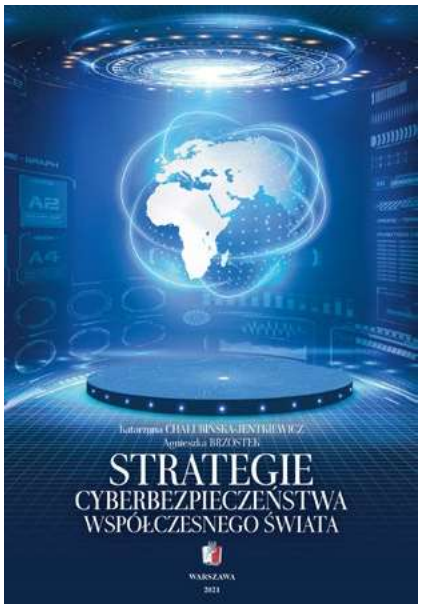
CYBERBEZPIECZEŃSTWO W POLSCE I NA ŚWIECIE

Pakiet 2 książki

ISBN 978-83-68170-44-3 (PDF)



SYSTEM
BEZPIECZEŃSTWA
W CYBERPRZESTRZENI RP

WARSZAWA
2018

Recenzenci:
płk dr hab. inż. Piotr Dela, prof. ASzWoj
dr hab. Mirosław Karpiuk, prof. UWM

Redakcja naukowa:
prof. dr hab. inż. Waldemar Kitler
dr hab. Katarzyna Chałubińska-Jentkiewicz, prof. ASzWoj
dr Katarzyna Badźmirowska-Masłowska

Opracowanie redakcyjne:
Lech Mleczko i Zbigniew Moszumański

Opracowanie językowe i korekta:
Krystyna Koziorowska

Opracowanie graficzne i projekt okładki:
Anna Skowrońska IDEAPRESS

Publikacja dofinansowana ze środków Akademii Sztuki Wojennej

Teksty zawarte w publikacji są efektem realizacji zadania badawczego „System cyberbezpieczeństwa RP – model rozwiązań prawnych" w ramach programu GRANT BADAWCZY MON [Nr umowy GB/4/2018/2018/DA]

Wydanie I

Wydawca:
Wydawnictwo Towarzystwa Wiedzy Obronnej
ul. 11 Listopada 17/19, 03-446 Warszawa
www.two.edu.pl
e-mail: kontakt@two.edu.pl

SKŁAD
Agencja Wydawnicza IDEAPRESS
Łukowska 1/149, 04-113 Warszawa
www.ideapress.pl

SPIS TREŚCI

Wstęp

Współczesne społeczeństwo często jest nazywane społeczeństwem informacyjnym, społeczeństwem trzeciej fali lub cyberspołeczeństwem. Na określenie nowej cywilizacji używane są również takie terminy, jak: era informacyjna, era kosmiczna, era elektroniczna czy też globalna wioska. Istnieje wiele definicji. Można przyjąć, że społeczeństwo informacyjne to takie, które posiada instrumenty techniczne i prawne, ale przede wszystkim ma wiedzę, która pozwala mu z tych instrumentów korzystać; dlatego często mówimy o społeczeństwie opartym na wiedzy. Jednym z podstawowych obszarów wiedzy TIK (technologie informacyjno-komunikacyjne – *Information and Communication Technologies*), którego znaczenie wciąż rośnie, jest bezpieczeństwo. Według „Computerworld Polska" (luty 2016, nr 2/1057) wartość rynku związanego z cyberbezpieczeństwem wrosła w 2014 r. w Polsce o 8 proc. i przekroczyła 300 mln dolarów. Z tym faktem wiąże się wzrost zatrudnienia w sektorze TIK, a tendencja ta według analityków ma się utrzymać do 2019 r. Tym samym specjalizacja z zakresu cyberbezpieczeństwa pojawia się na liście najbardziej poszukiwanych kompetencji. Szacunki wskazują także, iż wojsko potrzebuje co roku przynajmniej około 50 specjalistów w zakresie cyberbezpieczeństwa, w tym ekspertów w zakresie kryptografii, organizacji oraz bezpieczeństwa systemów teleinformatycznych, z dobrą znajomością regulacji prawnych związanych z tym obszarem.

Od pewnego czasu pojęcie bezpieczeństwa państwa silnie wiąże się z bezpieczeństwem sieci i cyberprzestrzeni. Należy zaznaczyć, że bezpieczeństwo w cyberprzestrzeni zawsze było obecne w polityce

bezpieczeństwa i obronności państwa jako ważny obszar łączący procedury oraz instrumenty prawne ochrony danych, informacji i systemów. Jest ono niezbędnym elementem prawidłowego postępu naukowo-technicznego i jako takie określa potrzeby ochrony tego obszaru nie tylko z punktu widzenia użyteczności, ale również ze względu na przeciwdziałanie zupełnie nieznanym dotąd zagrożeniom. W dziedzinie cyberbezpieczeństwa pojawia się wiele określeń, takich jak: bezpieczeństwo informatyczne, cyberbezpieczeństwo, bezpieczeństwo teleinformatyczne. W dobie globalnej informatyzacji, także sfery publicznej, w warunkach rozwoju portali społecznościowych, wszechobecnego mailingu, czyli wiadomości rozsyłanych na wiele adresów e-mailowych zgromadzonych w bazie danych, często dochodzi do nieuprawnionych działań, które mogą stanowić naruszenie dóbr osobistych, prawa własności czy praw konsumenckich. Jednak coraz częściej pojawiają się także cyberzagrożenia innego typu, które dotykają struktur władzy publicznej i samego państwa. Współcześnie, kiedy strefa prywatności człowieka wolna od ingerencji osób trzecich stopniowo się kurczy, w jednakowym, a może nawet większym stopniu proces ten dotyczy obszaru prawidłowego działania administracji publicznej oraz jej służb, także sił zbrojnych.

Przetwarzanie informacji w przestrzeni wirtualnej powoduje, iż konieczne staje się regulowanie kwestii dostępu do nich; dostęp ów może się bowiem stać źródłem zagrożeń, nawet w przypadku, kiedy nie mają one charakteru niejawnego. Coraz częściej ataki na informacje lub przy wykorzystaniu informacji przyjmują charakter masowy i wielokierunkowy. Ale nie tylko o ochronę informacji tu chodzi. Zagrożenia, jak określa to definicja cyberprzestrzeni, mogą wynikać z relacji między sieciami, między sieciami i komputerami, a także z relacji użytkowników z sieciami i komputerami; dotyczy to również relacji między użytkownikami oraz między komputerami.

Na ten globalny charakter zagrożeń związanych z bezpieczeństwem w cyberprzestrzeni wskazują kolejne debaty dotyczące przyszłych uregulowań prawnych. Jedną z nich była konferencja na temat „System bezpieczeństwa w cyberprzestrzeni RP", która odbyła się 11 grudnia 2018 r. w Sejmie RP, a której organizatorami byli: Komisja Obrony Narodowej Sejmu RP, Komisja Administracji i Spraw Wewnętrznych Sejmu RP we współpracy z Katedrą Prawa Mediów, Własności Intelektualnej i Prawa

Nowych Technologii Instytutu Prawa i Administracji Obronnej Wydziału Bezpieczeństwa Narodowego Akademii Sztuki Wojennej w Warszawie. W trakcie tego dyskursu pojawiła się dyrektywa wskazująca na potrzebę budowy systemu cyberbezpieczeństwa w Polsce obejmującego różne obszary działania jednostki i państwa oraz różne poziomy interwencji regulacyjnej. Efektem tych analiz jest przekazana w Państwa ręce publikacja. Należy zaznaczyć, że praca ta stanowi samodzielną monografię obejmującą szereg zagadnień, albowiem także poruszana w niej problematyka cyberbezpieczeństwa to obszar interdyscyplinarny obejmujący sektor publiczny oraz sektor prywatny.

Wobec wskazanych powyżej uwarunkowań konieczne stało się ukierunkowanie rozważań naukowych na zagadnienia związane z cyberbezpieczeństwem. To także konieczny element prawidłowego rozwoju społeczeństwa w zakresie organizacji i zarządzania obronnością państwa, zarówno w kontekście zewnętrznego bezpieczeństwa państwowego, jak i bezpieczeństwa wewnętrznego, praktycznie na każdym poziomie funkcjonowania społeczeństwa i samej administracji (struktura rządowa oraz samorządowa z organizacją krajowej infrastruktury państwa).

Należy zatem przyjąć, że cyberbezpieczeństwo jest zjawiskiem interdyscyplinarnym, korzystającym z dorobku wielu innych dziedzin (w tym z różnych dziedzin prawa). Aby jednak wyodrębnić je z całego systemu prawa i administracji publicznej (w tym drugim przypadku przede wszystkim organizacyjnie i podmiotowo), konieczne jest określenie zakresu działania, jakiego sfera ta dotyczy (zarówno w sensie przedmiotowym, podmiotowym, organizacyjnym, jak i funkcjonalnym). Dopiero wówczas będzie możliwe usystematyzowanie przedstawionej problematyki. W naszym przekonaniu jest to zabieg niezbędny w obliczu rozwoju TIK i cyberprzestrzeni oraz zagrożeń z nimi związanych dla obronności państwa i bezpieczeństwa jednostki. Wstępna diagnoza postawiona w niniejszej pozycji stanowi pierwszy krok w próbach dookreślenia zakresu merytorycznego systemu cyberbezpieczeństwa RP.

Waldemar Kitler
Katarzyna Chałubińska-Jentkiewicz
Katarzyna Badźmirowska-Masłowska