaźnik skuteczności politycznej	15,5	9. Wskaźnik skuteczności politycznej
		I.5. Wskaźnik ochrony praw autorskich	17,8	10. Wskaźnik ochrony praw autorskich
II. Wskaźniki społeczno-ekonomiczne	25	II.1. Wskaźniki poziomu wykształcenia	25,2	11. Wskaźnik liczby słabych studentów do ogólnej liczby studentów
				12. Wskaźnik liczb lat nauki
		II.2. Wskaźniki sprawności technicznej	27,4	13. Wskaźnik wzrostu wydajności pracy
				14. Wskaźnik liczby badaczy w sektorze badań i rozwoju (BR) na milion mieszkańców
				15. Wskaźnik liczby naukowców i inżynierów
				16. Wskaźnik poziomu znajomości j. angielskiego
		II.3. Wskaźniki handlowe	17,3	17. Wskaźnik procentowy eksportu technologii informacyjno-komunikacyjnej do eksportu całkowitego
				18. Wskaźnik procentowy importu technologii informacyjno-komunikacyjnej do importu całkowitego
				19. Wskaźnik wolności handlu
		II.4. Wskaźniki innowacyjności	30,1	20.Wskaźnik procentowy udziału sektora badań i rozwoju (BR) w PKB
				21. Wskaźnik patentowy
				22. Wskaźnik procentowy udziału sektora własności prywatnej i z kapitałem mieszanym w PKB
III. Wskaźniki infrastruktury technologicznej	26,3	III.1. Wskaźniki dostępu do technologii informacyjno-komunikacyjnych	20,3	23. Wskaźnik dostępności internetu
				24. Wskaźnik dostępności telefonii mobilnej
				25. Wskaźnik procentowy punktów Wi-Fi na milion mieszkańców
				26. Wskaźnik dostępności portali społecznościowych
		III.2. Wskaźniki jakości technologii informacyjno-komunikacyjnych	21,9	27. Wskaźnik liczby abonentów internetu szerokopasmowego na 100 mieszkańców
				28. Wskaźnik dostępności międzynarodowego Internetu szerokopasmowego
		III.3. Wskaźnik procentowy nakładów na technologie informatyczno-komunikacyjne do PKB	20,3	29. Wskaźnik procentowy nakładów na technologie informatyczno-komunikacyjne do PKB
		III.4. Wskaźniki przystępności technologii informacyjno-komunikacyjnych	11,7	30. Wskaźnik taryf telefonii mobilnej
				31. Wskaźnik taryf Internetu szerokopasmowego
		III.5 Wskaźnik bezpieczeństwa serwerów	25,8	32. Wskaźnik bezpieczeństwa serwerów
IV. Wskaźniki zastosowań przemysłowych	22,5	IV.1. Wskaźnik inteligentnych sieci	21,1	33. Wskaźnik inteligentnych sieci
		IV.2. Wskaźnik E-Zdrowia	16,2	34. Wskaźnik E-Zdrowia

[1] Szczegółowy opis definicji oraz zasad przydzielania wartości poszczególnym wskaźnikom znajduje się w materiale źródłowym EIU w załączniku II na s. 26–32.

Kategoria wskaźników	Waga [%]	Podkategoria wskaźników	Waga [%]	Wskaźniki
		IV.3. Wskaźniki zastosowań komercyjnych	30,4	35. Wskaźnik procentowy liczby firm oferujących zamówienia przez Internet do ogólnej liczby firm wykorzystujących Internet w działalności biznesowej
				36. Wskaźnik procentowy liczby indywidualnych klientów składających zamówienia przez Internet do ogólnej liczby internautów
				37. Wskaźnik procentowy liczby indywidualnych klientów bankowości elektronicznej do ogólnej liczby internautów
		IV.4. Wskaźnik inteligentnych systemów transportowych	21,1	38. Wskaźnik inteligentnych systemów transportowych
		IV.5. Wskaźnik administracji elektronicznej	11,3	39. Wskaźnik administracji elektronicznej

Źródło: *Cyber Power Index. Findings and Methodology*, Economist Intelligence Unit, 2011, http://www.boozallen.com/content/dam/boozallen/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf, s. 22, 24.

Wagi poszczególnych kategorii wskaźników są zbliżone z nieznaczną dominacją kategorii wskaźników prawno-regulacyjnych i kategorii wskaźników infrastruktury technologicznej (*ex aequo* 26,3) przed kategorią wskaźników społeczno-ekonomicznych (25) oraz kategorią zastosowań przemysłowych (22,5).

Analizie poddano miary potęg cybernetycznych 19 państw z grupy G20 (bez Unii Europejskiej) reprezentujących pięć regionów geograficznych: Europę Zachodnią, Europę Wschodnią i Azję Środkową, Bliski Wschód i Afrykę, Azję i Pacyfik oraz Amerykę.

Wartości wskaźników są w odpowiedni sposób normalizowane i sumowane według kategorii.

Wskaźniki sprzyjające potędze cybernetycznej (np. wzrost wydatków na BR) są normalizowane zgodnie z regułą:

$$x = \frac{x - Min(x)}{Max(x) - Min(x)}$$

gdzie: *Min(x)* – minimalna wartość danego wskaźnika gospodarczego w grupie 19 państw;

Max(x) – maksymalna wartość danego wskaźnika gospodarczego w grupie 19 państw.

W ten sposób znormalizowane wartości są przekształcane z przedziału 0–1 do przedziału 0–100, co umożliwia ich bezpośrednie porównanie z innymi wskaźnikami, w taki sposób, iż państwo o najwyższym wskaźniku przyjmuje wartość 100, a o najniższym wskaźniku wartość 0.

Tabela 3

Wydatki na badania i rozwój w stosunku do PKB

Państwo	Udział BR w PKB
Republika Korei	4,04
Japonia	3,39
Niemcy	2,93
Stany Zjednoczone	2,79
Australia	2,39
Francja	2,26
Chiny	1,98
Kanada	1,73
Wielka Brytania	1,72
Włochy	1,27
Brazylia	1,21
Rosja	1,12
Turcja	0,86
Indie	0,81
RPA	0,76
Argentyna	0,65
Meksyk	0,43
Arabia Saudyjska	b.d.
Indonezja	b.d.

Źródło: The World Bank, Research and development expenditure (% of GDP), http://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS (dostęp: 15.10.2015).

Wskaźniki niesprzyjające potędze cybernetycznej (np. taryfy telefonii mobilnej czy taryfy Internetu szerokopasmowego) są normalizowane z nieco inną regułą, przy tych samych oznaczeniach co wyżej, a mianowicie:

$$x = \frac{x - Max(x)}{Max(x) - Min(x)}$$

Wyniki pomiarów potęgi cybernetycznej 19 państw grupy G20 wskazują na dominację Wielkiej Brytanii, Stanów Zjednoczonych, Australii, Niemiec i Kanady (tabela 4). Największą wartość w pierwszej kategorii wskaźników prawno-regulacyjnych ze wszystkich kategorii wskaź-

ników uzyskały Niemcy (99,3) przed Stanami Zjednoczonymi oraz Wielką Brytanią (*ex aequo* 97,3).

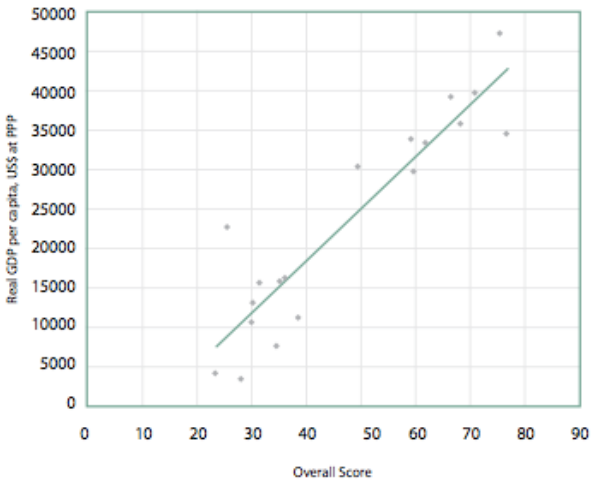
Tabela 4

Ranking potęgi cybernetycznej państw obliczonej modelem CPI (2011)

Pozycja	Państwo	Wartość CPI (w skali 0–100)	Region geograficzny
1	Wielka Brytania	76,8	Europa Zachodnia
2	Stany Zjednoczone	75,4	Ameryka
3	Australia	71,0	Azja i Pacyfik
4	Niemcy	68,2	Europa Zachodnia
5	Kanada	66,6	Ameryka
6	Francja	61,8	Europa Zachodnia
7	Republika Korei	59,7	Azja i Pacyfik
8	Japonia	59,3	Azja i Pacyfik
9	Włochy	49,5	Europa Zachodnia
10	Brazylia	38,6	Ameryka
11	Meksyk	36,3	Ameryka
12	Argentyna	35,4	Ameryka
13	Chiny	34,6	Azja i Pacyfik
14	Rosja	31,7	Europa Wschodnia i Azja Środkowa
15	Turcja	30,4	Europa Wschodnia i Azja Środkowa
16	RPA	30,2	Bliski Wschód i Afryka
17	Indie	28,3	Azja i Pacyfik
18	Arabia Saudyjska	25,7	Bliski Wschód i Afryka
19	Indonezja	23,5	Azja i Pacyfik

Źródło: *Cyber Power Index…*, s. 4.

Model funkcjonalny CPI umożliwia obliczanie korelacji pomiędzy wskaźnikami. Autorzy modelu zmierzyli także korelację wartości wskaźnika PKB na mieszkańca z ogólną wartością potęgi cybernetycznej 19 państw, uzyskując zaskakująco wysoki wynik – 0,92 (rysunek 1).



Źródło: *Cyber Power Index…*, s. 23.

Rys. 1. Współczynnik korelacji wielkości PKB per capita oraz ogólnej wartości potęgi cybernetycznej CPI

Autorzy modelu CPI w rzeczywistości mierzą jedynie defensywną moc cybernetyczną, chociaż nie deklarują tego w założeniach (a szkoda). Kategorie wskaźników mają bardzo zbliżone wagi, co pod tym względem zbliża tę motodę do tzw. ważenia neutralnego o jednakowych wagach i równomiernym rozkładzie wskaźników. Zróżnicowanie jest jednak wyraźne na poziomie wag podkategorii, których suma dla danej kategorii wynosi 100. Trudno kwestionować dobór wskaźników w tym modelu, aczkolwiek w kategorii wskaźników społeczno-ekonomicznych nie wyróżniono podkategorii wskaźników ekonomicznych, pomimo iż autorzy uznają znaczenie wskaźnika PKB per capita o bardzo wysokim wskaźniku korelacji z ogólną potęgą cybernetyczną państw G20. Zastanawiająca jest także pozycja Wielkiej Brytanii, jako lidera CPI, przed Stanami Zjednoczonymi.

Model A.M. Gomeza

Koncepcja pomiaru potęgi cybernetycznej państw zaproponowana przez Alberto Miguela Gomeza[23] została także oparta na metodzie wskaźnikowej, w której wyróżniono 50 wskaźników podzielonych na 6 kategorii: 1) infrastruktury, 2) gospodarki, 3) badań naukowych, 4) polityki

[23] Z treści źródłowego artykułu trudno jednoznacznie wywnioskować, czy A.M. Gomez jest autorem modelu, czy też tylko go charakteryzuje. Umownie jednak nazwano go modelem A.M. Gomeza. Zob. A.M. Gomez, *Identifying Cyber Strategies vis-a-vis Cyber Power*, http://www.academia.edu/6544932/Identifying_Cyber_Strategies_vis-a-vis_Cyber_Power (dostęp: 27.01.2015), p. IIIA.

i e-administracji, 5) społeczno-polityczną oraz 6) militarną. Na podstawie wyników pomiaru potęg cybernetycznych oraz analizy zdarzeń (zachowań państw) w cyberprzestrzeni (podmiot atakujący, obiekt atakowany oraz częstotliwość) A.M. Gomez wyróżnił cztery kategorie państw o ofensywnych i defensywnych zachowaniach w cyberprzestrzeni (tabela 5)[24]. Następnie, posługując się analizą statystyczną, dla każdej kategorii państw określił rodzaj stosowanego ataku, z uwzględnieniem roli podmiotu atakującego i atakowanego (tabela 6). W tym miejscu niejasna jest jednak przyjęta przez A.M. Gomeza reguła budowania macierzy typów cyberataków. W przypadku tej samej kategorii państw występujących jednocześnie w roli podmiotu atakującego i atakowanego powinno być pole puste. Przykładowo pole [EP-I; EP-I] oznacza, że Stany Zjednoczone są podmiotem atakującym samych siebie?

Tabela 5

Kategoryzacja zachowań państw w cyberprzestrzeni

Kategoria	Państwa
Defensywne I (EP-I)	Stany Zjednoczone
Ofensywne I (EA-I)	Chiny
Defensywne II (EP-II)	Australia, Kanada, Nowa Zelandia, Singapur, Japonia, Republika Korei, Filipiny, Rosja, Izrael
Ofensywne II (EA-II)	Chile, Indonezja, Malezja, Meksyk, Peru, Tajlandia, Wietnam, Indie, Iran, Pakistan, Bangladesz, Syria, Cypr, Turcja, Irak, Kuwejt, Gruzja, Liban

Źródło: A.M. Gomez, op. cit., s. 5, za: FireEye, *World war c: Understanding nation-state motives behind todays advanced cyber attacks*, FireEye, Tech. Rep.

Tabela 6

Macierz typów cyberataków

	Podmiot atakowany			
Podmiot atakujący	**EP-I**	**EA-I**	**EP-II**	**EA-II**
EP-I	atak na sieci	złośliwe oprogramowanie	atak na sieci	złośliwe oprogramowanie
EA-I	kradzież danych	atak na sieci	złośliwe oprogramowanie	złośliwe oprogramowanie
EP-II	złośliwe oprogramowanie	atak na strony internetowe	DoS/ DDoS	złośliwe oprogramowanie
EA-II	atak na strony internetowe	atak na sieci	DoS/ DDoS	atak na strony internetowe

Źródło: A.M. Gomez, op. cit., s. 6.

Państwa zaklasyfikowane do dwóch kategorii defensywnych – EP-I (kat. pierwsza – liderzy) i EP-II (kat. druga – pozostali) cechują dominujące wartości wskaźników z kategorii: infrastruktury, gospodarki, badań naukowych oraz polityki i administracji cyfrowej przy jednocześnie ich pozytywnej korelacji ze wskaźnikami pozostałych kategorii. Natomiast państwa z kategorii ofensywnych (EA-I i EA-II) charakteryzują się niskimi wartościami wskaźników z ww. kategorii grup, przy wyższym poziomie wskaźników z kategorii społeczno-politycznej oraz dominujących wskaźnikach z grupy militarnej (zwłaszcza EA-I). Jednocześnie występuje ujemna korelacja pomiędzy wskaźnikami z pierwszych czterech kategorii a wskaźnikami społeczno-politycznymi. Państwa z kategorii ofensywnych cechuje także stały wzrost wskaźników infrastruktury i gospodarczych. Liderem wśród państw ofensywnych (EA-I) są Chiny, których także potęga ogólna i wojskowa od lat dynamicznie wzrasta – osiągając obecnie trzecią pozycję w świecie po Stanach Zjednoczonych[25]. Liderem wśród kategorii państw defensywnych (EP-I) są natomiast Stany Zjednoczone.

Na podstawie uzyskanych tą metodą wyników badań, A.M Gomez wyróżnił trzy podstawowe strategie państw w cyberprzestrzeni:

- *strategia utrzymania potęgi cybernetycznej* – stosowana przez państwa aktywnie demonstrujące posiadane zdolności w cyberprzestrzeni, w celu zwiększenia ich potęgi ogólnej;
- *strategia osiągania równowagi* – polega na dążeniu państw do maksymalizowania ich cyberpotęgi, w celu uzyskania przewagi nad potencjalnymi agresorami, zarówno w cyberprzestrzeni, jak i poza nią, unikając jednak sytuacji konfliktо-

[24] A.M. Gomez podaje nazwy kategorii państw jako pasywne (ang. *established passive*, EP) i agresywne (ang. *emmerging aggresive*, EA), natomiast autor posługuje się jego zdaniem właściwszą terminologią: defensywne (ang. *defensive*) i ofensywne (ang. *offensive*), przy czym skróty oznaczeń pozostawiono w oryginale.

[25] Zob. M. Sułek, *Potęga państw. Modele i zastosowania*, Wyd. Rambler, Warszawa 2013, s. 168–193.

wych, które mogą zmniejszać ich potęgę ogólną (np. w sferze ekonomicznej).

• *strategia demonstrowania potęgi cybernetycznej* – stosowana przez państwa, w celu demonstrowania ich wzrastających zdolności w cyberprzestrzeni.

Prezentując model pomiaru potęgi cybernetycznej państw A.M. Gomez nie podaje szczegółów metodologicznych, koncentrując się głównie na jego implementacji w określaniu kategorii strategii państw w cyberprzestrzeni, wyróżniając ich zarówno defensywny, jak i ofensywny charakter. Proponowane w konkluzjach trzy kategorie strategii państw mogą jednak budzić wątpliwości. W zasadzie wszystkie państwa na miarę posiadanych możliwości dążą do zwiększania potęgi w cyberprzestrzeni – także Stany Zjednoczone i Chiny. Inną kwestią jest jej demonstrowanie w postaci określonych działań. W tym zakresie zastanawia także plasowanie Stanów Zjednoczonych na pozycji lidera w kategorii państw defensywnych wobec kierowanych wobec nich podejrzeń m.in. o atak cybernetyczny za pomocą robaka komputerowego „Stuxnet".

Zakończenie

Większość proponowanych w literaturze przedmiotu definicji potęgi cybernetycznej odnosi się do podstawowej jednostki politycznej, jaką jest państwo. Taką też konwencję terminologiczną przyjął w artykule autor. Należy przy tym zwrócić jednak uwagę na konieczność postrzegania potęgi cybernetycznej nie tylko w sensie podmiotowym, jakim jest jej dysponent (w tym wypadku państwo), lecz także w sensie przedmiotowym, gdzie m.in. należy wyróżnić: defensywną i ofensywną potęgę cybernetyczną. Powyższe czynniki w znacznym stopniu determinują wybór i implementację metody jej pomiaru oraz uzyskane za jej pomocą wyniki. Wobec braku powszechnie uznanej definicji potęgi cybernetycznej, badacze zajmujący się jej pomiarem powinni przyjmować własną konwencję terminologiczną, stosownie do przyjętej metody badawczej.

Wybór modelu CPI oznacza badanie wyłącznie defensywnej potęgi cybernetycznej, chociaż jego autorzy tego faktu *directe* nie definiują. Model A.M. Gomeza jest z założenia bardziej złożony, gdyż na podstawie obliczenia potęgi cybernetycznej państw metodą wskaźnikową pozwala na określanie strategii państw w cyberprzestrzeni zarówno pod względem ich defensywnych, jak i ofensywnych zdolności. Proponowany przez A.M. Gomeza podział na trzy główne strategie budzi jednak wątpliwości, chociażby z uwagi na fakt, że *de facto* wszystkie państwa, na miarę posiadanych zdolności, dążą do zwiększenia ich potęgi cybernetycznej – także Stany Zjednoczone i Chiny.

Obie metody wykorzystują powszechnie znaną metodę wskaźnikową stosowaną w algorytmach wczesnego ostrzegania. Niektóre wskaźniki pomiaru cyberpotęgi są wspólne dla obu modeli (np. gospodarczy czy technologiczny), niektóre zaś cechują indywidualnie każdy z nich (np. militarny w modelu drugim). Zastanawiający w przytoczonych przez A.M. Gomeza wynikach pomiarów jest brak Wielkiej Brytanii, która w modelu CPI jest absolutnym liderem w rankingu cyberpotęg państw. Podobnie jest z plasowaniem Stanów Zjednoczonych na pozycji lidera w grupie państw defensywnych, wobec powszechnych podejrzeń o atak cybernetyczny za pomocą robaka komputerowego „Stuxnet".

W mojej ocenie powyższe metody pomiaru potęgi cybernetycznej państw nie rozwiązują w pełni problemu badawczego i należy je traktować jako propozycje inspirujące do dalszych zaawansowanych badań nad tą problematyką z uwzględnieniem nie tylko państw, ale i innych podmiotów systemu bezpieczeństwa międzynarodowego (np. organizacji terrorystycznych).

Bibliografia

Białoskórski R., *Bezpieczeństwo informacji. Słownik pojęć i skrótów*, Wyd. Ubezpieczeń, Warszawa 2010.

Białoskórski R., *Cyberthreats in the Security Environment of the 21st Century*, "Journal of Security and Sustainability Issues" 2012, nr 4.

Białoskórski R., *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku*, Wyd. WSCiL, Warszawa 2011.

Białoskórski R., *Modelowanie konfliktów zbrojnych z wykorzystaniem procesu analizy hierarchicznej – kazus syryjski* [w:] M. Sułek (red.), *Potęgometria*, tom 2, Wyd. Europejskie Centrum Analiz Geopolitycznych, Warszawa 2015 (w druku).

Cyber Power Index. Findings and Methodology, Economist Intelligence Unit, 2011. http://www.boozallen.com/content/dam/boozallen/media/file/

Cyber_Power_Index_Findings_and_Methodology.pdf (dostęp: 27.01.2015).

Department of Defense Strategy for Operating in Cyberspace, lipiec 2011, http://www.defense.gov/news/d20110714cyber.pdf (dostęp: 27.01.2015).

Gomez A.M., *Identifying Cyber Strategies vis-a-vis Cyber Power*, http://www.academia.edu/6544932/Identifying_Cyber_Strategies_vis-a-vis_Cyber_Power (dostęp: 27.01.2015).

Kuehl D.T., *From Cyberspace to Cyberpower: Defining the Problem*, w: D. Kramer, H. Stuart, i L.K. Wentz, *Cyberpower and National Security Policy*, National Defense University, Potomac Books, Inc., 2009. http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf (dostęp: 27.01.2015).

Mattioli R., *The «State(s)» of Cybersecurity*, w: Giampiero Giacomello (red.), *Security in Cyberspace*, New York; London; New Delhi; Sydney, Bloomsbury, 2014.

Mazur M., *Cybernetyka i charakter*, wyd. 2, Wyd. Podkowa Leśna; Wyd. AULA, 1996.

National Security Presidential Directive/NSPD-54 Homeland Security Presidential Directive/HSPD-23, 8 styczeń 2008, https://epic.org/privacy/cybersecurity/EPIC-FOIA-NSPD54.pdf (dostęp: 27.01.2015).

Nye J.S., *Cyber Power*, Cambridge: Harvard Kennedy School, 2010, http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf (dostęp: 27.01.2015).

Panas E., *Potęga transnarodowych organizacji społeczeństwa obywatelskiego*, w: M. Sułek (red.), *Potęgometria*, tom I, Wyd. Europejskie Centrum Analiz Geopolitycznych, Warszawa 2013.

Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, 25 czerwiec 2013, http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html (dostęp: 27.01.2015).

Rattray G.J., *An Environmental Approach to Understanding Cyberpower*, 13 styczeń 2015. http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-10.pdf (dostęp: 27.01.2015).

Słownik Języka Polskiego, http://sjp.pwn.pl/sjp/cyberprzestrzeń;2553915 (dostęp: 27.01.2015).

Słownik komputerowy i encyklopedia informatyczna, http://www.i-slownik.pl/323,cyberprzestrzen (dostęp: 27.01.2015).

Sułek M., *Metody i techniki badań stosunków międzynarodowych*, Oficyna Wyd. ASPRA-JR, Warszawa 2004.

Sułek M., *Potęga państw. Modele i zastosowania*, Wyd. Rambler, Warszawa 2013.

The National Strategy to Secure Cyberspace, The White House Washington, luty 2003. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (dostęp: 27.01.2015).

THE CYBER POWER OF STATES: MEASUREMENT AND APPLICATION

Abstract

The article discusses the problem of measurement of cyber power of states using the example of two research models: Cyber Power Index (CPI) and A.M. Gomez. Both methods are based on the analysis of indicators. The first model values only defensive cyber power, the second defensive and offensive as well. Both of these cyber power dimensions can be seen as the main determinants of the directions of research for solutions to the above mentioned research problem. The second model serves for the estimating of a state's strategies in cyberspace from the- maintenance of cyber power, the achievement balance, and the demonstration of cyber power. The results of both models differ considerably enough and already confirm the complexity of this problem during the conceptual phase and highlight the need for further research.

Keywords – cyberspace, cyberpower, measurement, model

Introduction

The modern revolution of inforrmation is based on the global dependence on information and communication technology (ICT). The information world has the greatest capabilities of interactions in cyberspace at its disposal, creating both threats and opportunities. It concerns all subjects of international systems, equal government and non-government. Each subject can be attacker and victim of cyberthreats, cyberwar, cyberespionage, cyberterrorism and cyberdelinquency[1], the identification of which is one of the main problems of cybersecurity[2].

[1] See: R. Białoskórski, *Cyberzagrożenia w sìrodowisku bezpieczeństwa XXI wieku,* Wyd. WSCiL, Warszawa 2011.

[2] The author has suggested conceptual analysis of cyberthreat based on analysis of four factors: subject attacking, subject attacked, purposes and motivation. See: R. Białoskórski, *Cyberthreats in the Security Environment of the 21st Century,* 'Journal of Security and Sustainability Issues' 2012, No. 4, p. 255–258.

In this situation, the problem of measurement of cyber power is an important factor in the estimation of the power of states. In this article, the problem of defining the cyber power of states and how to measure it is addressed.

Inspiration for the research came from its innovatory character and the lack of elaboration in Polish scientific literature and consistent range with the main direction of scientific interest in the author's problem of *conflict prevention (CP)*, defined as the process of early warning and preventive reaction relying on constant monitoring and analysis of the evolution of events in the areas at risk of military conflict (*early warning*) and deciding on and taking preventive actions (*reaction preventive*) to prevent an armed conflict[3]. In view of the complexity of theproblem, the article only outlines the problems which that require more involved theoretical studies and empirical research.

Definition of cyber power

The definition of ''cyber power" is related with ''cyberspace". Mattiolli Rossella considers, that it is hard to define the border between cyberspace and cybersecurity, mainly from the point of view of the dynamic character of cyberspace and the lack of classically comprehended territoriality[4]. The Cybersecurity policy of the Republic of Poland defines security in cyberspace as a 'group of activities: the organisational, legal, technical, physical and educational affirmation of the undisturbed functioning of cyberspace'[5].

In literature, cyberspace is defined in principle, as: 1) a global information area, understood as a '*virtual area* in which communication proceeds between computers joined to an internet network'[6] or an 'area of opened intercommunication through joined computers and classic communication networks world-wide, taking into consideration all electronic communication systems (also the classical telecommuniation network) which send information from numeric dating sources or for assigning numeration[7] and 2) a strategic element of a state security system as a: 'responsive system – state control system… consists of thousands of computers,switchesandfiber-opticcables,operating the critical infrastructure'[8] or 'independent network of information technology infrastructure, including internet, telecommunication networks, computer systems and integrated processors and controllers acting in industrial critical infrastructure'[9] or 'military operation space (near: ground, air, marine, space)'[10]. With reference to the above, it is possible to conclude that *cyberspace is a global information area, containing a strategic element of a state's security system* and this definition is accepted by the author in the terminological convention of the researched problem[11]. However, one should not forget about the growing influence of transnational non-state subjects, which more actively take advantage of cyberspace for purposes not always consistent with the purposes of states on whose territories they are operating[12].

In terminological convention, the author has accepted the concept of realism from the theory of international relations, setting up a unitary state as the only one subject of international relations about anarchic character, a note on the liberal stream, and the meaning of the growing

[3] R. Białoskórski, *Modelowanie konfliktów zbrojnych z wykorzystaniem procesu analizy hierarchicznej – kazus syryjski*, in: M. Sułek (ed.), *Potęgometria*, Vol. II, Wyd. Europejskie Centrum Analiz Geopolitycznych, Warszawa 2015, p. 52.

[4] R. Mattioli, *The «State(s)» of Cybersecurity,* in: G. Giacomello (ed.), *Security in Cyberspace*, New York, London, New Delhi, Sydney, Bloomsbury, 2014, p. 27.

[5] *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, 25 czerwiec 2013, http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html (access: 27.01.2015).

[6] *Słownik Języka Polskiego*, http://sjp.pwn.pl/sjp/cyberprzestrzeń;2553915 (access: 27.01.2015).

[7] *Słownik komputerowy i encyklopedia informatyczna*, http://www.i-slownik.pl/323,cyberprzestrzen (access: 27.01.2015).

[8] *The National Strategy to Secure Cyberspace*, The White House Washington, February 2003, p. vii, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (access: 27.01.2015).

[9] *National Security Presidential Directive/NSPD-54 Homeland Security Presidential Directive/HSPD-23*, 8 January 2008, p. 7g, https://epic.org/privacy/cybersecurity/EPIC-FOIA-NSPD54.pdf (access: 27.01.2015).

[10] *Department of Defense Strategy for Operating in Cyberspace*, July 2011, http://www.defense.gov/news/d20110714cyber.pdf (access: 27.01.2015).

[11] Terminological convention is agreement among author and readers for definition obligatory author in the whole publication. M. Mazur, *Cybernetyka i charakter*, Edition 2, Wyd. AULA, Podkowa Leśna 1996, p. 27–28.

[12] See: E. Panas, *Potęga transnarodowych organizacji społeczeństwa obywatelskiego*, in: M. Sułek (ed.), *Potęgometria*, Vol. I, Wyd. Europejskie Centrum Analiz Geopolitycznych, Warszawa 2013, p. 78–94.

role of non-state subject, such as: *International Non-Governmental Organisations* (INGOs) and one-valued negative multinational subjects for which the author has included: *International Terrorist Organizations* (ITOs) and *International Criminal Groups* (ICGs). In the nearest future, we can expect an explosion of activity from these in cyberspace, especially the ITOs, mainly for mediumistic purposes, recruitment and operative communications. The relatively small cost of access to cyberweapons is a decisive factor compared to the simultaneous enormous capability of their destructive interaction, sometimes compared to weapons of mass destruction (WMD). The issue of estimating the cyber power of non-state subjects is equally important to that of the state and it requires advanced studyand is practically ignored in the literature[13]. Independently from the strong and weak points of concrete definitions of cyberspace, such perception places it in the sphere of the security of state (also in an international dimension), in the sphere of the protection and security of a government's communications networks and critical infrastructures of state[14]. In the operative dimension area of security[15], cyberspace differs in that users (individual and organised) are simultaneously its creators and its different physical characteristics (creation, stockpiling, transformation, exchange and taking advantage of flow of information by electronic means), which strongly affects all remaining operative areas (ground, air, marine and space)in the traditional sense of geographical area. Cyberspace is not only more dynamic and unforeseen from there, but it is also possible to include or to exclude it[16].

Daniel T. Kuehl, when defining cyber power, had searched for inspiration in analogy to the pioneer defining of marine power and air power, whose main idea is the ability to activate and utilise the environment for definite purposes. It verified that: *cyber power is the ability to use cyberspace for rendering influence on events in all operative areas and obtaining an advantage in all factors creating the cyber power*[17]. So, the measurement of cyber power is concerned with the measurement of a feature of the environment. This researcher has included its: 1) technological ability indicator (still changeable and variable for different users – state and non-state) and 2) organisational ability indicator.

Joseph S. Nye defines cyber power as the: ability for achievement of set up purposes behind the assistance of electronically linked information in cyberspace[18]. This researcher treats cyber power in the dimension of internal and external information interactions (virtual) and physical generating of *cyber soft power* and *intra cyberspace hard power*[19]. In the dimension of internal information interaction, we can deal with soft cyber power in the form of a system of norms and standards and with hard power in the form of DoS/DDoS cyberattacks[20] (table 1).

Table 1

Physical and Virtual Dimensions of Cyber Power

	Intra cyber space	Extra cyber space
Information Instruments	Hard: *Denial of Service* attacks (DoS)/ *Distributed Denial of Service* (DDoS)[1] Soft: Set norms and standards	Hard: Attack SCADA (*Supervisory Control And Data Acquisition*)[2] Soft: Public diplomacy campaign to sway opinion
Physical Instruments	Hard: Government controls over companies Soft: Infrastructure to help human rights activists	Hard: Bomb routers or cut cables Soft: Protests to name and shame cyber providers

[1] DoS attack relies on a large amount of data on an attacked computer system, that it is taken over or its activity paralysed. At the DoS attack, a lot of attacking computers controlled

[13] R. Białoskórski, Cyberthreats…, op. cit., p. 252–253. See: E. Panas, *Potęga transnarodowych organizacji społeczeństwa obywatelskiego*, in: M. Sułek (ed.), *Potęgometria*, Vol. I, Wyd. Europejskie Centrum Analiz Geopolitycznych, Warszawa 2013, p. 78–94.

[14] D.T. Kuehl, *From Cyberspace to Cyberpower: Defining the Problem*, in: D. Kramer, H. Stuart, L.K. Wentz, *Cyberpower and National Security Policy*, National Defense University, Potomac Books, Inc., 2009, http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf (access: 27.01.2015), p. 2.

[15] Notion 'operative' means in this case practical operation in data and place.

[16] See: G.J. Rattray, *An Environmental Approach to Understanding Cyberpower*, 13 January 2015, http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-10.pdf (access: 27.01.2015).

[17] D.T. Kuehl, *From Cyberspace…*, p. 12.

[18] J.S. Nye, *Cyber Power*, Cambridge: Harvard Kennedy School, 2010), http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf (access: 27.01.2015), p. 3–4.

[19] Ibidem, p. 3.

[20] Most generally, cyberattack expedient disturbance of correct functioning of correct cyberspace, *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, p. 6. In the article, this definition links to the widest operations in the framework of information operations.

earlier controlled by the intruder are engaged (e.g. Zombie). R. Białoskórski, *Bezpieczeństwo informacji. Słownik pojęć i skrótów*, Wyd. Ubezpieczeń, Warszawa 2010, p. 47–48.

[2] SCADA is the computer operation system controlling the steering of the technological and production process, relying on the collection and projection of the actual data (measurements)), controlling of process, alarming and data archiving, http://pl.wikipedia.org/wiki/SCADA (access: 27.01.2015).

Source: J.S. Nye, op. cit., p. 3.

This researcher suggests three variants of cyber power[21]:

Variant 1st: (A induces B do what B would initially otherwise not do)

Hard Power: denial of service attacks, insertion of malware, SCADA disruptions, arrests of bloggers

Soft Power: information campaign to change initial preferences of hackers, recruitment of members of terrorist organisations

Variant 2st: (Agenda control: A precludes B's choice by exclusion of B's strategies)

Hard Power: firewalls, filters, and pressure on companies to exclude some ideas

Soft Power: ISPs and search engines self monitor, ICANN rules on domain names, widely accepted software standards

Variant 3rd: (A shapes B's preferences, so some strategies are never even considered)

Hard Power: threats to punish bloggers who disseminate censored material

Soft Power: information to create preferences (eg. stimulate nationalism and "patriotic hackers,"), develop norms of revulsion (e.g. child pornography)

The lack of a generally recognised definition of cyber power means that researchers working on the problem of its measurement should accept personal terminological convention appropriate to the accepted research method.

Measurement of cyber power of state

Cyber power can be treated as part of defence and then we deal with *defensive cyber power* (DCP), and, in its offensive meaning, - offensive cyber power (OCP). The above-mentioned indicator determines directions of concepts of methods of measurements of cyber power, even if it is not expressed *expressis verbis*, as it is the example in the discussed CPI model.

CPI Model

The concept of the model of measurement of the *cyber power index* (CPI) has been processed by a group of The Economist Intelligence Unit (EIU) from the famous magazine 'The Economist' in cooperation with the Booz Allen Hamilton Group. Its purpose is creating rankings of the cyber ability of the states of the G20 Group in the scope of prevention and counteraction of cyber attacks and the promotion of problems of cybersecurity in the international environment. So, there is a *de facto* model of measurement of defensive cyber power.

It relies on calculating indicators of the cyber power of the state.

For this purpose, a matrix of 39 quantitative and qualitative indicators grouped in 4 categories and 19 subcategories, taking into consideration their average weight, was arranged (table 2). The matrix was processed using expert estimates[22].

All the expert indicators showed values growing on a scale from 0 to 100, where the greatest value of cyber power is 100.

Data banks present national and international statistic sources: The Economist Intelligence Unit (EIU), The UN Educational, Scientific and Cultural Organization (UNESCO), The International Telecommunications Union (ITU); The World Bank (WB).

[21] J. Nye, op. cit., p. 7.

[22] The expert estimate method requires, first of all, the careful selection of experts, most often on the basis of formal criterion (degree scientific, professional experience, scientific possesions, awards) or socially-moral (good report of co-worker, reliability, honesty, intransigence). In estimating the averaged estimating group (great liberty speaking out and presenting of results) the differences in individual and group of experts' estimates (possible psychological brake) and ethical aspects must be considered. See: M. Sułek, *Metody i techniki badań stosunków międzynarodowych*, Oficyna Wyd. ASPRA-JR, Warszawa 2004, p. 167–174.

Table 2

Matrix of indicators and weights of CPI cyber power index model[1]

Category of indicators	Weight [%]	Subcategory of indicators	Weight [%]	Indicators
I. Legal and Regulatory Framework	26.3	I.1. Government commitment ro cyber development	27.1	1. National cyber plan
				2. Public/private partnerships
		I.2. Cyber protection policy	24	3. Cyber enforcement authority
				4. Cybersecurity laws
				5. Cyber crime response
				6. International cybersecurity commitments
				7. Cybersecurity plan
		I.3. Cyber censorship	15.5	8. Cyber censorship
		I.4. Political efficacy	15.5	9. Political efficacy
		I.5. Intellectual property protection	17.8	10. Intellectual property protection
II. Economic and Social Context	25	II.1. Educational levels	25.2	11. Tertiary student enrollment as a percentage of total enrollment
				12. Expected years of education
		II.2. Technical skills	27.4	13. Labour productivity growth
				14. Researchers in research and development per million people
				15. Science and engineering degrees
				16. English literacy
		II.3. Trade	17.3	17. Information and communications technology exports as a percentage of total exports
				18. Information and communications technology imports as a percentage of total imports
				19. Openness to trade
		II.4. Innovation environment	30.1	20. Research and development as a percentage of gross domestic product
				21. Domestic patent filings
				22. Private equity and venture capital as a percentage of gross domestic product
III. Technology Infrastructure	26.3	III.1. ICT Access	20.3	23. Internet penetration
				24. Mobile cellular penetration
				25. Wi-Fi hotspots per million people
				26. Social media penetration
		III.2. ICT Quality	21.9	27. Fixed broadband subscribers per 100 inhabitants
				28. International Internet bandwidth
		III.3. IT Spending	20.3	29. Information technology spending as a percentage of gross domestic product
		III.4. ICT Affordability	11.7	30. Mobile phone tariffs
				31. Broadband Internet tariffs
		III.5 Secure servers	25.8	32. Secure servers
IV. Industry Application	22.5	IV.1. Smart grids	21.1	33. Smart grids
		IV.2. E-Health	16.2	34. E-Health
		IV.3. E-Commerce	30.4	35. Businesses placing orders via the Internet as a percentage of business using the Internet
				36. Individuals placing orders via the Internet as a percentage of Internet users
				37. Individual use of Internet banking as a percentage of Internet users
		IV.4. Intelligent transportation	21.1	38. Intelligent transportation
		IV.5. E Government	11.3	39. E-Government

Source: *Cyber Power Index. Findings and Methodology*, Economist Intelligence Unit, 2011, http://www.boozallen.com/content/dam/boozallen/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf, p. 22, 24.

[1] Detailed description of definition and principles of allocating of values are placed in the sorurce material of EIU in annex II, p. 26–32.

Weights of categories of indicators are approximated with insignificant domination of category of legal and regulatory indicators and the category of technological infrastructure (*ex aequo* 26.3) coming before the economic and social indicators category (25) and the category of industrial application (22.5).

The cyber power values of 19 states from the G20 (without the European Union) representing five geographic regions were analysed: Western Europe, East Europe and Middle Asia, Middle East and Africa, Asia and Pacific and America.

The values of the indicators are normalised in the proper manner and sum according to categories.

Favourable cyber power indicators (e.g. growth of expense on R&D) are normalised according to the rule:

$$x = \frac{x - Min(x)}{Max(x) - Min(x)}$$

gdzie: *Min(x)* – minimal value of given economic indicator in group of 19 states;

Max(x) – maximal value of given economic indicator in group of 19 states.

This way, normalised values are transformed from partition 0–1 to partition 0–100, which enables them to be directly compared to other indicators in such a way that the state accepts the highest indicator value 100, but the lowest indicator value 0.

Table 3

Expenses on research and development relative to GDP

Country	R&D/GDP
South Korea	4.04
Japan	3.39
Germany	2.93
United States	2.79
Australia	2.39
France	2.26
China	1.98
Canada	1.73
United Kingdom	1.72
Italy	1.27
Brazil	1.21
Russia	1.12
Turkey	0.86
India	0.81
South Africa	0.76
Argentina	0.65
Mexico	0.43
Saudi Arabia	lack data
Indonesia	lack data

Source: The World Bank, Research and development expenditure (% of GDP), http://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS (access: 15.10.2015).

Unfavourable indicators of cyber power (e.g. mobile telephone or internet tariffs) are normalised with other rules, at the same designations as above:

$$x = \frac{x - Max(x)}{Max(x) - Min(x)}$$

The measurements of the cyber power of 19 states from G20 indicate the domination of the United Kingdom, the United States, Australia, Germany and Canada (table 4). From all the indicators, Germany has the biggest value in the first legal and regulatory category (99.3), before the United States and United Kingdom (*ex aequo* 97.3).

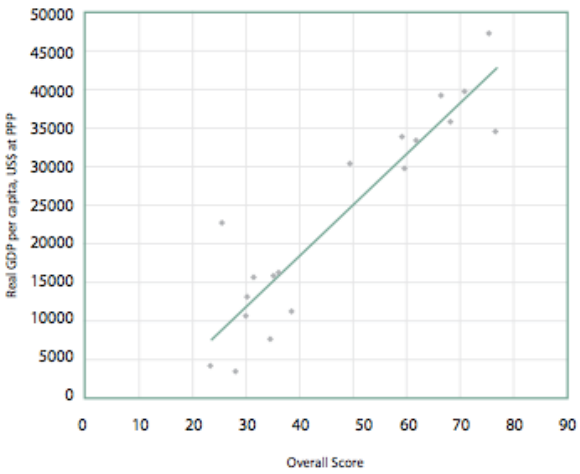
Table 4

Cyber Power Rankings CPI model (2011)

Rank	Country	CPI Score (0–100)	Geografical Region
1	United Kingdom	76.8	Western Europe
2	United States	75.4	America
3	Australia	71.0	Asia-Pacific
4	Germany	68.2	Western Europe
5	Canada	66.6	America
6	France	61.8	Western Europe
7	South Korea	59.7	Asia-Pacific
8	Japan	59.3	Asia-Pacific
9	Italy	49.5	Western Europe
10	Brazil	38.6	America
11	Mexico	36.3	America
12	Argentina	35.4	America
13	China	34.6	Asia-Pacific
14	Russia	31.7	Eastern Europe & Central Asia
15	Turkey	30.4	Eastern Europe & Central Asia
16	South Africa	30.2	Middle East & Africa
17	India	28.3	Asia-Pacific
18	Saudi Arabia	25.7	Middle East & Africa
19	Indonesia	23.5	Asia-Pacific

Source: *Cyber Power Index*..., p. 4.

The functional CPI model enables scaling of correlation among indicators. The authors of this model have also measured the correlation of value of GPD indicator on an inhabitant with the general value of the cyber power of 19 states, achieving a surprisingly high result – 0.92 (Figure 1).



Source: *Cyber Power Index*..., p. 23.

Figure 1. Scatter Plot of overall Cyber Power Rankings and GDP

The authors of the CPI model really only gauge the defensive cyber power, though they do not declare it in the foundations Categories of indicators have very similar weights, which, in this respect, approximate this method for so called 'natural weight' about the equal weights and even schedule of indicators. However, disparity is distinct at the level of subcategory weights which amount to 100 for a given category.

It is hard to challenge the selection of indicators in this model, although in the category of social and economic indicators the undercategory economic indicators is not marked, despite the authors regarding themeaning of GPD *per capita* indicator as a very high indicator of correlation with the general CPI of G20. The United Kingdom's position as leader ahead of the United States is also puzzling.

A.M. Gomez Model

The concept of measurement of cyber power of states has been based on the method suggested by Alberto Miguela Gomeza[23] and is also based on the indicator method, in which 50 indicators divided in 6 categories are placed: 1) infrastructure, 2) economy, 3) scientific research, 4) politics and e-goverment, 5) social-politic and 6) military. On the basis of the measurement result of cyber power and analyses of events (state's behaviour) in cyberspace (subject attacking, object attacked and frequency), A.M. Gomez has differentiated four categories of states regarding offensive and defensive behaviour in cyberspace (table 5)[24]. Next, using statistic analysis, he has defined the kind of applicable attack for each category of state, taking into consideration the role of the attacking and attacked subject (table 6). However, the construction matrix rule of the type of cyberattack proposed by A.M. Gomez is unclear. In the case of the same category of states taking a stand simultaneously in the role of attacking and attacked subject, there is obliged to be an empty field. For example, field [EP-I; EP-I] means that the United States is the attacking and attacked subject as well?

Tabel 5

Category of State in Cyberspace

Category of State	Country
Established Defensive I (EP-I)	United States
Emerging Offensive I (EA-I)	China
Established Defensive II (EP-II)	Australia, Canada, New Zealand, Singapore, Japan, South Korea, Philippines, Russia, Israel
Emerging Offensive II (EA-II)	Chile, Indonesia, Malaysia, Mexico, Peru, Thajland, Vietnam, India, Iran, Pakistan, Bangladesh, Syria, Cyprus, Turkey, Iraq, Kuwait, Georgia, Lebanon

Source: A.M. Gomez, op. cit., p. 5, FireEye, *World war c: Understanding nation-state motives behind todays advanced cyber attacks*, FireEye, Tech. Rep.

Tabela 6

Attack Type Matrix

	Target			
Initiator	**EP-I**	**EA-I**	**EP-II**	**EA-II**
EP-I	Network Attack	Malware	Network Attack	Malware
EA-I	Information Theft	Network Attack	Malware	Malware
EP-II	Malware	Defa-cement	DoS/ DDoS	Malware
EA-II	Defacement	Network Attack	DoS/ DDoS	Defa-cement

Source: A.M. Gomez, op. cit., p. 6.

[23] From the source of article it is hard to conclude, if A.M. Gomez is the author of this model or he characterizes it only. However, according to the conventionall terminology in this article, author calls its as A.M. Gomez model. See: A.M. Gomez, *Identifying Cyber Strategies vis-a-vis Cyber Power*, http://www.academia.edu/6544932/Identifying_Cyber_Strategies_vis-a-vis_Cyber_Power (access: 27.01.2015), p. IIIA.

[24] A.M. Gomez names categories of states as passive (established passive, EP) and aggressive (emerging aggressive, EA). The author prefers a defensive and offensive terminology, but he leaves summaries of designations the same as the original.

States classified for two defensive categories - EP-I (leaders) and EP-II (other) - feature a predominating value of indicators from these categories: infrastructures, economies, scientific research and politics and e-government, by remaining at their simultaneously positive correlations with the other indicators category. However, the states from the offensive category group (EA-I; EA-II) are characterised with low value indicators, and at a high level of indicators from the social and political category and especially from the military group predominating indicator (especially EA-I). Simultaneously, a negative correlation takes a stand among indicators from the first four categories and the social and political indicators. States from the offensive category also feature a constant growth of infrastructure and economic indicators. China is the leader of the offensive states (EA-I), whose general and military power has been dynamically growing for some years achieving third place in the world after the United States[25]. However, the United States is the leader in the category of defensive states (EP-I).

On the basis of these results, A.M. Gomez has differentiated three fundamental strategies of states in cyberspace:

- *maintenance of cyber power strategy* – used by states actively demonstrating their own ability in cyberspace, to increase their general power;
- *achievement balance strategy* - it relies on the aspiration of states for maximising cyberpower to obtain an advance on potential attackers in cyberspace and to escape a conflict situation, which can decrease its general power (e.g. in the economic sphere).
- *demonstration of cyber power strategy* – used by states to demonstrate their incremental ability in cyberspace.

In his model for measuring the cyber power of the state, A.M. Gomez gives no methodological details, concentrating mainly on its implementation in the definition of the category of strategy of states in cyberspace, in a defensive and offensive character. He concludes that three categories of the strategies of states can cause doubt. In principle, all states aim at escalation of power on measuring their own capability in cyberspace - the United States and China as well. The other problem is its demonstration in some activities. The United States role as leader in the category of defensive states directed to them to be suspicious about the cyber attack behind the computer bug 'Stuxnet'.

Conclusion

The definition of cyber power in the literature mostly concerns the state as a basic political unit. The author has accepted such terminological conventions in the article too. However, this means the need to perceive cyber power not only in its subjective meaning but also in the objective sense, e.g. defensive and offensive cyberpower. The above-mentioned indicators determine the choice and implementation of its method of measurement and achieving results. In accordance with the lack of a generally recognised definition of cyber power, researchers addressing this problem should accept individual terminological convention, appropriatefor the accepted research method. The choice of CPI model means research of exclusively defensive cyber power only, though authors do not define this fact. A.M. Gomez'z model is more compound from its foundation, because it allows the defining of state strategy in cyberspace on the basis of the indictators method, in respect of their defensive and offensive abilities too. A.M. Gomez's division into three main strategies introduces doubt, even in view of the fact that *de facto* all states, after measuring their own abilities, tend to increase their cyber power – including China and the United States. Both methods take advantage of the generally known indicators method applied in early warning algorythms. Some indicators of measurements of cyberpower are common for both types of models (e.g. economic or technological), some of them feature individually (e.g. military in the second model). In A.M. Gomez's results of measurement, the absence of the United Kingdom is puzzling, as it is the absolute leader in the state cyberpower rankings in the CPI model. The United States is placed as leader of the group of defensive states, in accordance with general suspicion about the cyber attack by the computer bug 'Stuxnet'.

The author concludes that the above-mentioned methods of measurements of the cyber power of states do not completely solve the research problem and should be treated as proposals for further advanced research of this problem not only considering the state but also the other subjects of the international security system (e.g. terrorist organisations).

[25] See: M. Sułek, *Potęga państw. Modele i zastosowania*, Wyd. Rambler, Warszawa 2013, p. 168–193.

Bibliography

Białoskórski R., *Bezpieczeństwo informacji. Słownik pojęcì i skroìtoìw*, Wyd. Ubezpieczeń, Warszawa 2010.

Białoskórski R., *Cyberthreats in the Security Environment of the 21st Century*, 'Journal of Security and Sustainability Issues' 2012, No. 4.

Białoskórski R., *Cyberzagrożenia w sìrodowisku bezpieczeństwa XXI wieku*, Wyd. WSCiL, Warszawa 2011.

Białoskórski R., *Modelowanie konfliktów zbrojnych z wykorzystaniem procesu analizy hierarchicznej - kazus syryjski*, in: M. Sułek (ed.), *Potęgometria*, Vol. 2, Wyd. Europejskie Centrum Analiz Geopolitycznych, Warszawa 2015.

Cyber Power Index. Findings and Methodology, Economist Intelligence Unit, 2011. http://www.boozallen.com/content/dam/boozallen/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf (access: 27.01.2015).

Department of Defense Strategy for Operating in Cyberspace, July 2011, http://www.defense.gov/news/d20110714cyber.pdf (access: 27.01.2015).

Gomez A.M., *Identifying Cyber Strategies vis-a-vis Cyber Power*, http://www.academia.edu/6544932/Identifying_Cyber_Strategies_vis-a-vis_Cyber_Power (access: 27.01.2015).

Kuehl D.T., *From Cyberspace to Cyberpower: Defining the Problem*, in: D. Kramer, H. Stuart, i L.K. Wentz, *Cyberpower and National Security Policy*, National Defense University, Potomac Books, Inc., 2009. http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf (access: 27.01.2015).

Mattioli R., *The «State(s)» of Cybersecurity*, in: Giampiero Giacomello (ed.), *Security in Cyberspace*, New York; London; New Delhi; Sydney, Bloomsbury, 2014.

Mazur M., *Cybernetyka i charakter*, Edition 2, Wyd. Podkowa Leśna; Wyd. AULA, 1996.

National Security Presidential Directive/NSPD-54 Homeland Security Presidential Directive/HSPD-23, 8 January 2008, https://epic.org/privacy/cybersecurity/EPIC-FOIA-NSPD54.pdf (access: 27.01.2015).

Nye J.S., *Cyber Power*, Cambridge: Harvard Kennedy School, 2010, http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf (access: 27.01.2015).

Panas E., *Potęga transnarodowych organizacji społeczeństwa obywatelskiego*, in: M. Sułek (ed.), *Potęgometria*, tom I, Wyd. Europejskie Centrum Analiz Geopolitycznych, Warszawa 2013.

Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, 25 June 2013, http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html (dostęp: 27.01.2015).

Rattray G.J., *An Environmental Approach to Understanding Cyberpower*, 13 January 2015. http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-10.pdf (access: 27.01.2015).

Słownik Języka Polskiego, http://sjp.pwn.pl/sjp/cyberprzestrzeń;2553915 (access: 27.01.2015).

Słownik komputerowy i encyklopedia informatyczna, http://www.i-slownik.pl/323,cyberprzestrzen (access: 27.01.2015).

Sułek M., *Metody i techniki badań stosunków międzynarodowych*, Oficyna Wyd. ASPRA-JR, Warszawa 2004.

Sułek M., *Potęga państw. Modele i zastosowania*, Wyd. Rambler, Warszawa 2013.

The National Strategy to Secure Cyberspace, The White House Washington, February 2003. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (access: 27.01.2015).