PRZEGLĄD TELEINFORMATYCZNY
NR 1-2, 2018

Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru

Maciej MARCZYK

Instytut Teleinformatyki i Automatyki, Wydział Cybernetyki WAT,
ul. Gen. W. Urbanowicza 2, 00-908 Warszawa
maciej.marczyk@wat.edu.pl

STRESZCZENIE: Cyberprzestrzeń jest przestrzenią komunikacyjną tworzoną przez systemy powiązań internetowych. Pozwala jej użytkownikom na komunikację w sieci i nawiązywanie relacji w czasie rzeczywistym. Cyberprzestrzeń jest także środowiskiem wymiany informacji za pomocą sieci i systemów komputerowych. Autor opisuje w artykule przestrzeń cybernetyczną jako wymiar aktywności człowieka, w której wszelkie działania odbiegają charakterem od środowiska fizycznego. Przedstawia zakres pojęciowy i strukturalny tej przestrzeni, która obok środowiska lądowego, morskiego, powietrznego i kosmicznego stała się nowym wymiarem działań człowieka także tych o charakterze militarnym.

SŁOWA KLUCZOWE: cyberprzestrzeń, sieć teleinformatyczna, zagrożenia

1. Wprowadzenie

Cyberprzestrzeń jest m.in. przestrzenią komunikacyjną tworzoną przez systemy powiązań internetowych. Pozwala jej użytkownikom na komunikację w sieci i nawiązywanie relacji w czasie rzeczywistym. Cyberprzestrzeń jest środowiskiem wymiany informacji za pomocą sieci i systemów komputerowych. Cyberprzestrzeń jest wymiarem aktywności, w której wszelkie działania odbiegają charakterem od środowiska fizycznego. Obok środowiska lądowego, morskiego, powietrznego jak i kosmicznego jest to nowy wymiar, w którym można prowadzić działania, w tym działania o charakterze militarnym. Oczywistym jest, że znacznym stopniu różni się od pozostałych wymiarów, ponieważ:

– Jest dziełem człowieka w odróżnieniu od płaszczyzny lądowej, morskiej, powietrznej czy też kosmicznej;
– Uczestnicy mają pełna kontrolę nad charakterem tego środowiska;
– Nie posiada ona ograniczeń terytorialnych.

Autorzy piszący o tej przestrzeni najczęściej przedstawiają cztery zasadnicze cechy cyberprzestrzeni, a mianowicie jej anonimowość, aterytorialność, systematyczność i globalny zasięg.

Pojęcie anonimowości odnosi się do możliwości zachowania anonimowości użytkowników cyberprzestrzeni. Należy jednak zaznaczyć, że anonimowość nie wynika z samej istoty cyberprzestrzeni, lecz ze słabości konstrukcji Internetu. Pierwotnie sieć Internet została zaprojektowana dla sektora wojskowego, któremu miała służyć do swobodnej i taniej informacji pomiędzy poszczególnymi placówkami i instytucjami. Wówczas nie myślano o potrzebie ochrony danych i sieci czy też identyfikacji użytkowników sieci, lecz o prostej konstrukcji, która nie wymagałaby uwierzytelnienia.

Aterytorialność cyberprzestrzeni sprawia, że wszelka aktywność użytkowników w jej obszarze nie nakłada na nich ram/ograniczeń w postaci chociażby granicy geograficznej czy też politycznej. W rzeczywistości oznacza to, że z każdego miejsca na świecie możliwe jest dokonanie połączenia z globalną siecią.

W praktyce ograniczeniem jest jednak:

– przepustowość łącza;
– możliwość technicznego połączenia się z siecią.

Cyberprzestrzeń została ukształtowana przede wszystkim przez proces integracji podstawowych form przekazu i interpretacji informacji, który pozwolił na stworzenie nowych warunków dla funkcjonowania człowieka. Takie zjawisko nazywane może być pojęciem multimedialności, gdzie w procesie wymiany i przekazywania informacji społeczeństwo nie korzysta już jedynie z wymiany werbalnej, lecz z przekazywania informacji za pomocą zdjęć wysyłanych przez Internet czy też filmów umieszczanych na różnych portalach internetowych. Innym istotnym elementem jest ciągła konwergencja systemów i usług umożliwiających komunikację czy też przesyłanie danych. Obecnie coraz bardziej zauważalne staje się zjawisko integracji technicznej, czyli stworzenie zintegrowanej platformy teleinformatycznej służącej do międzynarodowej komunikacji społecznej.

2. Wybrane naukowe spojrzenia na cyberprzestrzeń

Dotychczasowe rozważania pozwalają na przedstawienie cyberprzestrzeni w różnych ujęciach. Zdaniem autora w zależności od dziedziny nauki definicje

cyberprzestrzeni będą inaczej obrazowane, a przede wszystkim w różnym znaczeniu interpretowane. Inne spojrzenie na cyberprzestrzeń będą przedstawiać nauki techniczne, jeszcze inne nauki społeczne, socjologiczne czy też psychologiczne.

W obszarze nauk społecznych cyberprzestrzeń jest płaszczyzną służącą do komunikacji międzyludzkiej jak również nowym wymiarem rozrywki dla społeczeństwa. Józef Bednarek wyróżnił pięć podstawowych funkcji cyberprzestrzeni, do których zaliczamy [1]:

- Funkcja informacyjna;
- Funkcja ludyczna (rozrywkowa);
- Funkcja stymulująca;
- Funkcja wzorotwórcza;
- Funkcja interpersonalna.

Funkcja informacyjna cyberprzestrzeni określa, iż jest ona przestrzenią ciągłej wymiany informacji. Pozwala ona na błyskawiczne uzyskanie różnorodnych informacji z niemalże każdego aspektu życia człowieka czy też nauk. Istota funkcji ludycznej pozwala zaobserwować, iż cyberprzestrzeń pozwala na zaspokojenie potrzeb człowieka związanych z rozrywką czy oderwaniem się od codziennych zajęć. Możliwe jest to dzięki coraz większemu dostępowi do infrastruktury teleinformatycznej. Funkcja stymulująca wyraża się w inspiracji odbiorców do aktywnego odbioru treści znajdujących się w cyberprzestrzeni. Kolejna funkcja odnosi się do zjawisk tworzenia nowych standardów, ideałów czy też stylów życia, które obserwujemy wraz z rozwojem cywilizacyjnym. Coraz częściej spotykane są próby definiowania pojęcia cyberspołeczności czy też wirtualnej rzeczywistości.

Socjologiczne podejście do cyberprzestrzeni opisuje ją jako przestrzeń, gdzie następuje mieszanie się kultur gromadząc przy tym różne idee oraz informacje z całego świata. Pojęcie cyberprzestrzeni definiowane jest, jako *Nowa Wieża Babel* czy też *Cyber Termopile,* gdzie dochodzi do zacierania się różnic pomiędzy kulturami jak również jest obszarem ciągłych starć i konfliktów [11].

Cybernetyczne podejście do pojęcia cyberprzestrzeni definiuje ją jako przestrzeń otwartej komunikacji, gdzie sprzężenie zwrotne informacji pozwala na regulację systemów, zachodzenie relacji między nimi oraz dynamiczny rozwój i wytyczanie nowych szlaków [6].

Podejście psychologiczne to podejście, gdzie pojęcie cyberprzestrzeni utożsamiane jest z wirtualną rzeczywistością, jako przestrzeń zapośredniczona w kontekście technologii informacyjnej, w której obecne są wirtualne byty, niedostępne dla człowieka w ich cyfrowym, abstrakcyjnym wymierzę,

zobrazowane poprzez interfejs w wymiarze dostrzeganym wszelkimi zmysłami poprzez dźwięk lub też obraz [6].

Powyższe rozważania dotyczące cyberprzestrzeni definiują ją jako zinformatyzowaną przestrzeń wymiany informacji.

Największe znaczenie w procesie wymiany informacji posiada Internet, czyli termin oznaczający ogólnoświatową sieć komputerowa służącą wymianie informacji za pomocą znormalizowanych protokołów komunikacyjnych[1]. Za pomocą tej globalnej sieci użytkownicy z całego świata są w stanie komunikować się między sobą.

Dużego zaznaczenia w tym procesie nabiera infrastruktura teleinformatyczna, czyli zespół środków teleinformatycznych takich jak sieci czy systemy teleinformatyczne. W literaturze przedmiotu wyróżnić można liczne synonimy pojęcia Internet takie jak globalna sieć komputerowa, ekstranet, sieć ogólnoświatowa jak również w języku potocznym spotykane określenie net. Pojęcie Internetu (z ang. Inter-Network) w dosłownym tłumaczeniu to między sieć.

Można wyróżnić cztery zasadnicze elementy, które charakteryzują tą globalną sieć [3]:

- Nieograniczone zasoby informacji i danych dostępne i znajdujące się w Internecie;
- Interaktywność oznacza, iż w czasie rzeczywistym użytkownicy mogą ze sobą komunikować;
- Powszechność definiowana poprzez coraz łatwiejszy dostęp jak również łatwość i coraz większe jej znaczenie w niemal każdym aspekcie życia człowieka;
- Demokracja w myśl, której globalna sieć określana, jest najbardziej demokratycznym medium z możliwością całodobowego dostępu.

Zdaniem autora ważny jest również aspekt ekonomiczny, który definiuje globalną sieć jako jeden z najtańszych środków wieloaspektowych związanych z przetwarzaniem informacji czy źródeł rozrywki w stosunku do kosztów ponoszonych w wyniku dostępu do niego. Istotna jest również cecha powszechności, gdyż obecnie coraz większa część społeczeństwa nie wyobraża sobie życia bez szybkiego dostępu do Internetu.

[1] http://www.oxforddictionaries.com/definition/english/Internet,

3. Wybrane pojęcia w obszarze cyberprzestrzeni

Z pojęciem cyberprzestrzeni wiąże się kilka zasadniczych elementów definiujących ją, jako pewien spójny wymiar. Wśród tych elementów wyróżniamy: *systemy i sieci teleinformatyczne, dane i informację oraz użytkowników.*

System to wyodrębniony zbiór elementów materialnych lub abstrakcyjnych, wzajemnie powiązanych, jako całość z określonego punktu widzenia, mający przy tym takie właściwości, których nie posiadają jego elementy [8]. W dziedzinie technologii informacyjnej system będzie określany zbiorem powiązanych elementów służących do przetwarzania danych przez określone środki informatyczne.

Pojęcie **systemu teleinformatycznego** oznacza zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego [15]. Pojęcie systemu teleinformatycznych wiąże się więc ze zbiorem określonych urządzeń informatycznych, które służą do przetwarzania informacji za pomocą określonego medium transmisyjnego do urządzeń końcowych. Pojęcie medium transmisyjnego oznacza to nośnik używany do transmisji sygnałów w telekomunikacji umożliwiający rozchodzenie się fal akustycznych, elektrycznych, radiowych i świetlnych.

W środowisku cybernetycznym możemy wyróżnić sieci: teleinformatyczne, komputerowe lub telekomunikacyjne.

Analiza aktów prawnych wykazała, że **sieci teleinformatyczne** *to sieci pozwalającej na wysyłanie i odbieranie danych pomiędzy systemami informatycznymi pełniącymi rolę urządzeń końcowych* [16]. Józef Janczak określa natomiast sieć teleinformatyczną jako sieć pozwalającą na odbieranie oraz wysyłanie danych pomiędzy systemami teleinformatycznymi określanymi jako urządzenia końcowe [4]. Literatura przedmiotu pozwala określić sieć teleinformatyczną jako zbiór urządzeń takich jak router, switch czy modem wykorzystywanych do przekazywania informacji wysyłanych ze stacji roboczych [9]. Sieć teleinformatyczna może być więc infrastrukturą służącą do nadawania, transmisji jak i odbiór informacji przedstawionej w postaci cyfrowej[2] Zdaniem autora sieci teleinformatyczne to pewna architektura powiązań organizacyjnych i technicznych wykorzystywanych do połączenia systemów teleinformatycznych. Wykorzystuje ona specjalistyczne elementy

[2]http://epodlaskie.wrotapodlasia.pl/pl/dzialania/konferencja_informacyjna.htm?m=dload&debug=off&id=53.

teleinformatyczne służące do przekazywania informacji pomiędzy poszczególnymi urządzeniami informatycznymi.

Sieci komputerowe w literaturze przedmiotu określane głównie jako sieci informatyczne, to sieci służące do wymiany informacji pomiędzy osobami funkcyjnymi stanowisk dowodzenia wyposażonymi w komputery lub inne urządzenia informatyczne. Sieci komputerowe służą przede wszystkim ułatwieniu komunikacji pomiędzy poszczególnymi jej użytkownikami zarówno w sektorze prywatnym jak i w strukturach zhierarchizowanych. Sieci te pozwalają również w szybki sposób uzyskać dostęp do zasobów danej organizacji jak i globalnych informacji za pośrednictwem Internetu. Sieci komputerowe pozwalają wykonywać pracę zdalnie bez fizycznego kontaktu z danym urządzeniem, jak również pozwalają na udostępnienie zasobów sprzętowych podłączonych w środowisku sieciowym. Przykładem może być dostęp zdalny do urządzeń peryferyjnych takich jak skanery, drukarki sieciowe czy pamięci masowe oraz dyski wirtualne. W sieciach komputerowych wyróżnia się również dwa zasadnicze komponenty takie jak elementy aktywne i elementy pasywne sieci. Do elementów aktywnych zaliczyć można karty sieciowe, wzmacniacze, routery punkty dostępowe jak i koncentratory bądź przełączniki. W elementach pasywnych zaliczamy kanalizację kablowe, pomieszczenia techniczne, maszty transmisyjne itp. Warto zaznaczyć, iż sieci komputerowe mogą ograniczać się do jednego bądź kilku budynków, ale mogą też pokrywać obszary miasta, kraju a nawet kontynentów.

Jednym z podstawowych kryteriów podziału sieci komputerowych jest obszar, stąd wyróżnić możemy[3]:

- Sieci lokalne (LAN) zwane lokalnymi sieciami komputerowymi obejmującymi zazwyczaj małe obszary takie jak dom, biuro czy budynek.
- Sieci miejskie (MAN) jest to sieć miejska obejmująca swoim obszarem zazwyczaj miasto łącza kilka lokalnych sieci komputerowych.
- Sieci rozległe (WAN) obejmujące swym obszarem całe państwa i kontynenty. Przykładem takiej sieci może być Internet.

Kolejnym kryterium jest funkcja, stąd wyróżnić możemy:

- WLAN (ang. Wireless Local Area Networks) czyli bezprzewodowa sieć lokalna działająca na małym obszarze, w której urządzenia połączone są ze sobą przy użyciu komunikacji bezprzewodowej.
- SAN (ang. Storage Area Netowrks) zwane siecią pamięci masowej, która zapewnia systemom informatycznym dostęp do zasobów pamięci masowej. Obecnie używana jedynie w dużych korporacjach ze względu na złożoną strukturą i ogromne koszty implementacji jak i utrzymania.

[3]http://wireless-network-support.blogspot.com/2009/08/what-is-lan-wlan-wan-man-san-can-pan.html,

- CAN (ang. Controller Area Networks) jest to szeregowa magistrala komunikacyjna odporna na zakłócenia elektromagnetyczne dzięki zastosowaniu różnicowej transmisji bitów. Stosowana pośrednio w przemyśle np. w systemach samochodowych, gdzie istotna jest właśnie transmisji danych a niekoniecznie jej szybkość przesyłania. W tym rodzaju sieci maksymalna prędkość przesyłania danych to 1Mb/s w odległości do 40 metrów. Prędkość przesyłania danych spada wraz ze wzrostem odległości.
- PAN (ang. Personal Area Networks) rodzaj sieci komputerowej używanej do transmisji danych poprzez różne urządzenia użytkownika. Obecnie taką sieć można stworzyć za pomocą połączenia komputera, telefonu komórkowego (bądź smartfona), telewizora, tableta czy innych urządzeń użytkownika w jedną sieć wymiany danych.

Sieci telekomunikacyjne według Ustawy *Prawo telekomunikacyjne* to systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju [17]. Jest to zespół urządzeń telekomunikacyjnych znajdujących się na danym obszarze, przeznaczony do świadczenia usług telekomunikacyjnych.

W literaturze przedmiotu pomiędzy sieciami telekomunikacyjnymi i teleinformatycznymi można zaobserwować pewne prawidłowości związane z zależnościami funkcjonalnymi, które pozwalają porównać poszczególne przeznaczenia sieci [4]:

- Zarządzanie transmisją informacji;
- Wykorzystanie systemów teletransmisyjnych;
- Generowanie sygnałów z urządzeń do systemów transmisyjnych za pomocą określonych częstotliwości;
- Synchronizacja pomiędzy odbiornikiem i nadajnikiem;
- Adresowanie pakietów na kierunku odbiorca – nadawca;
- Wykrywanie i korekta błędów danych;
- Odpowiedni dobór drogi przepływu pakietu;
- Retransmisji z powodu błędów sieci i awarii;
- Formatowanie danych zawartych w wiadomości oraz ustalenie formatu wymiany wiadomości pomiędzy poszczególnymi urządzeniami końcowymi (stacjami roboczymi);
- Integracja zarządzania siecią oraz bezpieczeństwa sieci.

Kolejnym przytoczonym przez autora elementem są *dane* i *informacje.* **Dane** to informacje przedstawione w postaci umożliwiającej ich przetwarzanie za pomocą programów komputerowych lub będące wynikiem tego przetwarzania[4]. Dane reprezentują fakty i są przesyłane do świadomości odbiorcy w postaci komunikatu. Danymi można nazwać również pewne zbiory faktów, zjawisk, zdarzeń, cech przedmiotów lub obiektów, które są dostępne w bazach danych lub uzyskuje się je dzięki sensorom [10]. W systemach i sieciach teleinformatycznych wyróżnione zostało również pojęcie *danych osobowych,* czyli wszelkich informacji dotyczących zidentyfikowania lub możliwych do zidentyfikowania osoby fizycznej [18].

W sieciach teleinformatycznych wyróżniamy również dwa zasadnicze typy danych w nich przetwarzanych [18]:

- Dane lokalizacyjne, czyli te dane, które przedstawiają położenie geograficzne danego podmiotu korzystającego z usług telekomunikacyjnych. Przykładem takich danych może być długość i szerokość geograficzna, wysokość nad poziomem można. Dzięki tego typu danym możliwe jest określenie kierunku poruszania się danego obiektu jak również określenie jego dokładnej pozycji czy prędkości z jaką się porusza.
- Dane telekomunikacyjne odnoszące się bezpośrednio do danych usług sieciowych z jakich korzysta użytkownik. Przykładami takich danych może być np. rodzaj sieci źródłowej i końcowej, wykorzystywanym protokole przez użytkownika danej sieci, ilości wysyłanych i odbieranych danych w trakcie połączenia jak również czasie sesji czy wyborze trasy pakietów.

Pojęcie **informacji** natomiast jest niewątpliwie trudniejsze do zdefiniowania, bowiem różne dziedziny nauki definiują to pojęcie w zależności od charakteru czy też sposobu użycia. Jest to także zbyt szeroki obszar na jego opisanie w tym artykule. Najogólniej można przyjąć, że jest to określona treść przedstawiona za pomocą określonego języka lub kodu przez nadawcę do odbiorcy [14]. Połączenie informacji i danych przedstawił Jerzy Kisielnicki pisząc, że informacja to przekazywanie różnorodności, a jej znakową postacią są dane [5].

Pojęcia danych i informacji w języku potocznym często jest używane zamiennie a nieprecyzyjne określanie tych pojęć prowadzi do niewłaściwego zrozumienia samej istoty przekazywania informacji.

[4] http://encyklopedia.pwn.pl/haslo/3890542/dane.html,

4. Wybrane pojęcia zagrożeń cyberprzestrzeni

Najogólniej **zagrożenie** jest interpretowane jako sytuacja lub stan, w którym komuś zagrażają, lub w którym ktoś czuje się zagrożony [2]. W podejściu zarządzania kryzysowego zagrożenie będzie rozumiane poprzez pewne następstwo zdarzenia, które wywiera negatywny wpływ na funkcjonowanie politycznych i gospodarczych struktur państwa czy też na warunki bytowania ludności oraz stan środowiska naturalnego [7] Zagrożenie jest więc pewnym zdarzeniem, które powoduje zmniejszenie poziomu bezpieczeństwa danego podmiotu. Zdaniem autora pojęcie zagrożenie ma charakter interdyscyplinarny i w zależności od interpretowanej nauki pojęcie może nabierać innego znaczenia. Zagrożenie można utożsamiać z pewnym stanem jak i następstwem straty danej cechy czy tez przedmiotu. Zagrożenie wiąże się więc z pewnym stanem, który powoduje powstanie pewnej niebezpiecznej sytuacji dla danego podmiotu bądź otoczenia. Zdaniem autora kluczowe w terminologii jest również określenie, iż zagrożenie cechuje się pewnym prawdopodobieństwem wystąpienia. Mimo, że dane podmiot jest zagrożony to istotne jest określenie szansy wystąpienia danego zjawiska odbierającego poczucie bezpieczeństwa.

Zdaniem autora z pojęciem zagrożenia wiąże się również termin **bezpieczeństwa,** czyli stan, który daje poczucie pewności, i gwarancje jego zachowania oraz szansę na doskonalenie. Pojęcie bezpieczeństwa to jednak, podobnie jak znaczenie informacji, zbyt rozległy temat badawczy, nie mieszczący się w ramach tematyki tego artykułu.

Analiza literatury przedmiotu wykazała jednak, że oprócz pojęcia zagrożeń cyberprzestrzeni spotykane są również definicję cyberzagrożeń, zagrożeń w środowisku cybernetycznym czy też zagrożeń obszaru cyberprzestrzeni [12]. Zagrożenia dość często interpretowane są jako możliwości negatywnego wpływu na działanie podmiotów w cyberprzestrzeni. W przypadku zagrożeń w cyberprzestrzeni odnosząc się do aspektu przetwarzanych informacji można określić, że są nimi zdarzenia losowe bądź działania celowe mogące spowodować przesłanki do legalnego lub nielegalnego ujawnienia informacji, jej modyfikacji, zniszczenia czy ewentualnej kradzieży.

Zdaniem autora w procesie identyfikacji zagrożeń kluczowe jest zdefiniowanie środowiska cybernetycznego. Pojęcie to określane jest jako zespół wszelkich elementów i czynników będących w ścisłej współzależności, który wpływa na procesy informacyjne danego układu poprzez umacnianie stanów pożądanych i przeciwdziałanie owym stanom niepożądanym [13]. Elementami tego środowiska są wszelkie stacje robocze, terminale, koncentratory, serwery jak również w odniesieniu do SZ RP wszelkie radiostacje czy też radiolinie.

Ze względu na ich źródło pochodzenia wyróżnia się zagrożenia wewnętrzne i zagrożenia zewnętrzne.

Zagrożenia wewnętrzne dotyczyć będą wszelkich działań odnoszących się pośrednio lub bezpośrednio do elementów cyberprzestrzeni, na które oddziałuje podmiot wewnętrzny danego otoczenia. Zagrożenia zewnętrzne natomiast to takie zjawiska, które powstają na skutek działalności zewnętrznych podmiotów na dane środowisko. W przypadku zagrożeń wewnętrznych odnoszących się do środowiska sieci i systemów komputerowych będą wszelkie działania zachodzące wewnątrz danego systemu teleinformatycznego. Wśród nich wyróżnić można:

- Nieuprawniony dostęp do zasobów sieci;
- Kradzież informacji i danych przez użytkowników wewnętrznych;
- Niewłaściwe wykorzystanie aplikacji działających w systemie;
- Świadome wykorzystywanie luk systemów i oprogramowania;
- Awarie sprzętowe, łączy, czy też oprogramowania,
- Inne działania związane z wypadkami bądź spowodowane czynnikiem ludzkim.

Nieuprawniony dostęp do zasobów sieci oznacza, iż użytkownik do tego nieupoważniony jest w stanie pozyskiwać informację, do których nie powinien mieć dostępu. Nieautoryzowany dostęp do informacji można uzyskać w trzech obszarach. Pierwszym jest obszar centrali, gdy użytkownik nieuprawniony uzyskuje dostęp w głównych punktach dostępowych takich jak siedziba główna danej firmy czy też organy bądź obiekty zarządzające na szczeblu strategicznym. Przykładem może być siedziba główna banku czy też departament IT zajmujący się zarządzaniem sieciami i systemami teleinformatycznymi. Drugim obszarem jest określone stanowisko robocze, gdzie użytkownik za pomocą danego urządzenia jest w stanie uzyskać dostęp do poufnych informacji. Ostatnim jest obszar jest związany z liniami transmisyjnymi, gdzie napastnik uzyskuje dostęp do danych poprzez włamanie się w procesie ich transmisji. Pojęcie nieuprawnionego dostępu do zasobów sieci można nazywać również hackingiem komputerowym. Hacking komputerowy to pojęcie związane z działalnością użytkownika, który bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenia[5].

Kradzież informacji i danych przez użytkowników wewnętrznych oznacza działalność mającą na celu pozyskiwanie danych a w szczególności danych poufnych. Zdaniem autora kluczowe jest określenie podmiotów realizujących powyższe działania.

[5] http://www.cyberprzestepczosc.info/hacking_komputerowy.html,

Wyróżniamy trzy zasadnicze podmioty pozyskujące informację i dane poufne[6]: Hacker, Cracker i Phreaker.

Pojęcie hackera określa osobę uzyskującą dostęp do nieautoryzowanych informacji. Wśród typów hackerów wyróżnia się Black Hat czyli osoby działające na pograniczu prawa, aby móc włamywać się do systemów i sieci komputerowych bądź omijać zabezpieczenia korzystając z luk w ochronie. Celem jest pozyskiwanie informacji bądź chęć ujawnienia dostępu do owych danych celem pokazania sowich możliwości bądź podniesienia własnej wartości jako osoby posiadającej specjalistyczną wiedzę. Istnieją jeszcze hackerzy zaliczający się do grupy White Hat czyli osób, które z założenia unikają wyrządzenia poważnych szkód. Mają raczej na celu pokazanie danym instytucjom czy firmom luk w ich zabezpieczeniach oraz hakerzy, którzy przyjmują po części metody działania obu wyżej wymienionych grup nazywani Grey Hat.

Cracker to osoba świadomie łamiąca zabezpieczenia, ale w celu uzyskania własnych korzyści. Crackerzy często działając myślą o szkodzie dla danego systemu czy sieci teleinformatycznej bądź świadomej kradzieży informacji poufnych w celach finansowych.

Ostatnią grupą są tzw. Phreakerzy czyli osoby łamiące zabezpieczenia sieci telefonicznych celem uzyskania darmowych połączeń bez konieczności wpinania się w linię abonenta. Jest to jednak grupa, obecnie coraz mniej spotykana, gdyż obecnie usługi telekomunikacyjne są coraz powszechniejsze i coraz tańsze.

Niewłaściwe wykorzystanie aplikacji działających w systemie oznacza, iż użytkownicy mogą nieświadomie wykorzystywać oprogramowanie w ten sposób, że narażają funkcjonowanie całego systemu otwierając drogę do ujawnienia informacji nie tylko swoich, lecz również informacji, które mogą być utajnione. Niewłaściwe korzystanie z aplikacji może prowadzić do[7]:

- Dostępu osób trzecich do informacji prywatnych, firmowych czy innych poufnych danych;
- Ujawnienia haseł do systemów czy innych aplikacji;
- Umożliwić monitorowanie urządzeń poprzez inne aplikacje działające w tle systemów operacyjnych;
- Umożliwić śledzenie położenia danego użytkownika;
- Umożliwić uszkodzenia urządzeń teleinformatycznych;
- Wykorzystania prawdziwej tożsamości użytkownika do innych celów.

[6]http://gadzetomania.pl/11106,haker-cracker-phreaker-czym-roznia-sie-od-siebie-sieciowi-przestepcy,

[7] http://bitdefender.marken.com.pl/2014/clueful,

Świadome wykorzystywanie luk systemów i oprogramowania może prowadzić do innych działań wliczając w to kradzież informacji i ujawnienie informacji poufnych. Problematyka wykorzystywania luk w systemach i oprogramowaniu dotyczy w głównej mierze źle zaprojektowanych kodów aplikacji, porzuconej cyfrowej własności oraz innych błędów popełnianych przez użytkowników/pracowników[8].

Klasyfikacja zagrożeń cyberprzestrzeni w literaturze przedmiotu nie pozwala precyzyjnie określić, tych które stanowią największe zagrożenie dla funkcjonowania i bezpieczeństwa państwa. Możliwe jest jednak określenie tych, które występują najczęściej.

W opinii autora czynnikami, które powodują przeniesienie obecnych działań przestępczych jak również militarnych w sferę cyberprzestrzeni są:

- Niski koszt utrzymania jednostek militarnych (wojsko, sprzęt, amunicja itp.) w stosunku do małych kosztów utrzymania kilku osób mogących sparaliżować duży system, armię czy państwo (jednostki informatyków/hackerów);
- Trudne do udowodnienia przestępcze działanie w cyberprzestrzeni, rzadko udaje się w pełni obarczyć winą określony podmiot;
- Nieadekwatne rodzaje kar i egzekwowanie prawa, mniejsze konsekwencje prawne dotyczą kradzieży informacji, danych jak również środków finansowych przy użyciu cyberataków aniżeli w rzeczywistym realnym świecie;
- Możliwość ataku w cyberprzestrzeni z niemal każdego miejsca na świecie powoduje, iż nie jest potrzebny bliski kontakt w przypadku prowadzenia działań.

Podsumowując cyberprzestrzeń stała się nowym środowiskiem, które pozwala w dużym stopniu rozwijać się patologiom związanym z działaniami, grup przestępczych, terrorystów czy też oszustów. Na społeczności międzynarodowej spoczywa ogromna odpowiedzialność związana z tworzeniem procedur, mechanizmów i standardów poprawiających bezpieczeństwo w globalnej sieci komputerowej.

5. Zakończenie

W ramach przeprowadzonej analizy pojęciowej można stwierdzić, że cyberprzestrzeń jest nową przestrzenią komunikacyjną tworzoną przez systemy powiązań internetowych i potwierdzić założenie wstępne, że pozwala jej

[8] http://www.cisco.com/web/PL/prasa/news/2014/20140807.html,

użytkownikom na łatwiejszą komunikację w sieci i nawiązywanie relacji w czasie rzeczywistym. Jest zatem nowym wymiarem aktywności człowieka, w której wszelkie działania odbiegają charakterem od środowiska fizycznego.

Zdaniem autora działania podejmowane na rzecz ochrony cyberprzestrzeni nigdy nie będą jednak wystarczające, aby jakikolwiek podmiot mógł
w pełni czuć się bezpieczny. Nieograniczona ilość zagrożeń, jakie występują przy zbyt małej ilości rozwiązań wpływających na jej bezpieczeństwo nie napawa optymizmem. Jednak nadchodzące lata mogą w znacznym stopniu ukierunkować działania na korzyść zwykłych użytkowników sieci i bezpiecznej komunikacji między nimi.

Literatura

[1] BEDNAREK J, *Cyberprzestrzeń i roboty humanoidalne nowym wyzwaniem edukacji*, APS, Warszawa 2011.

[2] BRALCZYK J., *Słownik 100 tysięcy potrzebnych słów*, PWN, Warszawa, 2005.

[3] FRĄCZEK M., MARCZYK M., (red.) *Wybrane aspekty bezpieczeństwa cybernetycznego SZ RP*, AON, Warszawa, 2014.

[4] JANCZAK J., *Zarządzanie sieciami teleinformatycznymi opartymi na współczesnych technologiach taktycznych WLąd*, AON, Warszawa, 2011.

[5] KISIELNICKI J., *Rola informatyki w zarządzaniu*, |w|: BOGDANIENKO J., *Organizacja i zarządzania w zarysie*, WNW UW, Warszawa, 2010.

[6] KONIECZNY M., *Poszukiwanie tożsamości w cyberprzestrzeni. Implikacje pedagogiczne*, VULCAN, Wrocław, 2012.

[7] LIDWA, W., KRZESZOWSKI W, *Ochrona infrastruktury krytycznej*, AON, Warszawa, 2012.

[8] MICHNIAK J., *Dowodzenie i łączność,* AON, Warszawa, 2003.

[9] MICHNIAK J., *Teleinformatyka i technika biurowa,* AON, Warszawa, 2009.

[10] PACEK B., HOFFMAN R.*, Działania Sił Zbrojnych w Cyberprzestrzeni,* AON, Warszawa, 2013.

[11] WASILEWSKI J., *Zarys definicyjny cyberprzestrzeni*, ABW, Warszawa, 2013.

[12] WOŁEJSZO J., MARCZYK M., *Identyfikacja i charakterystyka cyberprzestrzeni wykorzystywanej na potrzeby militarne państwa*, AON, Warszawa, 2014.

[13] WOŁEJSZO J., (red) *Automatyzacja dowodzenia SZ RP w środowisku sieciocentrycznym*, Centrum Techniki Morskiej, Ośrodek Badawczo-Rozwojowy, Gdynia-Warszawa, 2013.

[14] WRZOSEK M., *Procesy informacyjne w zarządzaniu organizacją zhierarchizowaną*, AON, Warszawa, 2010

[15] Ustawa z dnia 18 lipca 2002 roku o *świadczeniu usług drogą elektroniczną*, art.2, ust. 3.

[16] Ustawa z dnia 15 kwietnia 2005 roku *o zmianie ustawy o ochronie informacji niejawnych* oraz niektórych innych ustaw.

[17] Ustawa z dnia 16 lipca 2004 roku *Prawo telekomunikacyjne,* art.2. ust.35.

[18] Ustawa z dnia 29 sierpnia 1997r. *o ochronie danych osobowych*, art. 6, ust. 1.

Cyberspace as a new dimension of human activity – conceptual analysis of the area

ABSTRACT: Cyberspace is a communication space created by Internet connections systems. It allows its users to communicate on the network and establish relationships in real time. Cyberspace is also an information exchange environment using networks and computer systems. In the paper, the author describes the cybernetic space as the dimension of human activity in which all activities diverge in character from the physical environment. It presents the conceptual and structural scope of this space, which, apart from the land, sea, air and space environment, has become a new dimension of human activities, including those of a military nature.

KEYWORDS: cyberspace, ICT network, threats

Praca wpłynęła do redakcji: 16.02.2018 r.