BARTOSZ BIERNACIK

War Studies University Akademia Sztuki Wojennej

b.biernacik@akademia.mil.pl

Nauka i najnowsze narzędzia informatyczne w służbie bezpieczeństwa cyberprzestrzeni – piątego wymiaru walki zbrojnej

Science and the latest IT tools in cyber security service – the fifth dimension of armed struggle

STRESZCZENIE

Celem artykułu jest wskazanie wpływu wykorzystania teorii naukowych w działaniach w cyberprzestrzeni. Opisana w zarysie teoria sieci bezskalowych stanowi podstawę funkcjonowania wielu narzędzi informatycznych wykorzystywanych do działań w cyberprzestrzeni. Poprzez krótkie nawiązanie do początków i rozwoju teorii sieci autor przedstawia zalety i wady tej teorii i jej wpływ na dzisiejsze możliwości systemów informatycznych. Na przykładzie kilku dostępnych obecnie na rynku rozwiązań komercyjnych autor wskazuje na możliwości, które posiadają wykwalifikowani operatorzy tych systemów do prowadzenia działań zarówno w samej cyberprzestrzeni w celu minimalizacji zagrożeń wynikających z aktywności cyberprzestępców oraz grup terrorystycznych, jak również na danych zgromadzonych w Internecie Rzeczy (IoT). Wyniki pracy specjalistów IT wskazują, że tego typu rozwiązania będą stanowiły coraz istotniejsze źródło wiedzy dla służb zajmujących się cyberbezpieczeństwem i odpowiedzialnych za przeciwdziałanie terroryzmowi. Opisana teoria sieci bezskalowych jest również podstawą do funkcjonowania sieci teleinformatycznych Sił Zbrojnych RP i skutecznie wzmacnia możliwości monitorowania znaczących węzłów sieci, co pozwala na optymalizację sił i środków wykorzystywanych do tego celu, jak również skraca czas niezbędny do wykrycia i zareagowania na ewentualne incydenty komputerowe. Jest to bardzo ciekawy obszar badawczy, którego eksploracja może dać wiele znaczących rozwiązań w zakresie cyberbezpieczeństwa, czego przykładem są wyniki badań zaprezentowane w tym artykule. Wzrastające znaczenie cyberprzestrzeni nie może zostać niezagospodarowane przez Siły Zbrojne, które de-

finiują cyberprzestrzeń jako piąty wymiar walki zbrojnej – najbardziej nieobliczalny i nieokreślony oraz dający największe efekty przy minimalnych nakładach. I co najważniejsze – zapewniający niemalże całkowitą anonimowość. Stąd należy traktować go jako najbardziej wpływową przestrzeń działań militarnych.

ABSTRACT

The purpose of this article is to indicate the impact of the use of scientific theories on cyberspace. The outline of the non-scalable network, outlined in this paper, is the basis for the operation of a number of IT tools used in cyberspace. By briefly referring to the origins and development of network theory, the author presents the advantages and disadvantages of this theory and its implications for today's IT systems. On the example of several commercially available IT solutions, the author points to the opportunities that qualified operators of these systems have to address in cyberspace in order to minimize cybercrime and terrorist threats, as well as data collected on the Internet of Things (IoT). The results of IT professionals show that such solutions will be an increasingly important source of knowledge for cyber security and counter-terrorism services. The theory of non-scalable networks is also the basis for the functioning of the Polish Armed Forces network and effectively enhances the ability to monitor significant network nodes, optimizing the strengths and resources used for this purpose, as well as reducing the time needed to detect and respond to possible computer incidents. This is a very interesting research area whose exploration can bring many significant cyber security solutions, as exemplified by the results of the research presented in this article. The increasing importance of cyberspace cannot be underestimated by the Armed Forces, which define cyberspace as the fifth dimension of armed conflict – the most unpredictable and unmatched and the most effective with minimal effort. And most importantly – providing almost complete anonymity. Hence, it should be regarded as the most influential space of military activity.

Słowa kluczowe: cyberprzestrzeń, teoria sieci bezskalowych, Internet Rzeczy (IoT), Siły Zbrojne Rzeczypospolitej Polskiej, IBM i2 Analyst's, GIS, ESRI.

Keywords: cyberspace, scale-free networks, Internet of Things, Armed Forces of the Republic of Poland, IBM i2 Analyst's, GIS, ESRI.

Wprowadzenie

Dynamika rozwoju technologii informacyjnych zmusza nas do wprowadzania kolejnych zmian w dotychczasowych sposobach działania. Zwykle te zmiany następują dla nas niemalże niezauważalnie. Cyberprzestrzeń jest jednym z przykładów nowej przestrzeni, której powszechność jest często dla ludzi niezauważalna. Cyberprzestrzeń, czyli coś, gdzie na co dzień „bywamy", z czego korzystamy, bez czego nie potrafimy się obyć, a jednak jeżeli mielibyśmy zde-

finiować ją jako termin, to pojawia się problem – no bo jak zdefiniować coś, co namacalnie nie istnieje, choć wiemy, że jest?

Należy zacząć od zdefiniowania tego terminu, korzystając z dostępnych w literaturze definicji cyberprzestrzeni.

Według Wielkiego Słownika Języka Polskiego cyberprzestrzeń to: „wyobrażony świat powstały dzięki połączeniu urządzeń komputerowych w sieci umożliwiającej komunikację" (http://www.wsjp.pl/index.php?id_hasla=49602&ind=0&w_szukaj=cyberprzestrze%C5%84). Z kolei w Internecie, w i-słowniku cyberprzestrzeń to: „przestrzeń komunikacyjna tworzona przez system powiązań internetowych. Cyberprzestrzeń podobnie jak telekomunikacja ułatwia użytkownikom sieci kontakty, także w czasie rzeczywistym. Przestrzeń otwartego komunikowania się za pośrednictwem połączonych komputerów i powiązań informatycznych pracujących na całym świecie. Definicja ta uwzględnia wszystkie systemy komunikacji elektronicznej (w tym również klasyczne sieci telefoniczne), które przesyłają informacje pochodzące ze źródeł numerycznych lub przeznaczone do numeryzacji. Cyberprzestrzeń powoli staje się podstawowym kanałem wymiany informacji".

Odwołując się do definicji leksykalnej, z której pochodzi termin cyberprzestrzeń – w języku angielskim i jego angielskiego brzmienia – cyberspace. Według słownika *Collins English Dictionary* "cyberspace – all of the data stored in a large computer or network represented as a three-dimensional model through which a virtual-reality user can move".

Inna słownikowa definicja jest znacznie bardziej rozbudowana. „Cyberspace – the space in which computer transactions occur, particularly transactions between different computers. We say that images and text on the Internet exist in cyberspace, for example. The term is also often used in conjunction with virtual reality, designating the imaginary place where virtual objects exist. For example, if a computer produces a picture of a building that allows the architect to "walk" through and see what a design would look like, the building is said to exist in cyberspace" (*The American Heritage® New Dictionary of Cultural Literacy*, Third Edition. Published by Houghton Mifflin Company).

Jako ostatnią z przytaczanych posłużmy się definicją z obszaru wojskowego, opublikowaną w dokumencie JP 3-12, gdzie cyberspace – „is a the global domain within the information environment consisting of the interdependent network of information technology (IT) infrastructures and resident data, inclu-

ding the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Developments in cyberspace provide the means for the US military, its allies, and partner nations to gain and maintain a strategic, continuing advantage in the operational environment (OE), and can be leveraged to ensure the nation's economic and physical security. Cyberspace reaches across geographic and geopolitical boundaries, much of it residing outside of US control, and is integrated with the operation of critical infrastructures, as well as the conduct of commerce, governance, and national security. Access to the Internet provides adversaries the capability to compromise the integrity of US critical infrastructures in direct and indirect ways. These characteristics and conditions present a paradox within cyberspace: the prosperity and security of our nation have been significantly enhanced by our use of cyberspace, yet these same developments have led to increased vulnerabilities and a critical dependence on cyberspace, for the US in general and the joint force in particular. Cyberspace can be described in terms of three layers: physical network, logical network, and cyber-persona. Each of these represents a level on which cyber operation (CO) maybe conducted" (Joint Publication 3-12 (R), Cyberspace Operations, 5 February 2013 p. I-1, I-2).

Należy również zaznaczyć, że cyberprzestrzeń została przyjęta jako piąty obszar działań w przypadku działań zbrojnych. Wprawdzie już we wspomnianym dokumencie JP 3-12 (Joint Publication 3-12 (R), Cyberspace Operations, 5th February 2013 p. I-2) wspomniano o cyberprzestrzeni w tym kontekście, jednak dopiero na szczycie NATO w Warszawie w lipcu 2016 roku oficjalnie uznano, że cyberprzestrzeń jest nowym, piątym środowiskiem walki po obszarze lądowym, przestrzeni powietrznej, obszarach morskich i kosmosie. Można w niej toczyć walkę i wojnę informacyjną. Cyberprzestrzeń jest obecnie traktowana jako bardzo istotne miejsce, w którym już w tej chwili prowadzone są działania zbrojne, mające na celu wpływanie na inne państwa w celu osiągnięcia własnych celów. Jest to niezmiernie obiecujący obszar dla wszystkich aktywnych „graczy", których celem jest np. destabilizacja gospodarcza, wpływ polityczny na wybrane kraje (wpływ na wyniki wyborów), jak również tworzenie przewagi informacyjnej nad pozostałymi państwami. Niewiele krajów wytworzyło już zdolności do prowadzenia aktywnych działań w cyberprzestrzeni, co powinno skłonić naszych decydentów nad prowadzeniem aktywnych działań w kierunku osiągnięcia zdolności do obrony przed agresją innych państw w cyberprzestrzeń RP.

Stąd nasuwają się pytania: w jaki sposób funkcjonuje cyberprzestrzeń, jak można ją opisać i zamodelować oraz w jaki sposób posiadaną wiedzę wykorzystać w celu osiągnięcia przewagi w tym wymiarze walki? A tezą, która przyświeca autorowi, jest wykazanie czytelnikom, że znajomość teorii sieci bezskalowych jest kluczowa do sprawnego zarządzania zasobami w cyberprzestrzeni i stanowi podstawę zarówno do prowadzenia działań obronnych, jak i ofensywnych. Świadomość zalet i wad oraz możliwość modelowania pewnych zjawisk w modelach matematycznych pozwala na znaczący wzrost efektywności w wykorzystaniu posiadanego zarówno potencjału ludzkiego, jak i sprzętowego w działaniach prowadzonych w cyberprzestrzeni oraz na minimalizację ryzyka wystąpienia zakładanych i skalkulowanych wcześniej ryzykownych zdarzeń (których zaistnienie można zasymulować, a zatem i w pewnym sensie przygotować się na ich ewentualne wystąpienie).

Cyberprzestrzeń jest o tyle istotna dla funkcjonowania państwa, że działania w niej mają bezpośredni wpływ na wszystkie jego kluczowe elementy składowe. Rysunek nr 1 przedstawia wpływ działań w cyberprzestrzeni na infrastrukturę krytyczną państwa.

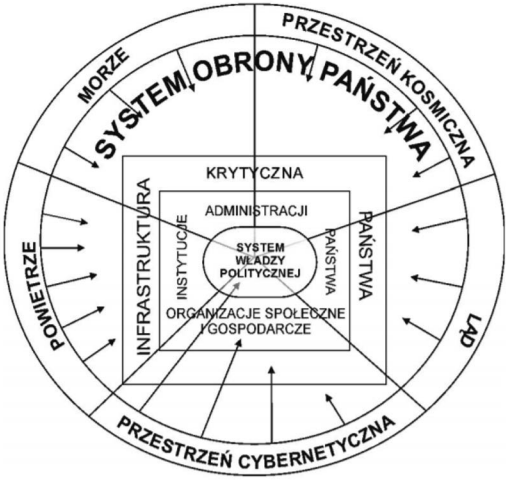
Wykorzystywane w tym celu są takie narzędzia, jak: cyberterroryzm, cyberszpiegostwo, haktywizm oraz operacje zbrojne w cyberprzestrzeni. Dla czytelników, którzy wątpią w realizm zagrożeń wynikających z rozwoju informatyki i istnienia piątego wymiaru działań zbrojnych, warto przytoczyć kilka przykładów na tego typu działania.

Działania w cyberprzestrzeni w sposób zorganizowany i przemyślany na niekorzyść drugiej strony są obecnie dość powszechne (specjaliści zajmujący się cyberbezpieczeństwem podają przykłady takiej aktywności z każdego dnia) i można przytaczać ich dość dużo (choć znacząca ich część nie jest znana opinii publicznej). Do najważniejszych z nich autor zalicza następujące, przedstawione poniżej: 2007 rok – Estonia przytaczana oficjalnie przez media jako pierwszy kraj na świecie zaatakowany w cyberprzestrzeni – poprzez Internet w niespotykanym wcześniej stopniu. W wyniku trwającej trzy tygodnie kampanii cyberataków nie tylko zablokowano strony internetowe wielu instytucji publicznych, lecz także naruszono wybrane elementy infrastruktury krytycznej.

W efekcie tego zdarzenia Estonia zdecydowała się na wyjątkowy krok, niespotykany nigdy wcześniej – wszystkie serwery rządowe przeniosła bowiem poza granice swojego kraju, aby ich bezpieczeństwo było chronione zarówno

przez fizyczną odległość od potencjalnego przeciwnika/agresora, jak również przez dodatkowe narzędzia informatyczne stosowane w kraju gospodarza ich danych. Ponadto byłby to również dodatkowy argument i szansa, w przypadku ponownego ataku, na udowodnienie go na arenie międzynarodowej – „złapanie agresora za rękę".

Rysunek 1. Wpływ cyberprzestrzeni na kluczowe elementy państwa



Źródło: P. Sienkiewicz, H. Świeboda, *Analiza systemowa bezpieczeństwa cyberprzestrzeni państwa,* Polskie Stowarzyszenie Zarządzania Wiedzą, seria: Studia i Materiały, nr 33, 2010, s. 29.

Drugi przykład z 2007 roku to z kolei aktywność Izraela, który we wrześniu, w ramach operacji „Orchard" dokonał sabotażu wobec systemu obrony przeciwlotniczej Syrii. Z kolei w sierpniu 2008 roku możliwości aktywnej działalności w cyberprzestrzeni wykorzystano przeciwko Kirgistanowi. Długotrwałe działania skierowane były na destabilizację tego rejonu świata. Innym przykładem działalności aktywnej to działalność Stanów Zjednoczonych przeciwko Iranowi. Amerykańskie służby wywiadowcze stworzyły, a następnie wykorzystały niezwykle zaawansowany, złośliwy program komputerowy Stuxnet, aby sabotować irański program atomowy. Właściwie należy wspomnieć, że powstała cała rodzina programów, pod nazwą Stuxnet, które były wielokrotną próbą wykonania ataku cybernetycznego na infrastrukturę krytyczną Iranu, w celu przerwania realizacji ich programu atomowego przez uszkodzenie wirówek niezbędnych

do produkcji na potrzeby programu atomowego. Efekty samego ataku są wątpliwe, gdyż Iran dysponuje obecnie znacznie większą liczbą wirówek niż przed atakiem, stąd początkowo ogłoszony przez USA sukces okazał się w dłuższej perspektywie porażką.

Możliwość działania w cyberprzestrzeni nie ogranicza się tylko do największych mocarstw współczesnego świata. Atakowani są również najwięksi gracze w tym wymiarze walki – tacy jak Stany Zjednoczone, które stały się najpopularniejszym obiektem miliardów prób włamań komputerowych w ostatnich latach. Cyberataki posłużyły ponadto jako nowy sposób wywierania nacisku politycznego podczas napięć na Półwyspie Koreańskim, między innymi w latach 2011 i 2013.

Niezmiernie istotny ostatnio stał się nowy rodzaj działań w cyberprzestrzeni – chodzi o całkowicie nowy wymiar działań – kreowanie sytuacji politycznej w krajach trzecich. Dowodem na to mogą być ostatnie wybory w USA, których wyniki budzą coraz większe wątpliwości, wraz z ujawnianiem przez prowadzących śledztwo specjalistów działań Federacji Rosyjskiej w trakcie ich trwania, co zadecydowało o wyborze obecnego prezydenta Stanów Zjednoczonych. Podobne próby podejmowane były w 2017 roku w trakcie wyborów w Niemczech oraz we Francji.

Analizując aktywność w cyberprzestrzeni, należy podkreślić, że w znaczącej większości (niestety dotyczy to również Polski), rządy poszczególnych państw, z wyjątkiem kilku pionierów w tej dziedzinie, nie dostrzegały szybko rosnącej skali wyzwań. Do przełomu w tym zakresie doszło dopiero niedawno, jednakże można mieć wątpliwości, czy nie nastąpiło to zbyt późno. Stąd należy z nadzieją przyjąć ogłoszoną w październiku 2017 roku decyzję Ministra Obrony Narodowej o stworzeniu nowego Rodzaju Sił Zbrojnych – Wojsk Cybernetycznych, decyzję niezmiernie ważną i kluczową dla Polski, jednakże podjętą o dekadę za późno, gdyż pierwszych jej efektów można się spodziewać właśnie po takim czasie, czyli pierwsze możliwe pozytywne efekty w bezpieczeństwa Polski w cyberprzestrzeni należy oczekiwać dopiero około 2030 roku…

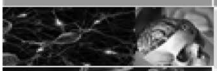
Jak zatem nauka może nas wspierać w lepszym zarządzaniu cyberprzestrzenią i zasobami w niej zgromadzonymi. Analiza przytoczonych definicji zmusza do zastanowienia, skąd aż taka rozpiętość w definiowaniu tego samego zjawiska. Okazuje się bowiem, że każda z tych definicji cyberprzestrzeni różni się od siebie. Jednak cechą wspólną jest występowanie połączenia, czyli sieci między

komputerami oraz wymiana danych. Stąd w dalszej części artykułu autor postara się przedstawić właśnie jedną z tych „stałych", występującą w definicjach cyberprzestrzeni, a więc niejako współtworzącą ją składową – sieci, dzięki którym wymiana danych czy też komunikacja jest możliwa.

Cały świat to sieć

„All the world is a net" – powiedział David Cohen i przytoczył ku temu swoje dowody, publikując na łamach czasopisma naukowego przykłady, gdzie można doszukać się występowania sieci w najróżniejszych formach. Rysunek 2 przedstawia przykład sieci, z istnienia których często nie zdajemy sobie nawet sprawy.

Rysunek 2. Przykłady sieci występujących w różnych aspektach naszego życia

	Sieć	Węzły	Gałęzie
	Układ nerwowy	Komórki nerwowe	Aksony i dendryty
	Sieci genetyczne	Białka i geny	Chemiczne interakcje
	Sieci transportowe	Miejscowości	Drogi (lotnicze, drogowe, kolejowe, wodne)
	World Wide Web	Dokumenty	Hiperlinki
	Internet	Routery	Połączenia (kable, światłowody i inne)
	Sieci społecznościowe	Osoby	Interakcje społeczne

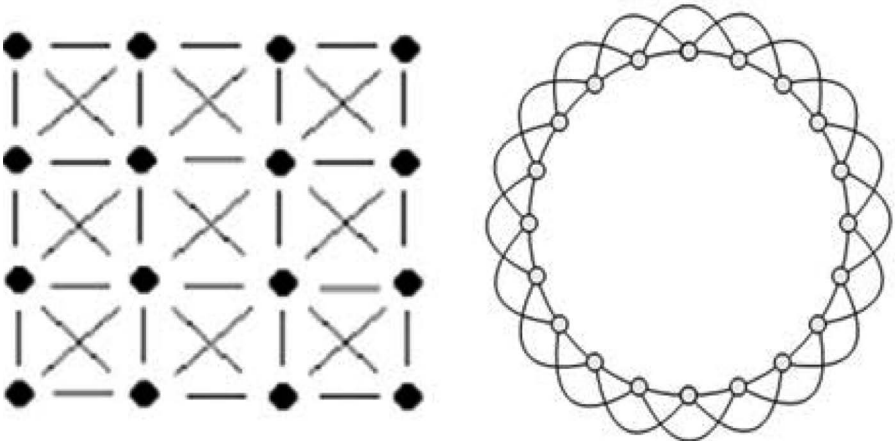
Źródło: opracowanie własne.

Istnienie sieci w naszych mózgach, w których siecią jest układ nerwowy, węzły stanowią komórki nerwowe, gałęziami zaś są dendryty i aksony, jest zapewne oczywiste dla każdego z nas, jednak można podać przykłady mniej oczywiste, jak choćby sieci społecznościowe, w których węzłami są osoby, a gałęziami ich powiązania z innymi – powiązania społeczne. Równie mało znane mogą być dla „zwykłych śmiertelników" informacje o budowie sieci Internet, gdzie węzłami są routery (oraz inne urządzenia sieciowe), a gałęziami połączenia między nimi (światłowody, kable i inne).

Jak zatem opisać w sposób naukowy to, co nas otacza i – jak się okazuje – jest dość powszechne? Problematyką sieci zajmowało się wielu znamienitych matematyków, dzięki którym teoria sieci jest dość rozbudowana i obejmuje najróżniejsze rodzaje sieci: od sieci deterministycznych (regularnych, fraktalnych, złożonych sieci deterministycznych), przez sieci przypadkowe, a w nich sieci statyczne (sieci małych światów, grafy przypadkowe, sieci z ukrytymi zmiennymi, sieci z zadanym hamiltonianie) oraz sieci ewoluujące (model Alberta Baràbasiego i inne). Wyniki ich prac znalazły wykorzystanie w wielu rozwiązaniach znanych nam na co dzień, a sama teoria sieci nadal się rozwija.

Jako pierwszy z przypadków można rozpatrzeć sieci regularne (rysunek 3), w których zakłada się istnienie stałej liczby węzłów z taką samą liczbą połączeń. Jest to przypadek bardzo trudny do odnalezienia w naturze, gdyż, jak wskazują sami matematycy, nawet diament ma w swojej strukturze kryształu skazy, które powodują, że nie stanowi on odwzorowania takiej sieci.

Rysunek 3. Przykłady sieci regularnych



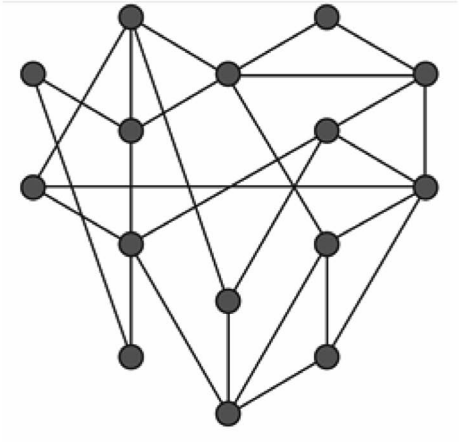
Źródło: opracowanie własne.

Na przeciwnym biegunie można przedstawić inny przykład sieci – sieci losowych, których cechą charakterystyczną jest to, że mają one ustaloną liczbę węzłów N; węzły te zaś posiadają losową liczbę połączeń o prawdopodobieństwie p. Każdy z węzłów takiej sieci ma w przybliżeniu taką samą liczbę połączeń (rysunek 4).

Rysunek 4. Przykład sieci losowej E-R

- Sieć o ustalonej liczbie węzłów **N**
- Węzły posiadają losową liczbę połączeń o prawdopodobieństwie **p**
- Każdy z węzłów ma w przybliżeniu taką samą liczbę połączeń

Paul Erdős
(1913-1996)



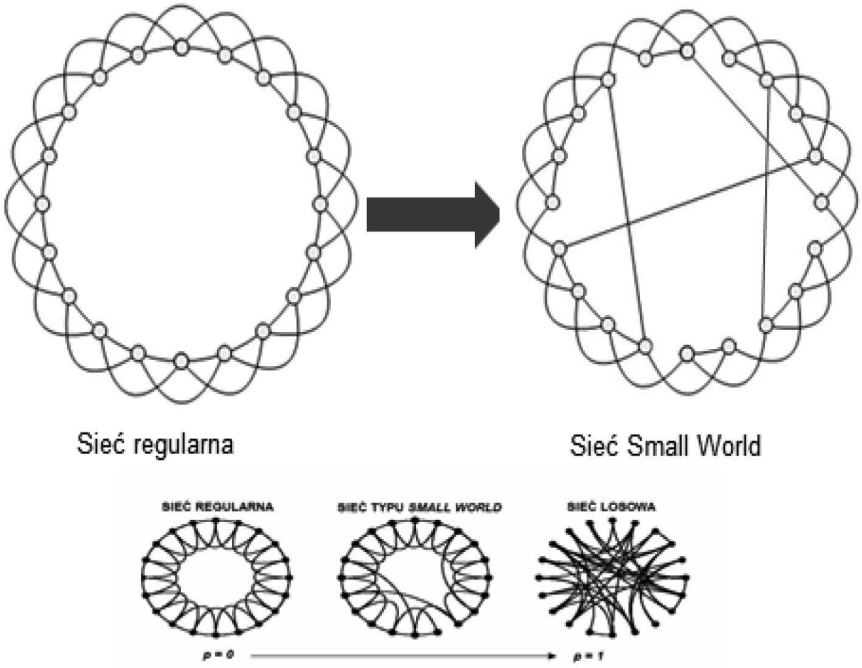
Źródło: opracowanie własne.

Sieci te są często nazywane sieciami E-R, od nazwy ich odkrywcy, węgierskiego matematyka, Paula Erdősa (26.03.1913–20.09.1996). Był on jednym z najwybitniejszych matematyków XX w., autorem ponad 1500 artykułów z koncepcjami matematycznymi, głównie z teorii liczb, kombinatoryki i teorii grafów.

Przytoczone przykłady są dość trudne do odnalezienia w realnym świecie, gdyż z jednej strony mamy do czynienia z idealizacją świata, z drugiej zaś z przykładem totalnej przypadkowości. Trudno za ich pomocą opisywać zjawiska występujące w naturze i wykorzystywać je do przewidywania zachowań zjawisk naturalnych. Rozwiązaniem pośrednim są sieci, które „przekształcają" idealne połączenia sieci regularnych w przypadek pośredni między sieciami losowymi a regularnymi. Tym pośrednim rodzajem sieci są sieci typu „Small World" (SW) (rysunek 5).

Naukowcy Watts i Strogatz zauważyli, że dokonując pewnego zabiegu na sieci regularnej, można otrzymać modele sieci, które można zidentyfikować w rzeczywistych systemach. Nie są one bowiem ani doskonale regularne, ani zupełnie losowe, a można je budować przez zastosowanie tzw. przekablowania (ang. rewiring) niektórych węzłów sieci regularnej.

Rysunek 5. Przykład sieci Small World – SW



Źródło: opracowanie własne.

Jeśli przez p oznaczymy prawdopodobieństwo, że powiązania losowo wybranego węzła sieci zostaną zmienione („przekablowane"), całą procedurę przejścia od sieci regularnej do sieci typu Small World opisać można następująco:

1. Wybieramy losowo węzeł.
2. Odcinamy jedno z jego (na ogół bliskich) powiązań.
3. Wybieramy losowo (na ogół odległy) węzeł.
4. Odcinamy jedno z jego powiązań.
5. Łączymy oba węzły.
6. Powtarzamy czynność 1–5 dopóki ułamek węzłów objętych zmodyfikowanymi połączeniami wyniesie p.

Stopień separacji – centrum grawitacji

Przykład sieci typu SW jest już zaczątkiem do naszych rozważań. Wyjaśnienie zjawiska jest możliwe za pomocą wyników eksperymentu, przeprowadzonego w Stanach Zjednoczonych. Polegał on na wykryciu pewnej reguły, polegającej na tym, że pomiędzy poszczególnymi węzłami sieci można określić tzw. stopień separacji, czyli uśrednioną odległość, którą należy pokonać od jednego dowolnego węzła, do drugiego dowolnego węzła tejże sieci.

Stanley Migram (ale nie tylko on, ponieważ podobne eksperymenty prowadzili również inni naukowcy) przeprowadził eksperyment, który miał na celu ustalenie, z jakim prawdopodobieństwem dwie losowo wybrane osoby będą się znały. W tym celu wysyłał przesyłki z Nebraski i Kansas w USA do Bostonu do osób losowych z zapytaniem, czy znają wskazaną w przesyłce osobę. Jeżeli tak, miały odesłać przesyłkę na adres zwrotny, jeżeli nie to miały ją przesłać dalej, do osoby, która według nich może wskazaną osobę znać.

Efekt eksperymentu nie był wprawdzie specjalnie spektakularny, gdyż tylko 64 z 296 przesyłek zostało dostarczonych do celu. Dało to jednak możliwość wyznaczenia średniej długości ścieżki dla dostarczonych przesyłek – wynosiła ona w przybliżeniu ~ 6.

Wyniki tych badań stały się siłą napędową do kolejnych eksperymentów. Najbardziej powszechną obecnie siecią jest najprawdopodobniej sieć społecznościowa Facebook, w której jak wykazały przeprowadzone badania, stopień separacji wynosi jedynie 3,75, czyli w przybliżeniu ~ 4.

Sposobem na zrozumienie pojęcia stopień separacji jest wykorzystanie w tym celu innej przykładowej sieci społecznościowej, na bazie której stworzona została gra „Kevin Bacon". Jest to przykład sieci znanych aktorów, którzy są podawani w zestawieniu aktorów i aktorek z przedstawicielem aktorów z Hollywood – Kevina Bacona. Na stronie www.cs.virginia.edu/oracle można podawać dowolne nazwiska aktorów i aktorek i sprawdzić, z jakim stopniem separacji pomiędzy wskazanym aktorem lub aktorką a Kevinem Baconem mamy do czynienia. Wspomniany aktor jest uznawany za osobę będącą tzw. centrum grawitacji (ang. centre of gravity), czyli znaczącym węzłem w danej sieci, o czym więcej w dalszej części artykułu. We wspomnianej sieci aktorów początkowo odgrywał tę rolę właśnie aktor Kevin Bacon, ale z upływem czasu okazało się, że sieć ewoluuje i obecnie wielu innych znanych aktorów i aktorek można wskazać jako lepsze centrum wszechświata/grawitacji od wspomnianego aktora – co ilustruje poniższy rysunek 6.

Rysunek 6. Lista 30 aktorów i aktorek - centrów wszechświata/grawitacji w Hollywood

1. **Eric Roberts** (I) (2.83285)
2. **Michael Madsen** (I) (2.85125)
3. **Harvey Keitel** (2.85789)
4. **Danny Trejo** (2.85820)
5. **Samuel L. Jackson** (2.86360)
6. **Robert De Niro** (2.86777)
7. **Donald Sutherland** (I) (2.86991)
8. **Udo Kier** (2.87229)
9. **Malcolm McDowell** (2.87378)
10. **Michael Caine** (I) (2.87567)
11. **Martin Sheen** (2.87602)
12. **Willem Dafoe** (2.87956)
13. **Seymour Cassel** (2.88339)
14. **Morgan Freeman** (I) (2.88826)
15. **David Carradine** (2.88939)
16. **John Hurt** (2.89290)
17. **Dennis Hopper** (2.89446)
18. **Christopher Plummer** (I) (2.89467)
19. **John Savage** (I) (2.89628)
20. **Max von Sydow** (I) (2.89663)
21. **Bruce Willis** (2.89665)
22. **Rance Howard** (2.89719)
23. **John Malkovich** (2.90096)
24. **Christopher Lee** (I) (2.90431)
25. **Liam Neeson** (2.90484)
26. **Richard Riehle** (2.90500)
27. **Christopher Walken** (2.90538)
28. **Tom Sizemore** (2.90773)
29. **John Turturro** (2.90803)
30. **Ben Kingsley** (2.90825)

W nawiasach podano wyliczony stopień separacji.

Źródło: opracowanie własne na podstawie wyników na stronie www.cs.virginia.edu/oracle . [dostęp październik 2017].

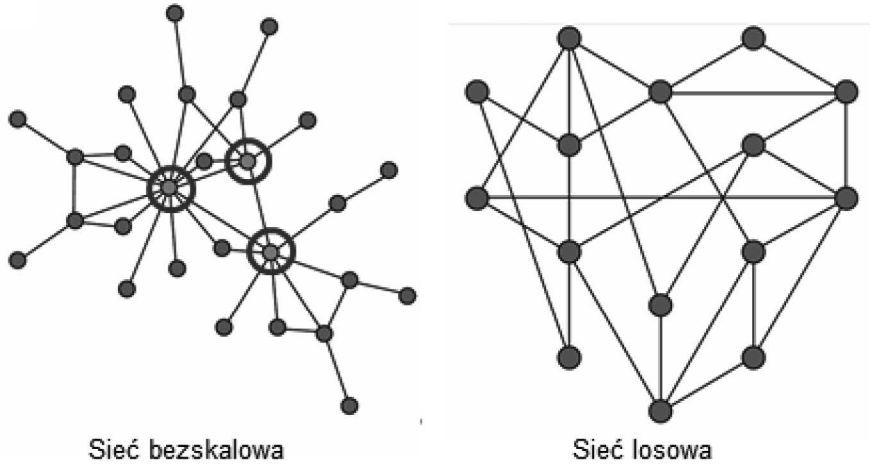
Innym przykładem sieci o określonym stopniu separacji jest powszechnie znana sieć – sieć stron WWW. Okazuje się bowiem, że przejście z dowolnej strony WWW na inną, losową stronę WWW można wykonać, wykonując 19 kliknięć, czyli stopień separacji w przypadku stron WWW wynosi 19 (John Guare, New Scientist, 4 December 1999, p. 24).

Swoje badania nad tymi wynikami przeprowadził również inny uczony, Albert Barabàsi. Według jego obliczeń nawet przy wzroście liczby stron WWW o 1000%, stopień separacji wzrośnie z 19 jedynie do 21 kliknięć.

Sieci bezskalowe

Wyniki tych badań, wskazujące na sieci, w których istnieją bardzo znaczące węzły (takie jak wspomniana gwiazda Hollywood Kevin Bacon), podczas gdy inne są dla istnienia samej sieci mniej istotne, skłoniły Alberta Barabàsi do stworzenia i opisania (rysunek 7) nowego rodzaju sieci – sieci bezskalowych (ang. Scale-Free networks).

Rysunek 7. Przykład sieci bezskalowej Alberta Barabàsiego



Zaznaczone na niebiesko węzły to huby.

Źródło: opracowanie własne.

Zauważył on bowiem w opisanych wcześniej rodzajach sieci ER i SW następujące problemy:

- liczba N węzłów jest w większości realnych sieci zmienna, otwarta i zwiększa się w trakcie życia sieci;
  - przykład – sieć stron WWW: ciągłe dodawanie nowych dokumentów;
- prawdopodobieństwo połączenia dwóch wierzchołków p nie jest losowe i jednakowe;
  - przykład – nowe węzły „chcą się przyłączać" do „dobrze znanych" węzłów (Google, CNN, WP, Onet itp.).

Albert Barabàsi zauważył, że istnieją w sieciach, takich jak Internet, czy też w sieciach społecznościowych, węzły o bardzo dużej liczbie połączeń, jak również węzły o małej liczbie połączeń. Te o dużej liczbie połączeń nazwał hubami, czyli elementami o bardzo istotnym znaczeniu dla sieci. Można je porównać do wspomnianych wcześniej centr grawitacji, jak ma to miejsce w przypadku sieci aktorów i przywołanego aktora Kevina Bacona.

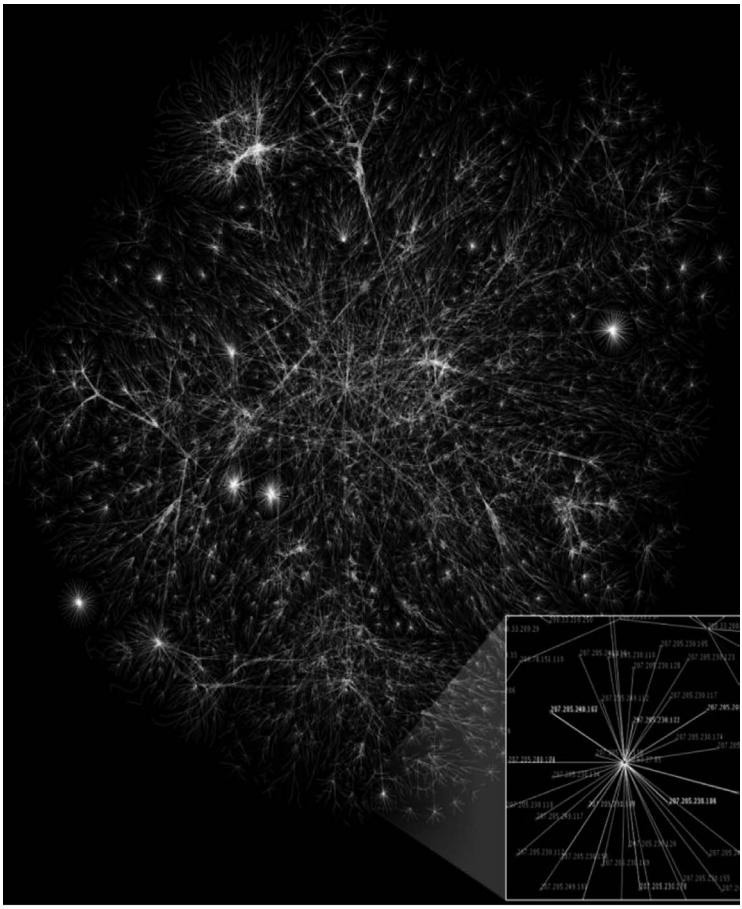
Z tych rozważań powstał model tzw. sieci bezskalowych, które charakteryzują się tym, że:

1. Istnieje w nich ciągły wzrost liczby węzłów i połączeń.

2. Posiadają one połączenia „preferowane" do węzłów posiadających najwięcej połączeń – dołączenia preferencyjne (ang. preferental attachement).
3. Węzły posiadające dużą liczbę połączeń to huby.
4. Huby mają bardzo istotny wpływ na całą sieć.

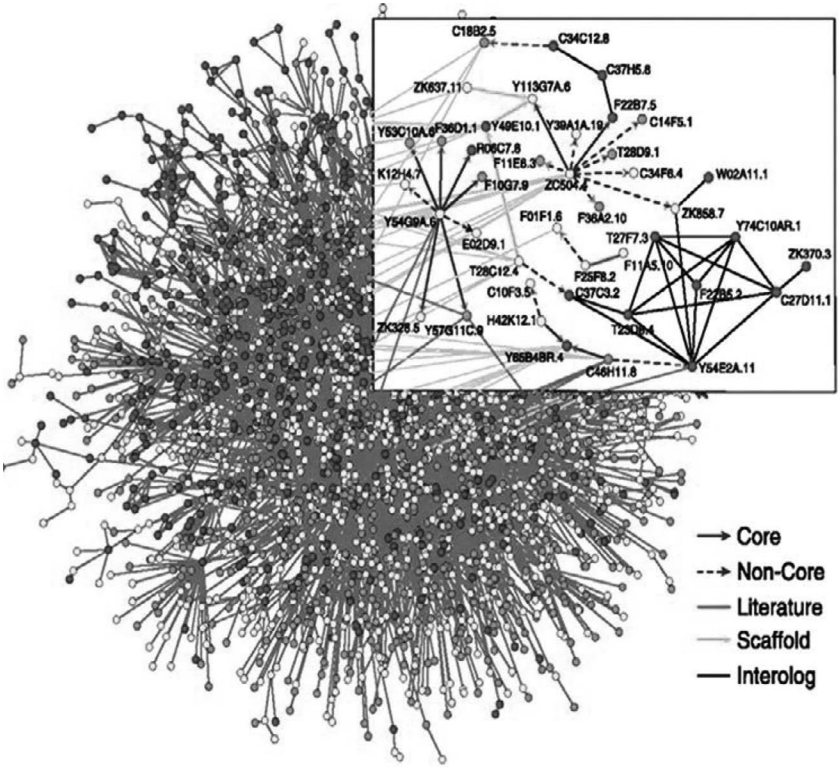
Przykładów sieci bezskalowych można podać bardzo wiele, praktycznie z każdej dziedziny naszego życia. Od wspomnianego Facebooka, przez sieć Internet (rysunek 8), a na mapach sieci interakcji białek kończąc (rysunek 9).

Rysunek 8. Przykład sieci bezskalowej – Internet



Źródło: https://en.wikipedia.org/wiki/Scale-free_network (dostęp: grudzień 2016).

Rysunek 9. Przykład sieci bezskalowej – sieć interakcji białek



Źródło: http://jcs.biologists.org/content/118/21/4947 (dostęp: listopad 2016).

I to można uznać za zaletę tego typu sieci. Jednak ten sam atak, na 5% węzłów, ale tym razem przeprowadzony na huby, czyli na węzły istotne dla sieci, powoduje podwojenie stopnia separacji, czyli w sposób znaczący obniża się skuteczność funkcjonowania zaatakowanej sieci.

Jakie znaczenie mają wymienione powyżej cechy sieci bezskalowych dla naszej działalności w cyberprzestrzeni? Znajomość ich zalet i wad ma istotny wpływ na funkcjonowanie naszych systemów wojskowych i sieci dostarczających do nich danych. Z jednej strony daje nam to szansę na lepsze ich zabezpieczanie, znając bowiem ich „słabe strony", możemy przeciwdziałać możliwym atakom z zewnątrz, a z drugiej strony mamy szansę na działania aktywne, zakłócając lub całkowicie likwidując wybrane sieci komunikacyjne strony przeciwnej.

Charakterystyczne dla sieci bezskalowych jest to, że są znacznie bardziej odporne na ataki od sieci losowych. Badania pozwoliły ustalić, że atak na sieć bezskalową na losowe 5% węzłów nie powoduje zwiększenia liczby skoków potrzebnych do jej pokonania (stopni separacji).

Inny, bardziej wymowny przykład, to atak losowy na sieć. Sieć bezskalowa jest odporna na ataki skierowane losowo. Znacznie bardziej prawdopodobne jest wówczas wyeliminowanie węzła niebędącego hubem – w efekcie skutki są odczuwane jedynie lokalnie i nie dezintegrują sieci jako całości. Natomiast zaatakowanie odpowiednio dużej liczby hubów może spowodować całkowitą dezintegrację sieci – czyli pozwala na całkowite wyeliminowanie jej z działania. Tabela 1 przedstawia zestawienie największych korzyści i zagrożeń wynikających z teorii sieci bezskalowych.

Tabela 1. Korzyści i zagrożenia związane z sieciami bezskalowymi

Lp.	Korzyść	Zagrożenie
1	**Usunięcie 5% przypadkowych węzłów** z sieci bezskalowej **nie wpływa** na zwiększenie liczby skoków potrzebnych do pokonania sieci	**Usunięcie 5% hubów** z sieci bezskalowej powoduje **podwojenie liczby skoków** potrzebnych do pokonania sieci
2	Sieć bezskalowa jest **odporna na ataki skierowane losowo**. Znacznie bardziej prawdopodobne jest wówczas wyeliminowanie węzła niebędącego hubem – w efekcie skutki są odczuwane jedynie lokalnie i nie dezintegrują sieci jako całości	Zaatakowanie **odpowiednio dużej liczby hubów** może w praktyce **całkowicie wyeliminować sieć z użytku**
3	Posiadając odpowiednie narzędzia, można monitorować takie sieci i eliminować „huby", a tym samym dezintegrować całe grupy terrorystyczne działając cały czas w ukryciu	Działania terrorystów (np. ISIS) są bardzo trudne do wykrycia, a efekty ich działań wpływają bardzo destruktywnie na sytuację w Europie – do przygotowania zamachów, wyszukiwania nowych członków terroryści wykorzystują sieci m.in. społecznościowe (Facebook, Twitter)
4	Skuteczna ochrona hubów może znacząco ograniczyć lub całkowicie uniemożliwić „epidemię" wirusów	Rozprzestrzenianie się **wirusów sieciowych** w przypadku „napotkania" na swojej drodze odpowiednio dużej liczby hubów oznacza **„epidemię"**

Źródło: opracowanie własne.

Podobnie do podanych powyżej przykładów cechy te można odnaleźć w sieciach społecznościowych, takich jak Facebook, Twitter i innych.

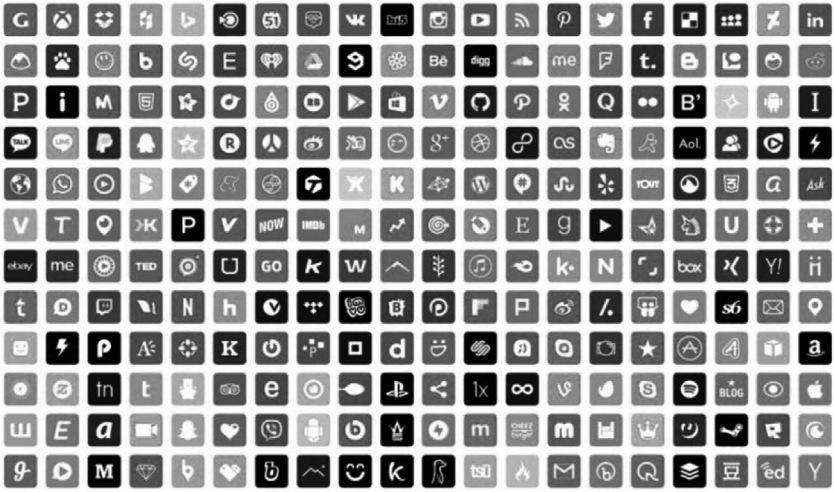
Cytując prof. Sienkiewicza: „w globalnym społeczeństwie uzyskaliśmy informacje nawet w nadmiarze, stwarzamy warunki do czerpania z niej wiedzy i żyjemy nadzieją na pozyskania mądrości. Uzyskaliśmy wolność, w tym »wolność do wyboru«, lecz nie uległa bynajmniej redukcji niepewność i poczucie ryzyka w sytuacjach decyzyjnych w złożonym i dynamicznym środowisku" (Sienkiewicz, 2013).

Internet Rzeczy (IoT)

Dynamika rozwoju Technologii Informacyjnych spowodowała, że Internet przekształcił się w nowy byt – Internet Rzeczy (ang. Internet of Things – IoT). Jest to miejsce, w którym gromadzone są ogromne ilości danych, nad którymi coraz trudniej zapanować i wykorzystać (rysunek 10). Jednakże wspomniana teoria sieci bezskalowych daje możliwości wykorzystania najnowszych rozwiązań – systemów informatycznych, do ich analizy i wyciągania niezbędnych informacji, pozwalających na uzyskanie świadomości sytuacyjnej – a w efekcie wiedzy niezbędnej do proaktywnego reagowania na zdarzenia, które jeszcze nie miały miejsca, a które w najbliższym czasie mogą się wydarzyć – patrz działalność grup terrorystycznych i planowanie przez nie ataków terrorystycznych przy wykorzystaniu sieci społecznościowych w IoT. Ma to miejsce obecnie, a narzędzia informatyczne starają się dać odpowiednie narzędzia siłom porządkowym starającym się przeciwdziałać ich aktywności.

Działania terrorystów (np. ISIS) są bardzo trudne do wykrycia, a efekty ich działań wpływają bardzo destruktywnie na sytuację w Europie – bardzo istotne w tym wszystkim jest to, że do przygotowania zamachów, wyszukiwania nowych członków terroryści wykorzystują sieci m.in. społecznościowe (Facebook, Twitter). Stąd pojawiła się ostatnio konieczność nadzorowania tych sieci i badania różnych grup społecznościowych, kontrolowania ich działań, poznawania hubów w danej grupie i oddziaływanie na te grupy w taki sposób, aby wyprzedzać działania terrorystów oraz minimalizować ich skuteczność. Takie informatyczne narzędzia powstały i są szeroko wykorzystywane przez służby specjalne wielu krajów. Autor miał okazję obserwować praktyczny pokaz działania takiego narzędzia, jednak ze względu na niejawny charakter tych działań nie ma możliwości na szersze zaprezentowanie sposobu jego działania, którego istotą jest uzyskanie przez operatora możliwości rozpoznania sposobu konstrukcji danej sieci, wyszukania w czasie zbliżonym do rzeczywistego hubów i umożliwienie nadzorowania ich aktywności.

Rysunek 10. Liczba sieci społecznościowych dostępnych w Internecie stale rośnie – stają się trudne do śledzenia przez „zwykłego" użytkownika



Źródło: http://google.pl (dostęp: październik 2017).

Jednym z narzędzi informatycznych dającym ogromne możliwości i funkcjonalności specjalistom z zakresu bezpieczeństwa jest rodzina rozwiązań informatycznych oferowanych obecnie przez firmę IBM pod nazwą i2 (rysunek 11).

Rysunek 11. Możliwość „opanowania" portali społecznościowych przez narzędzia informatyczne i dokonanie analizy danych w nich zgromadzonych

Źródło: materiały firmy IBM dotyczące rozwiązań i2.

Jest to bardzo szeroki wachlarz rozwiązań, obejmujący takie rozwiązania jak:

- i2 Analyst's Workstation;
- i2 Analyst's Notebook:
  - i2 Analyst's Notebook Connector for ESRI;
  - ii2 Analyst's Notebook Premium;
  - ii2 Analyst's Notebook SDK.
- i2 Analyze;
- i2 Chart Reader;
- i2 COPLINK;
- i2 Enterprise Insight Analysis;
- i2 iBase;
- i2 iBase IntelliShare;
- i2 iBase Plate Analysis;
- i2 Integrated Law Enforcement;
- i2 Pattern Tracer;
- i2 Text Chart.

Lista rozwiązań pochodzi ze strony producenta, choć nie jest to zapewne lista pełna (http://www-03.ibm.com/software/products/pl/atoz#tab_F-K oraz http://www-03.ibm.com/software/products/pl/category/prescriptive-analytics [dostęp kwiecień 2017 r.]).

Każde z wymienionych rozwiązań to oddzielne rozwiązanie dedykowane wybranym aspektom analizy danych. Można jednak w sposób zwięzły i mocno uogólniony opisać możliwości tych rozwiązań jako całości – jednej rodziny rozwiązań. Każdy z wymienionych produktów jest w pełni współzależny od pozostałych i do wykonania pełnej analizy danych czy stworzenia pełnego obrazu badanej sieci powiązań być może będzie konieczne skorzystanie z więcej niż jednego rozwiązania z tej rodziny systemów.

I2 umożliwia efektywne przechowywanie danych i zarządzanie nimi. Oprogramowanie konsoliduje informacje przechowywane w centralnej lokalizacji i automatyzuje powtarzalne zadania. Co podkreśla producent, rodzina tych rozwiązań pozwala na uwolnienie wartości tkwiącej w danych. Użytkownicy mogą płynnie przechodzić między różnymi typami analiz: trendów, wzorców w danych, wzorców przestrzennych lub powiązań istniejących w danych (http://www-03.ibm.com/software/products/pl/analysts-workstation [dostęp kwiecień 2017 r.]).

Cytując producenta oprogramowania: „IBM i2 Analyst's Workstation to zintegrowany pakiet narzędzi do analizy wielowymiarowej i wizualizacji, który umożliwia analitykom bezpośrednie wykorzystanie posiadanych informacji oraz oferuje im potężny aparat wspomagający interpretację tych informacji. Upraszcza tworzenie i rozpowszechnianie praktycznych opracowań wspomagających śledztwa i operacje wywiadowcze" (http://www-03.ibm.com/software/products/pl/analysts-workstation [dostęp kwiecień 2017 r.]).

Z kolei kolejne z rodziny rozwiązań, „IBM i2 Analyst's Notebook to środowisko wizualnej analizy wywiadowczej, które pomaga w optymalnym wykorzystaniu wartości informacji zbieranych przez instytucje publiczne i przedsiębiorstwa. Umożliwia analitykom szybkie porządkowanie, analizowanie i wizualizowanie danych pochodzących z różnych źródeł i skraca czas potrzebny na wydobycie najważniejszych informacji ze złożonych danych, oferując intuicyjny i kontekstowy interfejs użytkownika. IBM i2 Analyst's Notebook pomaga rozpoznawać i przewidywać przestępstwa kryminalne, akty terroru i oszustwa – oraz odpowiednio wcześnie im zapobiega" (http://www-03.ibm.com/software/products/pl/analysts-notebook [dostęp kwiecień 2017 r.]).

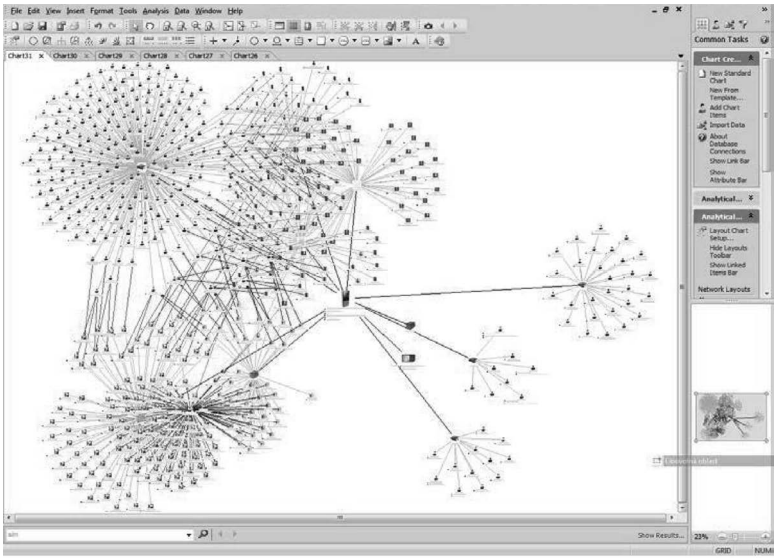
Warto podkreślić, że wykorzystanie tego rozwiązania pozwala m.in. na (http://www-03.ibm.com/software/products/pl/analysts-notebook [dostęp kwiecień 2017 r.]):

- błyskawiczne łączenie odrębnych elementów danych w jeden, spójny obraz sytuacji;
- identyfikację kluczowych osób, zdarzeń, związków i schematów, które bez odpowiednich narzędzi analitycznych mogłyby pozostać niedostrzeżone;
- lepsze zrozumienie struktury, hierarchii i metod działania struktur przestępczych i terrorystycznych;
- uproszczone formy prezentacji złożonych danych, które ułatwiają szybkie i bezbłędne podejmowanie decyzji operacyjnych.

Możliwości analityczne tej rodziny rozwiązań są nie do przecenienia, w szczególności w odniesieniu do analizy powiązań w sieciach społecznościowych. Połączeń, a raczej powiązań, między osobami, grupami, które na pozór nie mają nic ze sobą wspólnego (rysunek 12).

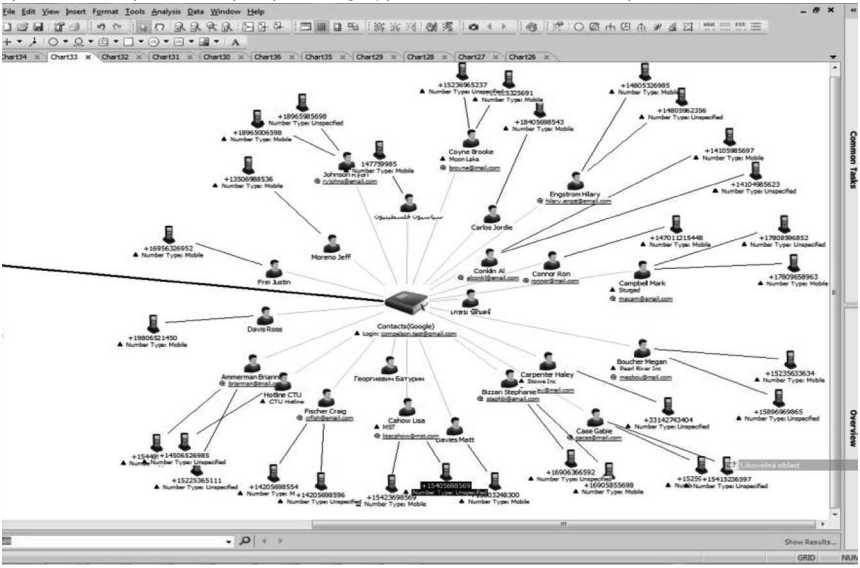
Należy również wspomnieć o innych możliwościach istniejących w środowisku wszechobecnego Internetu – analizy połączeń sieci komórkowych (rysunki 13 i 14), połączeń wykonywanych i odbieranych, a także kontaktów zapisanych w telefonach, jak również całej aktywności zapamiętanej w telefonach typu smartphone.

Rysunek 12. Przykład błyskawicznego łączenia odrębnych elementów danych (np. członków sieci społecznościowych) i ich wizualizacja pozwalająca na dostrzeganie niewidocznych na pozór powiązań



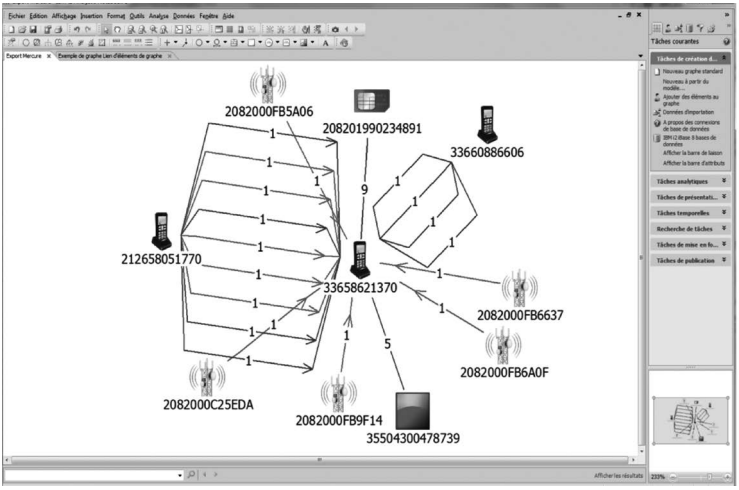
Źródło: materiały firmy IBM dotyczące rozwiązań i2.

Rysunek 13. Przykład analizy aktywności grupy osób w sieciach komórkowych



Źródło: materiały firmy IBM dotyczące rozwiązań i2.

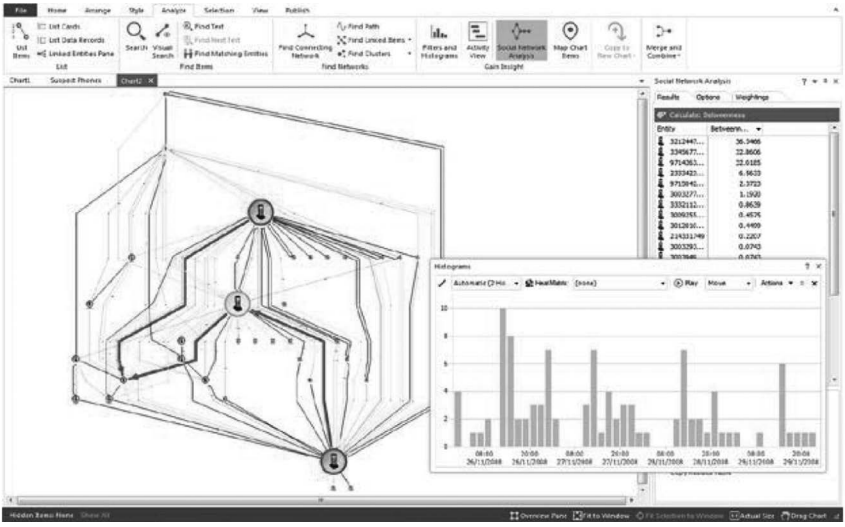
Rysunek 14. Przykład analizy szczegółowej telefonów komórkowych wraz z ich lokalizacją podczas wykonywania wybranych połączeń



Źródło: materiały firmy IBM dotyczące rozwiązań i2.

Dalsza analiza zebranych danych umożliwia dokonanie powiązania czasu i miejsca (rysunki 15 i 16) wybranej grupy osób i ich aktywności.

Rysunek 15. Zaawansowane narzędzia do analizy wizualnej pomagają szybko uzyskać odpowiedzi na pytania „kto, co, kiedy, dlaczego i gdzie"

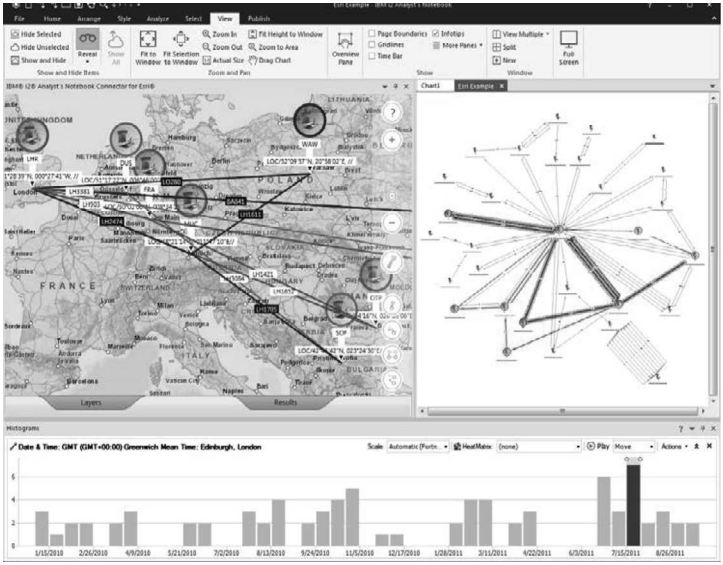


Źródło: materiały firmy IBM dotyczące rozwiązań i2.

Rysunek 16. Możliwa jest analiza i wizualizacja „zwyczajów" badanych osób/grup

Źródło: materiały firmy IBM dotyczące rozwiązań i2.

Rysunek 17. Połączenie z rozwiązaniami GIS (np. firmy ESRI) pozwala na umiejscowienie analizowanych danych zarówno w czasie, jak i miejscu

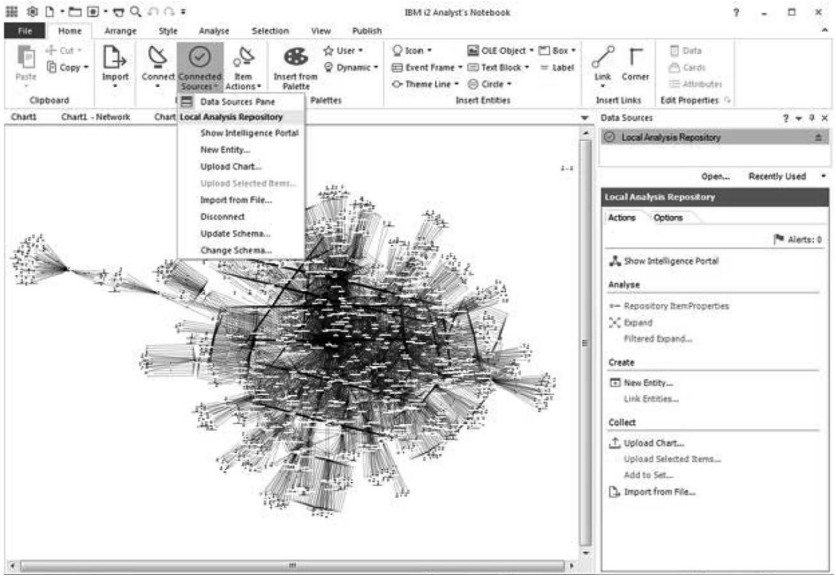


Źródło: materiały firmy IBM dotyczące rozwiązań i2.

Możliwe jest bardzo szybkie i automatyczne zobrazowanie „zwyczajów" analizowanych osób – miejsca ich przebywania, sposobu przemieszczania (rysunek 17), czasu wykonywania połączeń i mnóstwa innych niezbędnych analitykom danych.

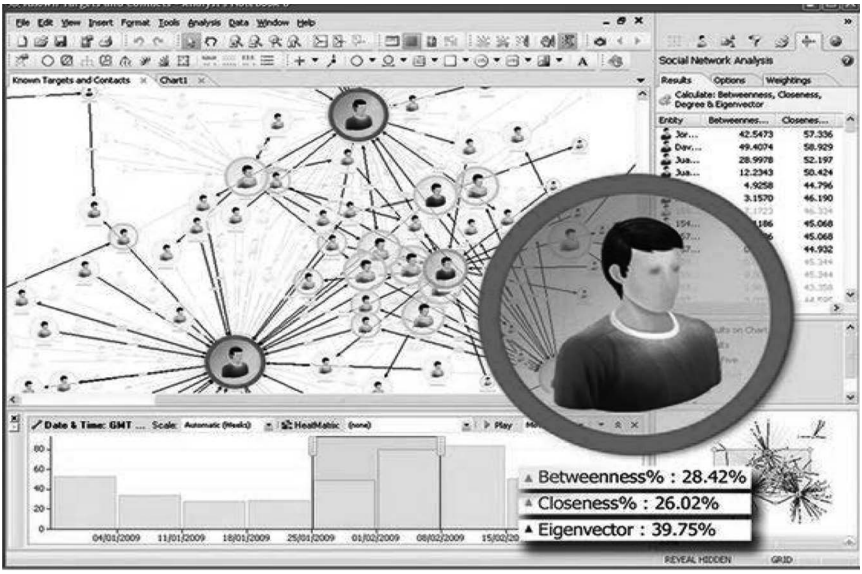
Taka analiza ma na celu wyłonienie z całego gąszczu dostępnych danych, wstępnie niemożliwych w sposób manualny do analizy (rysunek 18) w rozsądnym czasie wyników i uzyskaniu odpowiedzi na zasadnicze pytania: „kto?, co?, kiedy?, dlaczego? i gdzie?". W najlepszym przypadku uzyskujemy wskazanie na konkretną osobę/osoby, będące podejrzanymi w badanej sprawie (rysunek 19).

Rysunek 18. Wstępna sieć powiązań praktycznie niemożliwa do analizy w sposób manualny w rozsądnym czasie bez wykorzystania narzędzi analitycznych



Źródło: materiały firmy IBM dotyczące rozwiązań i2.

Rysunek 19. Możliwe do uzyskania wskazanie na podejrzane osoby dzięki rozwiązaniom IBM i2



Źródło: materiały firmy IBM dotyczące rozwiązań i2.

Autor pragnie podkreślić, że opisane rozwiązania to zaledwie drobny wycinek możliwości rodziny rozwiązań IBM i2, pozwalających na wyodrębnianie z ogromu danych tego, co jest potrzebne czy inaczej – istotne, analizowania ich zarówno przez wzajemne powiązania, jak i przez analizę zawartości (np. dokumentów tekstowych, e-maili itp.). Efekt wykorzystania informatyki w tym przypadku jest taki, że dzięki ich zastosowaniu powstaje możliwość uzyskania możliwości działań proaktywnych, wynikających z szybszego dotarcia do ukrytych powiązań, a przez to do wykorzystania możliwości, jakie niesie ze sobą wiedza na temat sieci bezskalowych. Wykorzystanie tej wiedzy na swoją korzyść i zabezpieczenie możliwych elementów narażonych na atak, zniszczenie, mających znaczący wpływ na nasze działania (huby). Opisane rozwiązania nie są jedynymi dostępnymi na rynku narzędziami analitycznymi, pozwalającymi na działania na ogromnych ilościach danych i zwracaniu wyników analizy w czasie zbliżonym do rzeczywistego nawet w przypadku, gdy do pracy wykorzystywany jest „zwykły" komputer – czy to laptop, czy też komputer stacjonarny.

Postęp w tej dziedzinie jest bardzo szybki i trudny do porównania w innych dziedzinach życia. Podkreślają to w szczególności specjaliści zajmujący się

na co dzień analizą danych z wielu źródeł. Inne dostępne narzędzia pozwalają na podobne działania jak opisane powyżej, jednak w znacznie szerszym zakresie, sięgając swoimi „sensorami" nawet do tzw. DarkNetu, jednak ze względu na ich charakter i wykorzystujące je w swoich działaniach służby specjalne nie zostaną one opisane w szczegółach. Wszystkich zainteresowanych odsyłam do kontaktu z autorem artykułu.

Autor nie wspomniał również o wielu narzędziach pozwalających np. na analizę obrazu wideo, i to w taki sposób, że np. film z monitoringu trwający 24 godziny, po wstępnej analizie może trwać (w zależności od ilości danych na nim zawartych) około kilku minut. Analiza wstępnie przefiltrowanego filmu jest znacznie prostsza i krótsza i pozwala na szybsze wykrycie najistotniejszych informacji. Chodzi o narzędzie firmy Comarch. Szczegóły są dostępne pod adresem: *http://securityplatform.comarch.pl/#zastosowanie*, choć znacznie więcej szczegółów można znaleźć po kontakcie z przedstawicielami producenta.

Podsumowanie

Pierwszym wnioskiem, który można podać z powyższego tekstu, jest to, że sieci bezskalowe są obecnie w naszym otoczeniu w różnych formach, choć być może nie zawsze zdajemy sobie z ich istnienia sprawę. Cyberprzestrzeń, wymagająca do swego istnienia nośnika w postaci sieci, jest doskonałym przykładem, gdzie sieci bezskalowych możemy szukać. Są one bardzo obiecujące i należy prowadzić dalsze badania naukowe z nimi związane. Znajomość ich cech charakterystycznych daje ogromną przewagę i ułatwia zabezpieczenia własnych sieci tego typu. Można bowiem zwielokrotnić uwagę nad zabezpieczaniem hubów, których bezpieczeństwo, jak wykazują badania jest niezmiernie istotne dla ich funkcjonowania, a mniejszą uwagę skupić na węzłach nieznaczących. W rezultacie może to dać znacznie lepsze efekty niż próba zabezpieczania całej sieci w sposób jednolity.

Z drugiej strony znajomość struktury sieci bezskalowej po stronie przeciwnika umożliwia dokonywanie znacznie skuteczniejszych ataków, a więc działań aktywnych na sieci strony przeciwnej, które mogą zakończyć się całkowitym wyeliminowaniem tych sieci. Daje to również możliwość lepszego rozpoznawania przez własne rozpoznanie i kontrolowanie działalności – istniejące narzędzia informatyczne dają możliwość tworzenia schematów badanych sieci, wynajdywania w nich hubów i kontrolowania ich aktywności.

Działania w cyberprzestrzeni w kontekście piątego wymiaru walki stanowią bardzo ważny obszar, w którym Siły Zbrojne RP muszą w najbliższym czasie osiągnąć wysoki poziom zaawansowania. Jest to niezbędne dlatego, że wspomniane przykłady mają duży wpływ na funkcjonowanie państwa jako całości i – jak wskazuje prof. Sienkiewicz – bezpośrednio wpływają na funkcjonowanie wszystkich jego kluczowych elementów. Dodatkowym atutem cyberprzestrzeni jest dość łatwe utrzymanie statusu nierozpoznanego agresora, co jeszcze bardziej uatrakcyjnia wszelkie próby prowadzenia działań bez ujawniania swojej prawdziwej tożsamości, a tym samym prowadzenia działań w sposób bezkarny. Stąd w ocenie autora ten wymiar działań będzie najbardziej wykorzystywanym w najbliższej przyszłości sposobem na wpływanie na atakowane kraje zarówno pod względem gospodarczym, jak i politycznym.

Można również stwierdzić, że opisana teoria sieci bezskalowych jest niezmiernie interesująca i jej dalsza eksploracja może dać ciekawe rezultaty. W efekcie wykorzystania tej teorii dostępne narzędzia informatyczne są również podstawą do szybkiej, dokładnej i bazującej na znaczących zasobach analizy danych pochodzących z Internetu. Dane te mogą być podstawą do wypracowania odpowiednich działań, a przede wszystkim do działań proaktywnych, wyprzedzających działania innych oponentów, niekoniecznie pozytywnie nastawionych do reszty otoczenia. Działania wielu grup terrorystycznych opierają się na m.in. wykorzystywaniu sieci społecznościowych do wymiany informacji i planowaniu swoich działań. Stąd ich aktywne nadzorowanie, możliwe dzięki rozwiązaniom IT, te działania terrorystom znacznie utrudnia, co niewątpliwie należy zaliczyć do zalet wspomnianych rozwiązań informatycznych.

Poruszana tematyka wymaga dalszych badań i zgłębiania możliwości wykorzystania narzędzi informatycznych w środowisku wszechobecnych połączeń internetowych dających duże możliwości jak również stwarzających wielkie zagrożenia.

Bibliografia

Albert R., Jeong H., Barabási A.L., *The Internet's Achilles, heel: error and attack tolerance of complex networks*, "Nature", 27 Jul 2000, 406(6794): 378–382, https://www.nature.com/articles/35019019.

Barabási A.L., *The physics of the Web*, "Physics World – PhysicsWeb", July 2001, https://cs.wellesley.edu/~cs249B/papers/Barabasi-%20The%20physics%20of%20the%20Web%20%28July%202001%29%20-%20Physics%20World%20-%20PhysicsWeb.pdf.

Barabási A.L., Bonabeau E., *Scale-Free Networks*, "Scientific American", May 2003, vol. 288, issue 5, http://icosystem.com/site/wp-content/uploads/SciAm2003.pdf.

Cohen D. (2002). *All the world's a net*, "New Scientist Magazine", vol. 174, issue 2338.

Collins English Dictionary – Complete & Unabridged 2012 Digital Edition © William Collins Sons & Co. Ltd. 1979, 1986 © HarperCollinsPublishers 1998, 2000, 2003, 2005, 2006, 2007, 2009, 2012.

Gibney A. (2016). *Zero Days*, reżyseria: Alex Gibney, gatunek: film dokumentalny czas trwania: 115 min., USA.

Guare J., *Small worlds, Everything is connected*, "New Scientist", December 1999, issue 2215, 4, https://www.newscientist.com/issue/2215/.

https://en.wikipedia.org/wiki/Scale-free_network [dostęp: grudzień 2016].

http://jcs.biologists.org/content/118/21/4947 [dostęp: listopad 2016].

http://www-03.ibm.com/software/products/pl/category/prescriptive-analytics [dostęp: kwiecień 2017].

http://www-03.ibm.com/software/products/pl/analysts-notebook [dostęp kwiecień 2017].

IBM, Materiały promocyjne i2 Analyst.

i-słownik, https://www.i-slownik.pl/323,cyberprzestrzen/ [dostęp: październik 2017].

Jallonen J., *Dni, które wstrząsnęły Estonią*, https://www.eesti.pl/dni-ktore-wstrzasnely-estonia-11963.html [dostęp: październik 2017].

Joint Publication 3-12 (R), *Cyberspace Operations*, "Joint Electronic Library system", 5 February 2013, http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf.

Kasprzyk R. (2008). *Własności sieci złożonych posiadających cechy Small World i Scale Free*, ISI WCY WAT, Biuletyn Instytutu Systemów Informatycznych, s. 125–130.

Kozłowski A., *Prezydent Ilves dla Cyberdefence24: Rosyjski atak na Estonię był samobójczą bramką,* http://www.cyberdefence24.pl/493176,prezydent-ilves-dla-cyberdefence24-rosyjski-atak-na-estonie-byl-samobojcza-bramka [dostęp: październik 2017].

Majkowski W., *Koniec śledztwa w sprawie cyberataku na Estonię*, http://www.politykaglobalna.pl/2012/08/koniec-sledztwa-w-sprawie-cyberataku-na-estonie/ [dostęp: październik 2017].

Narbutt A., *Terroryzm w sieci zagraża wszystkim*, „Rzeczpospolita" z 11.06.2007, https://7dni.wordpress.com/2007/06/14/terroryzm-w-sieci-rosyjska-napasc-na-estonie/.

Pawlak A., *Jak Izrael pokrzyżował atomowe plany Iranu,* „Die Welt" z 7.05.2013, http://www.dw.com/pl/jak-izrael-pokrzy%C5%BCowa%C5%82-atomowe-plany-iranu/a-16796757.

Sienkiewicz P., Świeboda H. (2010). *Analiza systemowa bezpieczeństwa cyberprzestrzeni państwa,* Polskie Stowarzyszenie Zarządzania Wiedzą, seria: Studia i Materiały, nr 33.

Sienkiewicz P. (2013). *Ucieczka od wolności w globalnym społeczeństwie informacyjnym,* Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług, nr 105 Europejska przestrzeń komunikacji elektronicznej. T. 2, s. 759–768.

Titan R., *10 najgroźniejszych cyberataków*, http://wiadomosci.onet.pl/ciekawostki/10-najgrozniejszych-cyberatakow/djx4j [dostęp: październik 2017].

Wielki Słownik Języka Polskiego, (http://www.wsjp.pl/index.php?id_hasla=49602&ind=0&w_szukaj=cyberprzestrze%C5%84 [dostęp: październik 2017].

Tarapata Z. (2012). *Czy sieci rządzą światem? Od Uulera do Barabasiego,* ISI WCY WAT, „Biuletyn Instytutu Systemów Informatycznych" 10, 31–51.

The American Heritage® New Dictionary of Cultural Literacy, Third Edition. Published by Houghton Mifflin Company.

www.cs.virginia.edu/oracle, Kevin Bacon game.