7

TECHNOLOGIA INFORMACYJNA W OBSZARZE CYBERBEZPIECZEŃSTWA PAŃSTWA I SPOŁECZEŃSTWA

7.1 WSTĘP

Ogromny potencjał Internetu doprowadził do zmiany znaczenia granic geograficznych przez co odległość geograficzna przestała odgrywać taką rolę jak w poprzednich dekadach. Posiadanie komputera oraz dostęp do Internetu umożliwił sprawniejsze prowadzenie większości działań administracyjnych, politycznych i biznesowych bez wymogu obecności w miejscu pracy. Każda osoba z komputerem osobistym może stać się nadawcą treści. Współcześnie nie jest niczym nadzwyczajnym zjawisko pobierania, przesyłania i zapisywania wiadomości przy pomocy jednego ruchu myszy komputerowej czy kliknięcia klawisza.

Dyskusja na temat cyberprzestępczości podkreśla szereg sprzeczności i problemów, wynikających ze złożoności zjawiska jakim jest dynamiczny rozwój technologii. Dalsza szybka ewolucja kluczowych technologii w kierunku coraz większej konwergencji mediów nadawczych, mediów komunikacyjnych i elektroniki domowej tworzy wiele spornych kwestii. Ponieważ technologia stwarza nowe możliwości rozwoju społecznego, stwarza również i nowe wyzwania.

Naruszenie bezpieczeństwa w cyberprzestrzeni jest wstępem do rozważań na temat znaczenia technologii. Trzeba jednak podkreślić, że Internet umożliwia jego użytkownikom popełnianie przestępstw, które wcześniej byłyby poza ich możliwościami. Cyberprzestrzeń stała się zaawansowanym środkiem komunikacji, który powiela także szkodliwe wzorce ludzkich zachowań.

W niniejszym artykule analizowane są wymagania stawiane przed społeczeństwem, które są potrzebne, aby zachować poczucie cyberbezpieczeństwa. Celem artykułu jest analiza funkcjonowania instytucji publicznych w zakresie polityki cyberbezpieczeństwa. Drugim ważnym celem w pracy jest zdefiniowanie potrzebnych kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni w różnych instytucjach publicznych.

Główną tezą pracy jest stwierdzenie, że obok nauk technicznych również nauki społeczne mogą stanowić pomoc przy rozwiązywaniu problemów związanych

z technologią informacyjno-komunikacyjną i jej zastosowaniem. Cyberbezpieczeństwo jest zagadnieniem przekrojowym dotyczy szerokiego zakresu stosowania technologii i odbywających się przy jej pomocy procesów społecznych, ponieważ sieć internetowa, komputery, programy, dane i aplikacje są narzędziem regulującym codzienne ludzkie czynności. Warto zatem zastanowić się, który z powyższych obszarów wiedzy determinuje i wymusza określony sposób funkcjonowania. Być może nie ma rozstrzygającej odpowiedzi, bowiem oba obszary funkcjonują ze sobą w symbiozie.

Artykuł wskazuje na otocznie społeczno-polityczne, które jest obecne i towarzyszy procesom technologicznym oraz determinuje ich funkcjonowanie. Na marginesie tych rozważań warto wskazać, że artykuł porusza również dylemat funkcjonowania względem siebie dwóch obszarów tj. technologii i społeczeństwa.

Praca przedstawia także sposób, w jaki autor ma nadzieję, na zwiększenie poziom zaufania między rządem a sektorem prywatnym w kwestiach związanych z cyberbezpieczeństwem. W tym miejscu przedstawiane są także rekomendacje dotyczące stosowania proponowanych rozwiązań, które mają wspierać i wzmacniać współpracę międzysektorową.

7.2 SPOŁECZEŃSTWO INFORMACYJNE

Rewolucja w technologii informatycznej, która rozpoczęła się w latach dziewięćdziesiątych, przekształciła społeczeństwa wielu państw w grupę, którą przyjęło się nazywać społeczeństwem informacyjnym [3, 22]. Ustawiczne przetwarzanie i wykorzystywanie danych, wynika z potrzeb obywateli i środowiska w którym funkcjonują. Jest to jedna z głównych cech współczesnego społeczeństwa.

Obywatele, organizacje publiczne oraz prywatne są w coraz większym stopniu uzależnione od technologii i sieciowych systemów. Instytucje działające w sektorze państwowym bądź prywatnym podczas swojego funkcjonowania (obejmującego m.in. korzystanie z usług sieciowych) posiadają swoje wewnętrzne regulaminy oraz zapisy określające stosowne postępowanie. Te – czasem także – rygorystyczne procedury pozwalają na poczucie bezpieczeństwa, choć oczywiście nie dają pełnej gwarancji na uniknięcie problemów. Zupełnie inaczej sytuacja wygląda w kontekście codziennej egzystencji społeczeństwa informacyjnego, które znacznie bardziej podatne jest na zagrożenia.

Bezpieczeństwo informacji i prywatność w Internecie są krytycznym obszarem funkcjonowania grup społecznych. Wiele tematów badawczych kładzie nacisk na podejście socjotechniczne, aby lepiej zbadać rolę technologii informacyjnej w ważnych kwestiach dotyczących prywatności i informacji online. Bez wystarczającej wiedzy na temat zagrożeń w świecie cybernetycznym decyzje dotyczące zachowania i niewidocznych zagrożeń mogą mieć negatywny wpływ na bezpieczeństwo infrastruktury krytycznej i mogą powodować fizyczne szkody w rzeczywistym świecie.

W erze informacyjnej kluczowe stają się systemy informacyjne, które powiązane są z ogółem społeczeństwa, a zwłaszcza z różnymi grupami użytkowników. A zatem istnieje wzajemne powiązanie między technologią a otoczeniem społecznym użytkownika. Warto jednak na marginesie zauważyć, że pozyskiwanie i przetwarzanie danych nie jest zjawiskiem nowym i wywodzi się z obszaru bezpieczeństwa państwa, a szczególnie z jego działań odbywających się w ukryciu. Tak jak w przypadku operacji wywiadowczych, które wyprzedzają często działania wojenne, tak i na poziomie polityki i biznesu informacje stały się kluczowymi elementami w społeczeństwie i mogą być wykorzystywane w bardziej wydajny sposób dzięki technologii informacyjnej [5, 17].

Innowacja jaka zaistniała dzięki technologii cyfrowej była najważniejszą rewolucją w ubiegłym stuleciu. Jej wpływ na społeczeństwo jest wyjątkowym zjawiskiem. Jednak wpływ cyberprzestrzeni na ludzi dopiero zaczyna być rozumiany. Współcześnie osoby prywatne są bardziej niż kiedykolwiek dostępne oraz bardziej możliwe do poznania za pomocą Internetu. Wytworzyła się także nowa kultura silnie związana z cyberprzestrzenią. Zmianie ulegają stosunki społeczne, styl życia, a także i sposób pracy, który nie jest już tak zdeterminowany określonym miejscem. Ponieważ dostęp do Internetu staje się coraz szerzej dostępny można zauważyć, że główne podziały społeczne – dotychczas oparte na nierównościach ekonomicznych – obecnie opierają się na dystrybucji co do dostępu do informacji [20].

7.3 CYBERBEZPIECZEŃSTWO

Wraz ze wzrostem świadomości społecznej na temat ryzyka oraz zagrożeń w cyberprzestrzeni, równolegle może wzrastać poziom umiejętności cyberprzestępców, który pozwala pokonać bariery chroniące systemy informatyczne będące w posiadaniu indywidualnych osób bądź organizacji. Niewystarczające bezpieczeństwo stanowi poważną przeszkodę w wprowadzaniu nowych technologii informacyjnych dla wielu podmiotów [4].

Cyberbezpieczeństwo definiuje się najczęściej w kontekście zapobiegania uszkodzeniom, ochronie oraz w perspektywie przywracania zdolności do poprawnego funkcjonowania komputerów, systemów łączności elektronicznej czy też usług komunikacji odbywających się w cyberprzestrzeni. Drugim elementem definicyjnym jest ochrona informacji zawartych w przestrzeni komunikacji elektronicznej, w celu zapewnienia poufności z jednoczesnym uwierzytelnieniem osób do tego upoważnionych [1].

Cyberbezpieczeństwo odnosi się często do trzech odrębnych, ale powiązanych ze sobą poziomów: pierwszym z nich jest ochrona komputerów, nośników pamięci oraz informacji na nich zawartych; drugim jest umiejętność ochrony przed atakami leżąca po stronie zarówno wewnętrznych regulacji odnoszących się do pracy personelu jak i zabezpieczeń cybernetycznych; trzeci odnosi się do procesu edukacji czy też ustawicznych szkoleń, które będą udoskonalać umiejętności, poszerzać

wiedzę użytkowników oraz korespondować z dynamicznie zmieniającymi się zagrożeniami [6].

Celem cyberbezpieczeństwa jest ochrona cyberprzestrzeni oraz jej cennych zasobów. Bezpieczeństwo w sieci obejmuje działania związane z komputerami, systemami komunikacji elektronicznej oraz usługami wykonywanymi za ich pomocą, a także z łącznością elektroniczną i bezpieczeństwem informacji. Reasumując cyberbezpieczeństwo obejmuje ochronę sieci komputerowych, reagowanie na ataki, koordynowanie gotowości do ataków, monitorowanie sieci, wykrywanie i zapobieganie możliwym atakom cybernetycznym.

7.4 INTERDYSCYPLINARNOŚĆ CYBERBEZPIECZEŃSTWA

Cyberprzestrzeń kształtuje obecnie ogromną liczbę dziedzin życia i tematów badawczych. Wiele dyscyplin naukowych zajmuje się tematami związanymi z bezpieczeństwem internetowym. Analizy badawcze w zakresie informatyki, systemów informacyjnych, przetwarzania informacji, czy technologii informacyjno-komunikacyjnych już od dłuższego czasu badane są w perspektywie cyberbezpieczeństwa. W wielu badaniach temat cyberprzestrzeni sprowadzony jest do systemów zabezpieczeń, bezpieczeństwa danych i ich użyteczności, bezpieczeństwa sieci, kryptografii, bezpieczeństwa oprogramowania jak i bezpieczeństwo platform mobilnych.

Wdrażanie projektów mających poprawić stan bezpieczeństwa łączy w sobie często tematy z odmiennych dyscyplin naukowych. Dlatego Internet stanowi wyzwanie nie tylko dla badaczy z obszaru nauki technicznych, ale i również dla badaczy z zakresu politologii, socjologii, kryminologii, którzy próbują zrozumieć odmienny i często rozbieżny zakres zachowań od powszechnie uznanych i obowiązujących norm społecznych. Całościowe podejście do problemu cyberbezpieczeństwa umożliwia badanie środowiska cybernetycznego w sposób zorientowany na multidyscyplinarność. Stosowanie badań przy pomocy odmiennych dyscyplin naukowych może przyczynić się także do lepszego opisu określonych parametrów ludzkiego działania w środowisku cyfrowym.

W zakresie cyberbezpieczeństwa pomocne okazują się techniki badań społecznych, które wskazują na umiejscowienie oraz rolę jaką spełniają narzędzia technologiczne w ludzkim otoczeniu. Innymi słowy czynnik społeczny stanowi pomoc przy zrozumieniu m.in. motywacji, która towarzyszy podczas korzystania z nowoczesnych technologii. Część badań wskazuje także – poza analizą ryzyka, czy też opisem odmiennych poziomów bezpieczeństwa w administracji publicznej – na potrzebę uwzględnienia również perspektywy legislacyjnej.

Jak już wskazano cyberbezpieczeństwo obejmuje wiele dziedzin życia i tematów badawczych. Obecnie także wiele dyscyplin naukowych wkracza w zakres tematyczny związany z bezpieczeństwem internetowym jak np. socjologia Internetu czy też polityka bezpieczeństwa. Obszarem zainteresowań technologii informacyjnej w aspekcie społecznym jak i politycznym jest przede wszystkim tożsamość

kulturowa i interakcje międzyludzkie oraz środowisko polityczne, które coraz bardziej przenosi swoją działalność w sferę cyberprzestrzeni.

Innowacja technologiczna doprowadziła do sytuacji, w której rzeczywistość jest znacznie bardziej złożona niż miało to miejsce w przeszłości. Współczesne realia często wykraczają poza możliwości definicyjne, językowe czy też możliwości pomiarowe. Wymagają także refleksji na temat stosowania nowych narzędzi metodologicznych, na których ze swej natury opiera się nauka. Przeszkodą w analizie badawczej nad cyberprzestępczością, jest brak statystyk, sprawozdań oraz badań, które mają na celu oszacowanie zakresu cyberprzestępczości, a zwłaszcza nadużyć i przestępczości w sieci.

7.5 ZNACZENIE EDUKACJI DLA CYBERBEZPIECZEŃSTWA

Coraz szersze zastosowanie technologii informacyjnych i komunikacyjnych we wszystkich dziedzinach życia wymaga od społeczeństwa wciąż nowych umiejętności w zakresie cyberbezpieczeństwa. Dynamicznie zachodząca transformacja społeczeństwa informacyjnego stwarza także stały popyt na technologie wykorzystujące multidyscyplinarne dane. Prowadzenie badań i rozwoju oraz edukacja na temat cyberprzestrzeni zwiększa wiedzę społeczną a wraz z nią bezpieczeństwo państwa. Można przypuszczać, że wraz ze znaczeniem polityki bezpieczeństwa będzie wzrastać poziom nakładów na edukację, zatrudnienie i rozwój produktów w zakresie cyberprzestrzeni. Rozwój technologii i innowacji sprzyja wzrostowi gospodarczemu i obronności narodowej. Współpraca badawcza między tymi sektorami wzmacnia zatem bezpieczeństwo państwa.

W miarę im mocniej świat staje się uzależniony od cybertechnologii, tym bardziej potrzebni stają się pracownicy w zakresie bezpieczeństwa w sieci, aby chronić m.in. krajową infrastrukturę krytyczną, która w większości już przypadków funkcjonuje w oparciu o systemy komputerowe. Strategie i plany w zakresie bezpieczeństwa w cyberprzestrzeni wymagają ustawicznego podnoszenia poziomu wiedzy obywateli, a także i pracowników podmiotów działających w zakresie gospodarki i administracji publicznej.

Kompetencje w zakresie cyberbezpieczeństwa to nie tylko wiedza techniczna, ale i umiejętności obywatelskie, dlatego też ważna jest obecność problematyki cyberbezpieczeństwa na różnych poziomach edukacji. Szkoła zatem musi zapewnić młodym ludziom wystarczającą znajomość cyberprzestrzeni, zrozumienie jej zagrożeń oraz możliwość odpowiedniej profilaktyki oraz ochrony nie tylko w aspekcie technologicznym ale i społecznym [10]. Innymi słowy edukacja może obejmować takie kształcenie i szkolenie w zakresie bezpieczeństwa w sieci, które zapewnia podstawowe umiejętności oraz kwalifikacje potrzebne do zagwarantowania podstawowego poziomu cyberbezpieczeństwa.

Oczywistym celem edukacji jest zapewnienie szerokiego spektrum wykształcenia dla przyszłych ekspertów funkcjonujących w różnych dziedzinach społeczeństwa, których umiejętności know-how spełniają jednocześnie oczekiwania

z zakresu innowacji jak i bezpieczeństwa. Drugim również ważnym zadaniem edukacyjnym jest zapewnienie praktycznej edukacji w zakresie cyberprzestrzeni, odpowiadającej potrzebom współczesnej rzeczywistości.

W tym przypadku punktem wyjścia może być Europejska Agenda Cyfrowa, która w swym dokumencie na lata 2011-2020 wskazuje, że umiejętności informatyczne, umiejętności komunikacyjne, znajomość oraz wykorzystanie mediów społecznościowych stanowi podstawową umiejętność w procesie korzystania z usług cyfrowych. Dlatego też – jak należy sądzić – powyższe umiejętności mogą być zaliczone w zakres integralnej części kształcenia w szkołach, jak również w podstawowych oraz uzupełniających szkoleniach nauczycieli [4].

Oczywistym warunkiem skutecznej edukacji jest zwiększenie wiedzy z dziedziny informatyki, tak aby bezpieczeństwo w sieci zajmowało jedno z bardziej znaczące miejsc w systemie nauczania. Niezbędne jest więc zrozumienie tego, co każdy obywatel potrzebuje wiedzieć o bezpieczeństwie internetowym. Większość uczelni w Polsce – szczególnie politechniki oraz uniwersytety posiadające kierunek bezpieczeństwo narodowe – podkreśla znaczenie badań nad cyberbezpieczeństwem z jednoczesną edukacją. Obecnie szkoły wyższe zapewniają naukę w zakresie cyberprzestrzeni wyłącznie ze swojej perspektywy bez jasnej wizji kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni.

Edukacja w sferze publicznej może pozytywnie kształtować obecność w cyberprzestrzeni, poprzez wskazywanie na dobry bądź zły model zachowania. Jednak sprawozdawczość medialna o cyberprzestępczości może być nadmiernie eksponowana. Jedna dramatyczna historia może kształtować opinię publiczną i wzbudzić niepokój publiczny, często powodując zapotrzebowanie na natychmiastowe oraz doraźne rozwiązania w sytuacjach niezwykle złożonych. Pojawiają się w takich sytuacjach postawy mówiące o tym, że jedynym możliwym sposobem zwalczania cyberprzestępczości jest użycie twardego prawa i surowych środków zaradczych. Konsekwencją takiej postawy jest zaostrzenie sporu dotyczącego granic bezpieczeństwa kosztem takich wartości jak wolność [8].

Poziom wiedzy ma wpływ na zachowanie pracowników instytucji publicznych w dziedzinie bezpieczeństwa komputerów i informacji. Skuteczny rozwój wiedzy dotyczącej bezpieczeństwa cybernetycznego wymaga określenia obszarów kompetencji pracowników w powiązaniu z miejscem pracy, tak aby każdy zakres obowiązków miał zapewniony wystarczający zakres wiedzy. Drugim istotnym elementem jest także zachowanie użytkowników Internetu w zakresie ochrony prywatności. Dlatego ważną rolę odgrywa edukacja, która pozwala zrozumieć zagrożenia płynące z cyberprzestrzeni. Internet stał się krytycznym obszarem informacji, jednakże brakuje wykwalifikowanej kadry, co jest czynnikiem, który przyczynia się w znacznym stopniu do słabości bezpieczeństwa instytucji publicznych oraz społeczeństwa wobec różnych zagrożeń cybernetycznych.

7.6 CYBERATAKI

Obecne wyzwania bezpieczeństwa wynikają przede wszystkim z różnych zagrożeń związanych z cyberprzestrzenią. Cel ataku może być niedrogi, osiągalny z dowolnego miejsca na świecie, a serwery poleceń, które wykonują operację, mogą być umieszczone w dowolnym kraju, ukrywając w ten sposób rzeczywistego sprawcę ataku.

Cyberataki przeciwko instytucjom publicznym jak i obywatelom określonych państw są coraz częściej spotykanym zjawiskiem. Obecnie nie ma potrzeby posiadania już tysięcy samolotów i oddziałów żołnierzy, aby zniszczyć lub sparaliżować ważne instytucje rządowe. Można to zrobić przy wykorzystaniu stosunkowo niewielkiej grupy osób posiadających wiedzę oraz połączone ze sobą komputery w sieć, która może być wykorzystana do wywołania awarii niemal każdego systemu komputerowego na świecie [15].

Globalny świat cybernetyczny łączy państwa, przedsiębiorstwa i obywateli w zupełnie nowy sposób. Połączenia internetowe są zespolonym ze sobą systemem instytucji, który reguluje ich codzienne funkcjonowanie począwszy od kontroli ruchu lotniczego po oczyszczalnie ścieków. Ze względu na łatwość ataku cybernetycznego, trudno jest przewidzieć oraz powstrzymać tego typu zdarzenie, ponieważ nawet najlepsze systemy bezpieczeństwa na świecie nie zapewniają pełnej gwarancji bezpieczeństwa, zwłaszcza że stają się na co dzień celem wielu cyberataków. Takich prób oraz możliwości, które stwarzają realne zagrożenie są tysiące. O skali zagrożenia świadczy fakt, że Interpol oszacował, iż istnieje aż 30000 stron internetowych z oprogramowaniem hakerskim, które może pobrać każdy użytkownik Internetu na swój komputer [14].

7.7 WYBRANE CYBERATAKI W PRZESTRZENI POLITYCZNEJ

Rosnąca komunikacja w Internecie może stanowić zagrożenie dla państwa jak i społeczeństwa w wyniku możliwości zaistnienia różnych problemów związanych z prywatnością i bezpieczeństwem informacji [9]. Wraz z pojawieniem się Internetu jako podstawowej infrastruktury komunikacyjnej społeczeństwa obawy o bezpieczeństwo w cyberprzestrzeni dramatycznie wzrosły. Sfera cybernetyczna to nowe pole bitwy, a luki w zabezpieczeniach tworzą wymierne zagrożenie dla bezpieczeństwa narodowego. Z tego m. in. powodu cyberprzestrzeń jest narażona na ataki hakerów i terrorystów.

O konsekwencjach cyberataków świadczy fakt, że w przypadku zaistnienia takiego zdarzenia może dojść do zakłócenia funkcjonowania sieci elektrycznej w państwie, czy też może mieć ono negatywny wpływ na stabilność systemów finansowych. Dlatego też często stosowanym określeniem takiej sytuacji jest „cybernetyczny Pearl Harbor" [21].

Technologia zapewnia wiele punktów, które są szansą dla napastników w celu wykrycia luk w zabezpieczeniach. Stąd pewnie druga metafora, która ma odniesienia do rywalizacji militarnej. Otóż cyberbezpieczeństwo na wiele sposobów stanowi

wyścig zbrojeń między napastnikami i obrońcami. Zwiększony postęp technologiczny powoduje, że współcześnie cyberprzestrzeń stała się elementem taktyki wojennej.

Na poziom świadomości po stronie decydentów politycznych jak i społeczeństwa miało wpływ szereg wydarzeń. Ilustracją wykorzystania cyber technologii w konflikcie zbrojnym są napięcia między Gruzją i Rosją, które wybuchły w 2008 roku. Nastąpiły w tym czasie cyberataki przeciwko gruzińskim serwisom rządowym, których celem było utrudnienie rządowi skutecznego komunikowania się z obywatelami w sprawie konfliktu [7]. Istnieje również wiele dowodów na to, że nowy rząd Ukrainy jest celem cyberprzestrzeni, który może być związany z konfliktem jaki ma miejsce między Ukrainą a Rosją [13, 18].

Innym przykładem wykorzystania cybertechnologii w zakresie polityki bezpieczeństwa jest program o nazwie Stuxnet, który w 2010 roku zniszczył kilka atomowych wirówek w Iranie. Wirus został rzekomo stworzony przez Izraelskich oraz amerykańskich ekspertów [2].

O znaczeniu informacji, szczególnie tych będących w posiadaniu rządu bądź działających na jego zlecenie służb, wiele mówią wydarzenia z czerwca 2013 roku, które dotyczą ujawnienia tajnych dokumentów przez Edwarda Snowdena. Ujawnienie informacji na temat prowadzenia nadzoru służb amerykańskich nad prywatnymi informacjami przesyłanymi i przechowywanymi za pomocą cyberprzestrzeni, a podjętych w imię zapewnienia bezpieczeństwa narodowego, wywołało niezadowolenie opinii międzynarodowej. Skandal był tym większy, że podsłuch nie dotyczył tylko prywatnych wiadomości zwykłych obywateli USA, ale również czołowych polityków z innych państw.

Pod koniec 2014 roku koreański cyberatak na firmę Sony Pictures spowodował zniszczenie danych i wyłączenie tysięcy komputerów oraz ujawnił informacje osobiste pracowników firmy Sony. Warto podkreślić, że przemysł high-tech utrzymuje miliony miejsc pracy. A zatem tego typu ataki stanowią zagrożenie dla bezpieczeństwa gospodarczego państwa.

Powyższe wydarzenia nie są jednoznacznie negatywne, pomimo ich możliwego rozmiaru konsekwencji oraz udowodnienia możliwości jakie dają narzędzia cybernetyczne. Okazuje się bowiem, że te przypadki unaoczniły zagrożenia, ale i zmusiły rządy wielu państw do podjęcia określonych działań zapobiegawczych. Konflikt cybernetyczny staje się coraz bardziej realnym zagrożeniem dla bezpieczeństwa narodowego, decydenci polityczni powinni rozważyć także, jak promować najlepsze badania na rzecz bezpieczeństwa cybernetycznego na szczeblu rządowym.

7.8 CYBERPRZESTĘPCZOŚĆ

Cyberprzestrzeń jest wirtualnym środowiskiem, w którym wartość ekonomiczna w dużej mierze uzależniona jest od czynników intelektualnych, niż od aspektów fizycznych. Innymi słowy, wraz ze wzrostem możliwości biznesowych

i społecznych pojawiają się zupełnie nowe sytuacje kryminalne. Cyberprzestrzeń zmienia rozumienie własności i kontroli, rozmywa także tradycyjne granice między działalnością przestępczą a cywilną. W związku z tym pojawia się wiele istotnych pytań co do tego, jaka jest dokładnie definicja cyberprzestępczości i w jakim stopniu to zjawisko różni się od innych działań, które obecnie uznawane są za przestępstwa.

Cyberprzestępczość to termin, który związany jest z niewłaściwym wykorzystaniem komputerów. Warto jednak zauważyć, że cyberprzestępczość to przestępstwa, które są wykonywane przy pomocy komputerów w sieci lub są jedynie związane z komputerami, ale istotne znaczenie w definiowaniu tego pojęcia odgrywa również otoczenie fizyczne. Jak bowiem potraktować przypadek, w którym dokonane jest nielegalne pozyskanie hasła do konta, a w jego następstwie prowadzone są działania, których skutkiem będzie awaria systemu w cyberprzestrzeni? Okazuje się zatem, że procedury, zabezpieczenia, weryfikacje itp. mechanizmy są równie ważne w przestrzeni cybernetycznej jak i przestrzeni fizycznej [20].

Aby móc lepiej zrozumieć, w jaki sposób Internet stał się narzędziem aktywności przestępczej, ważne jest, aby najpierw scharakteryzować wpływ transformacji technologicznej. Globalizacja poszerzyła zasięg i możliwości przestępców poza tradycyjne granice.

Internet stał się kanałem dla działalności przestępczej, który tworzy nowe możliwości do stosowania przemocy. Niestety, te same cechy generują także wiele informacji, których celem jest m.in. manipulacja i tworzenie fałszywej rzeczywistości, i których nie da się łatwo uchwycić, aby uzyskać spójną definicję szkodliwego zachowania, czy też zidentyfikować nowe formy ryzyka.

Wiele publicystycznych źródeł informuje o coraz częstszym występowaniu cyberprzestępczości. To z kolei zjawisko prowokuje do postawienia pytania, czy cyberprzestrzeń prowadzi do zwiększenia liczby przestępstw czy też w swej rzeczywistości tworzy nowe – niespotykane do tej pory – zagrożenia? Wpływ Internetu na przestępczość jest dosyć szeroki, a zatem wymaga wyjaśnień.

Cyberprzestrzeń przyniosła technologiczne korzyści tradycyjnym przestępstwom, w tym produkcja i dystrybucja pornografii dziecięcej, handel bronią i narkotykami, oszustwa finansowe, naruszenia własności intelektualnej oraz inne przestępstwa, z których wszystkie mają znaczne konsekwencje ludzkie i ekonomiczne [19].

Cyberprzestrzeń być może stanowi okazję do ich zaistnienia w nowym wymiarze i w dużym stopniu ułatwia dokonywanie przestępstw. Idąc dalej tym tropem, można zastanowić się czy cyberprzestępczość jest kategorią przestępczości potrzebującą nowej teorii czy też lepiej zrozumieć to zjawisko przy pomocy nowych technologii? [20].

Istnieją dwa istotne cyberzagrożenia, które związane są z publikowaną treścią: pierwsza to obsceniczna postawa, a drugie agresywne zachowanie. Oba zjawiska są powszechnie zauważalne i obecne na różnego rodzaju portalach społecznościowych.

Obsceniczność związana jest z handlem materiałami seksualnymi w cyberprzestrzeni. Jednak dyskusja na temat np. cyberpornografii pokazuje niezwykłą złożoność problemu z uwagi na fakt, że zjawisko to niekoniecznie jest niezgodne z prawem.

O stopniu komplikacji w sposobie interpretowania nagości świadczy przykład wielu reklam i teledysków, które mają charakter kontrowersyjny i które emitowane są przez środki masowego przekazu w krajach europejskich bez zauważalnego protestu społecznego. Natomiast te same obrazy telewizyjne mogą być prawnie zakazane w niektórych społeczeństwach islamskich, bez względu na całkowitą akceptację przez inne kraje.

Często spotykaną definicją cyberprzestępczości jest sprowadzenie tego pojęcia do takich zdarzeń jak: krzywda moralna, materialna, psychiczna, która wynikła na skutek mowy nienawiści. Cyberprzemoc dotyczy gwałtownego wpływu działalności cybernetycznej na osobę prywatną bądź publiczną. Chociaż takie działania nie mają w sobie przemocy fizycznej, ofiara będzie jednak odczuwać siłę i gwałtowność aktu co w rezultacie może przynieść długoterminowe konsekwencje psychologiczne. Działanie te zwane także jako „hate" przynosi tragiczne skutki szczególnie w grupie młodych ludzi.

Przypadki cyberprzestępczej działalności można sklasyfikować w kilku grupach. Do pierwszej z nich można zaliczyć sytuację, w której technologia jest zaangażowana w przestępstwo, ale nie wykorzystuje specyficznych cech Internetu. Na przykład fora i grupy dyskusyjne rozpowszechniają wiedzę na temat tego jak popełnić przestępstwa.

Zjawisko „hackingu" jest dobrym przykładem tego, jak Internet, głównie poprzez grupy dyskusyjne, łączy osoby o wspólnych wartościach oraz umożliwia im realizacje potrzeb poprzez wspólne prowadzenia działań. Następuje więc integracja osób ze specyficznymi umiejętnościami w celu wspólnego działania lub odtworzenie ich umiejętności i wiedzy.

Jeśli jednak tego typu wypowiedzi lub domeny internetowe zostaną usunięte, to prawdopodobnie takie działania zostaną zmniejszone pod względem liczby, to jednak nadal będą utrzymywane i będą prowadzone przez alternatywne formy komunikacji jak np. telefon czy też usługa pocztowa.

Po drugie, Internet stworzył środowisko ponadnarodowe, które zapewnia zupełnie nowe możliwości szkodliwych działań będących obecnie przedmiotem prawa karnego lub cywilnego. Przykłady takich działań obejmują handel materiałami erotycznymi, środkami odurzającymi lub też bronią.

Po trzecie, wirtualna przestrzeń marginalizuje znaczenie czasu i odległości co bezpośrednio wpływa na transfer – często nielegalny lub szkodliwy – własności intelektualnych. Taka czynność obejmuje nieupoważnione przesyłanie w cyberprzestrzeni produktów w szczególności do miejsc docelowych, które nie podlegają jurysdykcji przez państwo, na terenie którego dokonany został transfer. Zjawisko to może stanowić jeszcze większe zagrożenie oprócz przesyłu produktów

bez wiedzy i przyzwolenia ich autora. Może ono być także sposobem na popularyzację szkodliwych treści, wzywających do dokonywania zamachów terrorystycznych.

Przestępstwa w cyberprzestrzeni dokonywane są przez różne osoby i organizacje o odmiennych celach i motywacjach jak i umiejętnościach. Mogą to być więc samotni przestępcy, motywowani finansowo, ideologicznie, religijne bądź też chęcią zemsty. Na drugim końcu spektrum cyberprzestępczości znajdują się międzynarodowe struktury polityczne lub terrorystyczne, których tryb działania w zakresie komunikacji i funkcjonowania online w dużej mierze odzwierciedla organizacje korporacyjne [20].

Cyberataki stały się coraz bardziej kosztowne dla firm. Ich konsekwencją są oczywiście koszty finansowe, ale i również utrata zaufania oraz prestiżu w oczach klientów. Często występującym przestępstwem są również włamania do komputera, które można określić jako nieautoryzowany dostęp do systemu komputerowego, w którym prawo własności zostało już wcześniej ustalone.

Zjawisko cyberprzestępstwa sprowadza się głównie do uzyskiwania nieautoryzowanego dostępu do systemów cyfrowych w celu pozyskania poufnych informacji, uszkodzenia danych lub powodowania zakłóceń w pracy. Cyberataki mogą być przeprowadzane także w sposób, który nie wymaga uzyskiwania nieautoryzowanego dostępu. Udane ataki cybernetyczne mogą powodować znaczne koszty dla firm, które są ich ofiarami.

Kradzież skomplikowanych projektów, planów, innowacji czy też produktów, będących efektem żmudnej i długotrwałej pracy, może zostać utracony w przeciągu sekundy. Niezwykle często ceniona własność intelektualna zostaje skradziona przez cyberprzestępców, hakerów lub określone państwa.

Motywacją dla cyberprzestępczości są w dużej mierze zyski finansowe, zgodnie z zasadą: po co popełniać kradzież o wysokim stopniu ryzyka, jeśli można tego dokonać np. poprzez wiele oszustw o mniejszej wartości w zaciszu własnego domu.

Kwestie związane z cyberbezpieczeństwem nie są wystarczająco rozumiane przez ogół społeczeństwa, a szczególnie przez pracowników instytucji publicznych. Specjaliści oraz technologia może w większości przypadków zapewnić ochronę przed cyberatakimi, jednak istnieją także sytuacje, które wymykają się systemom zabezpieczeń. Do takich zdarzeń można zaliczyć przypadkowe lub umyślne działania osób mających dostęp do systemu. Drugi natomiast przypadek wskazuje na możliwość zaistnienia luki w zabezpieczeniach łańcucha dostaw, które mogą pozwolić na przedostanie się złośliwego oprogramowania lub zainfekowanego nim sprzętu podczas procesu jego nabywania [19].

W wyniku korzystania z codziennych narzędzi cyfrowych pomagających np. uporządkować obowiązki w pracy, pozyskać informacje o zdrowiu, skorzystać z portali społecznościowych, zakupów, odsłuchania muzyki, obejrzenia filmów itp., konsumenci mogą stać się nieświadomie ofiarami cyberprzestępców, których

początkowym celem jest pozyskanie jak najwięcej danych o wybranej osobie. Aplikacje internetowe są również skutecznym narzędziem pozwalającym na śledzenie ruchów użytkownika. Poczucie ustawicznej kontroli w społeczeństwie wynika z nadania „panoptycznych" cech technologii internetowej [16]. Większość państw jest atrakcyjnym celem cyberprzestępców, ponieważ ich sieci zawierają najważniejsze informacje o obywatelach, w tym dokumentację dotyczącą zdrowia i prowadzenia pojazdów, rejestry edukacyjne i karne, licencje zawodowe oraz informacje podatkowe.

Ta nieprzerwana obserwacja nie jest domeną tylko i wyłącznie organów bezpieczeństwa państwa, ale staje się też coraz bardziej cechą organizacji działających w sektorze prywatnym, a także grup przestępczych. Te ostatnie mogą śledzić ofiary i dokonywać szkodliwych działań z ogromnego dystansu. Podobne możliwości identyfikowania przestępców mają organy ścigania [20].

Wielu użytkowników nie posiada wystarczających zasobów ani wiedzy na temat wszystkich cyberzagrożeń, co nie pozwala im na indywidualne zbudowanie skutecznej cyberochrony. Obywatele nie są w stanie w pełni i dokładnie ocenić, jak dobrze przedsiębiorstwa chronią ich prywatność. Te same systemy, które umożliwiają prywatnym przedsiębiorstwom zbieranie danych osobowych, wykorzystywane są także w nabywaniu informacji w celu ich sprzedaży reklamodawcom. Jest to swego rodzaju asymetryczna relacja między użytkownikiem a instytucją. Bezpieczeństwo obywateli jest uzależnione od decyzji instytucji co do których są ograniczone formy kontroli. Ponadto użytkownicy nie mają wystarczającej wiedzy i możliwości nadzoru nad dostawcą usług internetowych [19]. Osoby takie nie są w stanie skutecznie bronić się przed tak groźnym zagrożeniem, jak cyberatak. Podobnie jak w sprawach dotyczących bezpieczeństwa narodowego i kwestii związanych z wojną, wydaje się, że konsumenci muszą polegać na swoim rządzie i jego służbach w celu ich ochrony.

7.9 WSPÓŁPRACA MIĘDZYSEKTOROWA W ZAKRESIE CYBERBEZPIECZEŃSTWA

Choć przedsiębiorstwa i jednostki funkcjonujące w obszarze infrastruktury krytycznej mają najwyższy poziom zabezpieczeń w zakresie cyberbezpieczeństwa to jednak ich kompetencje są rozdrobnione. Okazuje się więc, że w celu poprawy cyberbezpieczeństwa organizacje muszą poświęcić więcej wysiłku w zakresie wzajemnej współpracy. Zarówno poszczególne państwa jak i instytucje nie mogą samotnie walczyć z tym problemem, zwłaszcza, że trudno jest udowodnić, kto jest autorem ataku cybernetycznego. Konieczne są zatem działanie zbiorowe. Warunkiem realizacji dużych projektów zarówno pod względem gospodarczym jak i pod względem zachowania bezpieczeństwa jest, tworzenie współpracy między instytucjami państwowymi, środowiskiem akademickim oraz przemysłem. Tak zaistniały system stwarza możliwość łączenia zarówno zarządzania informacją, wykorzystywania informatycznych doświadczeń z konkurencyjnością

przedsiębiorstw oraz osiągnięciem bądź utrzymaniem przewagi na silnie konkurencyjnym rynku.

Powtarzającym się tematem w dyskusji na temat cyberbezpieczeństwa jest napięcie istniejące między sektorem publicznym i prywatnym. Informacje przechowywane przez firmy prywatne mogą obejmować tajemnice handlowe, informacje o klientach, czy też dane o projektach w fazie opracowywania. Za każdym razem, gdy uzyskuje się lub posiada się dostęp do wielu prywatnych informacji, to bez odpowiednich procedur, pojawiają się dużo wątpliwości i kontrowersji w procesie ich zarządzania.

Prywatne informacje przechowywane przez rząd mogą zawierać wrażliwe dane dotyczące problematyki militarnej, strategii negocjacyjnych bądź prywatnej korespondencji czołowych polityków, która w przypadku ujawnienia może skutkować kompromitacją wcześniej wypracowanego publicznego wizerunku. Poufne informacje są przechowywane zarówno przez osoby prywatne, jak i publiczne [11].

Instytucje mają ogromną potrzebę poprawy badań nad cyberbezpieczeństwem, ale jedną z największych przeszkód jest brak zaufania oraz strach przed niepewnością co do losów informacji powierzonych drugiej stronie. Rząd nie chce, aby informacje o zagrożeniach cyberbezpieczeństwa były przekazywane innym instytucjom bądź za ich pomocą do opinii publicznej. Podobnie jak w przypadku sektora prywatnego, który nie chce, aby tajemnice handlowe lub wrażliwe informacje konsumenckie stały sie powszechnie znane. Obawa przed wyciekiem informacji po obu stronach, czyli rządu i sektora prywatnego jest doskonałą ilustracją znaczenia informacji. Warto zauważyć, że istnieją różne oczekiwania wynikające z odmienności celów, ponieważ każda z tych grup ma na celu maksymalizację własnego interesu.

Głównym zadaniem jakie stoi przed obiema sferami jest więc skoncentrowanie wysiłków na znalezienie równowagi między cyberbezpieczeństwem a cyberprywatnością. Jednym z punktów mogących rozwiązać ów problem jest stworzenie takiego prawodawstwa, które będzie sprzyjać współpracy i zaufaniu między sektorem publicznym i prywatnym. Kolejnym rozwiązaniem jest gromadzenie informacji w zbiorze, który pozostaje na wyłączność instytucji, która jest ich właścicielem. Wybrany fragment takiego kompendium ważnych informacji, byłby udostępniony po odpowiednio wcześniejszym sprawdzeniu. Następna uwaga odnosi się do spostrzeżenia, że agencje rządowe oraz firmy uczestniczące w tym systemie współpracy nie powinny być zmuszane do wymiany informacji. A zatem konieczna jest pewnego rodzaju autonomia, która zamiast osłabiać międzysektorowe zaufanie, będzie wzmacniać poczucie prywatności oraz wspierać współpracę.

Prawo ochrony prywatności ewoluowało w ciągu XX wieku, jednak postęp technologiczny zwłaszcza w zakresie cyberprzestrzeni doprowadził do jeszcze bardziej skomplikowanych pod względem prawnym i moralnym sytuacji.

Wydarzenia z 11 września 2001 roku pod wpływem presji publicznej zmusiły rządy wielu państw do wprowadzenia wszechstronnego nadzoru. Na marginesie rozważań dotyczących współpracy instytucji warto zasygnalizować, że debaty z zakresu polityki bezpieczeństwa oraz funkcjonowania cybertechnologii często powodują podkreślenie dychotomii między sprzecznymi interesami [12]. Refleksja na temat funkcjonowania technologii dotyka problemu dążenia do osiągnięcia równowagi pomiędzy prywatnością a bezpieczeństwem. Obywatele – najczęściej w wyniku informacji medialnych – wyrażają swoje zaniepokojenie stopniem inwazji w prywatne życie, którą przeprowadzają służby rządowe.

W kontekście współpracy w ramach cyberbezpieczeństwa jednym z głównych uczestników są instytucje naukowe, które z jednej strony, aby być innowacyjne muszą współpracować z sektorem prywatnym. Ponadto ich wyniki badań najczęściej korespondują z zapotrzebowaniami gospodarki rynkowej. Z drugiej strony instytucje badawcze są zazwyczaj organizacjami sektora publicznego. A zatem są organizacjami doskonale łączącymi wiedzę i doświadczenie z zakresu sektora prywatnego z sektorem państwowym. Reasumując w celu zrównoważenia prywatności i bezpieczeństwa oraz wspierania współpracy między sektorem publicznym i prywatnym mostem łączącym obie sfery jest nauka.

Wiele sieci komputerowych i infrastruktury krytycznej znajdują się w sektorze prywatnym, co oznacza, że rząd nie może sam nimi zarządzać. Ale faktem jest, że sektor prywatny również nie może tego robić sam, ponieważ rząd, jest instytucją która często dysponuje najnowszymi informacjami na temat nowych zagrożeń. Sposób na obronę państwa przed cyberzagrożeniami polega na tym, że rząd i przemysł współpracują ze sobą, dzieląc się odpowiednimi informacjami jako partnerzy.

7.10 PODSUMOWANIE

W dzisiejszym świecie nauka o polityce jak i o bezpieczeństwie analizując problem cyberbezpieczeństwa wykracza poza ramy obszaru militarnego. Jednym z głównych zainteresowań badawczym są scenariusze zagrożeń i rozwój krajowego systemu obrony. Technologia informacyjna odpowiada na potrzeby ludzkie, za którymi stoi rozwój technologii, w wyniku którego następuje integracja informacji, organizacji, biznesu, edukacji i polityki. Powyższy artykuł wskazuje również na potrzebę posiadania kompetencji z obszaru edukacji dla cyberbezpieczeństwa.

Wraz z pojawieniem się technologii cyfrowej, naruszenie dóbr drugiej osoby staje się bardzo łatwym i powszechnym procederem. Stworzenie gotowych rozwiązań w sprawie cyberbezpieczeństwa nie jest prostym zadaniem, m. in. z uwagi na coraz bardziej wielobiegowy świat.

Cyberzagrożenia pokazują, że stopniowo państwo oraz obywatele tracą kontrolę nad infrastrukturą informatyczną. Ponadto cyberataki są coraz bardziej wyrafinowane, stąd zapewne znacznie większe zaangażowanie rządów na całym

świecie w sferze poprawy cyberbezpieczeństwa. Ochrona cyberprzestrzeni powoli traktowana jest jako priorytet bezpieczeństwa narodowego.

Przemysł, organy ścigania, agencje wywiadowcze muszą współpracować w celu przeciwdziałania zagrożeniom ze strony przestępców, hakerów czy też hacktiwistów i terrorystów. Jest to szczególnie ważne, ponieważ zagrożenie działalnością przestępczą m.in. w sektorze usług finansowych nadal wzrasta.

LITERATURA

1. M. Cavelty Dunn. *Cyber-Security and Threat Politics. US Efforts to Secure the Information Age*. Londyn Routledge, 2008, ss. 19-23.
2. S. Collins, S. McCombie. "Stuxnet: the emergence of a new cyber weapon and its implications." *Journal of Policing, Intelligence and Counter Terrorism*, vol. 7/1, ss. 80-91, 2012.
3. N. Degele. "Knowledge in the information society." *World Futures. The Journal of New Paradigm Research*, vol. 50/1-4, ss. 743-755, 1997.
4. Digital agenda for Europe, źródło: https://europa.eu/european-union/topics/digital-economy-society_en [dostęp:03.03.2017].
5. P. Duchessi. "Chengalur-Smith I., Client/server benefits, problems. Best practices." *Communications of the ACM*, vol.41/5, ss. 87-94, 1998.
6. H. W. Fischer. "The role of the new information technologies in emergency mitigation, planning, response and recovery." *Disaster Prevention and Management: An International Journal*, vol. 7/1, ss.28-37, 1998.
7. E. Gamreklidze. "Cyber security in developing countries, a digital divide issue. The case of Georgia." *The Journal of International Communication*, vol. 20/2, ss. 200-217, 2014.
8. M. Górka. „Wolność czy bezpieczeństwo? Przyczynek do rozważań na przykładzie ustawy o działaniach antyterrorystycznych z dnia 10 czerwca 2016 roku." *e-Politikon*, vol. 9, ss. 49-79, 2016.
9. K. E., Greenaway, Y. E., Chan, R.E. Crossler. "Company information privacy orientation: a conceptual framework." *Information Systems Journal*, vol. 25/6, ss. 579–606, 2015.
10. L. Herrington, R. Aldrich. "The Future of Cyber-Resilience in an Age of Global Complexity." *Politics*, vol. 33/4, ss. 299–310, 2013.
11. J. P. Kesan, C. M. Hayes. (2014). "Creating a „Circle of Trust" to Further Digital Privacy and Cybersecurity Goals." *Michigan State Law Review*. [On-line].5, ss.1475-1489. Dostępny: http://digitalcommons.law.msu.edu/lr/vol2014/iss5/6 [Marzec 03, 2017].
12. J. E. Kirtley. "Transparency and Accountability in a Time of Terror: The Bush Administration's Assault on Freedom of Information." *Communication Law and Policy*, vol. 11/4, ss. 479-509, 2006.
13. D. Lane. "The International Context: Russia, Ukraine and the Drift to East-West Confrontation." *International Critical Thought*, vol. 6/4, ss.623-644, 2016.
14. J. Lyne. (2013, Wrzesień). "30,000 Web Sites Hacked A Day. How Do You Host Yours?." *Forbes*. [On-line]. 17, s.30. Dostępny: https://www.forbes.com/sites/jameslyne/2013/09/06/30000-web-sites-hacked-a-day-how-do-you-host-yours/#2a7381701738 [Marzec 04, 2017].

15. S. J. Shackelford. (2010, Styczeń). "Estonia TwoandaHalf Years Later: A Progress Report on Combating Cyber Attacks." *Journal of Internet Law*. [Online]. s.22-29. Dostępny: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1499849 [Marzec 04, 2017].
16. Ch. A. Smith, T. Bellier, J. Altick. "Ego-Panopticism: The Evolution of Individual Power." *New Political Science*, vol.33/1, ss. 45-58, 2011.
17. H. Tiirmaa-Klaar. "Building national cyber resilience and protecting critical information infrastructure." *Journal of Cyber Policy*, vol. 1/1, ss. 94-106, 2016.
18. T. Thomas. "Russia's Military Strategy and Ukraine: Indirect, Asymmetric—and Putin-Led." *The Journal of Slavic Military Studies*, vol.28/3, ss. 445-461, 2015.
19. L. J. Trautman. "Cybersecurity: What about U.S. Policy?." *Journal of Law, Technology and Policy*, vol. 341, s. 355, 2015.
20. D.S. Wall, "The Internet as a Conduit for Criminals Activity," w *Information Technology and the Criminal Justice System*, red., A. Pattavina, Londyn: Sage, 2005, ss. 77-98.
21. J.J. Wirtz. "The Cyber Pearl Harbor." *Intelligence and National Securit*, vol.32/1, ss.1-10, 2017.
22. F. Webster. "What information society?." *An International Journal*, vol.10/1, ss. 743-755, 1994.

Data przesłania artykułu do Redakcji: 04.2017
Data akceptacji artykułu przez Redakcję: 06.2017

dr Marek Górka
Politechnika Koszalińska
Wydział Humanistyczny
ul. Kwiatkowskiego 6e, 75-343 Koszalin, Polska
tel./fax: +4894 343 91 71, e-mail: marek_gorka@wp.pl

TECHNOLOGIA INFORMACYJNA W OBSZARZE CYBERBEZPIECZEŃSTWA PAŃSTWA I SPOŁECZEŃSTWA

Streszczenie: *Polityka bezpieczeństwa jest kwestią kluczową dla społeczeństwa informacyjnego. Oprócz zwiększenia zasobów technologicznych w dziedzinie cyberprzestępczości potrzebne są także nowe metody, instrumenty i umiejętności leżące po stronie personelu pracującego w administracji oraz w instytucjach wchodzących w zakres infrastruktury krytycznej. Głównym tematem tego artykułu jest wskazanie na cyberbezpieczeństwo jako zjawisko obecne na styku nauk społecznych oraz technicznych. Zrozumienie oraz zdefiniowanie zagrożeń w zakresie bezpieczeństwa w sieci, może pomóc organizacjom w sektorze publicznym i prywatnym. Cyberbezpieczeństwo jest skomplikowane zjawiskiem. Wynika to przede wszystkim z natury nowoczesnego środowiska, w którym przechowywane są kluczowe informacje dla wielu instytucji. Ponieważ zarówno sektor publiczny, jak i prywatny potrzebują wykwalifikowanych pracowników w obszarze cyberbezpieczeństwa nauka odgrywają ważną rolę w dziedzinie bezpieczeństwa w sieci.*

Słowa klucze: *cyberbezpieczeństwo, bezpieczeństwo informacji, cyberprzestępczość, edukacja dla cyberbezpieczeństwa, społeczeństwo informacyjne*

INFORMATION TECHNOLOGY IN THE AREA OF CYBER SECURITY OF THE STATE AND SOCIETY

Abstract: *Security policy is a key issue for information society. In addition to increasing technological resources in cybercrime, new methods, instruments and skills are needed for staff working in the administration as well as for institutions involved in critical infrastructure. The main theme of this article is to point to cyber security as a phenomenon at the junction of social and technical sciences. Understanding and defining network security threats can help organizations in the public and private sectors. Cybersecurity is a complex phenomenon. This is primarily due to the nature of a modern environment in which key information is stored for many institutions. As both the public and private sectors need qualified staff in cyber security, science plays an important role in cybersecurity.*

Key words: *cyber security, information security, cybercrime, education for cyber security, information society*