Wstęp
Introduction

Cyberprzestrzeń może wydawać się bardzo oddalona od sfery obronności i bezpieczeństwa narodowego. W ciągu ostatnich 20 lat technologie cyfrowe połączyły nasze życie osobiste i zawodowe, podniosły konkurencyjność firm na niespotykany dotąd poziom, a także zbliżyły administrację do użytkowników. Każdy bowiem korzysta z połączonych sieci z zaawansowanymi programami cyberobrony. Na poziomie indywidualnym atak może być przeprowadzony wielopłaszczyznowo i przynieść rozległe szkody, tj. kradzież tożsamości, próby wyłudzenia czy utrata danych osobowych, włamania do sieci osobistych oraz kradzież rodzinnych pamiątek. Cyberprzestrzeń stała się miejscem konfrontacji, zawłaszczania danych osobowych, szpiegowania naukowego, gospodarczego i handlowego dziedzictwa firm będących ofiarami konkurencji lub obcych mocarstw czy też wstrzymywania usług niezbędnych do prawidłowego funkcjonowania gospodarki lub życia codziennego, narażenia utraty suwerenności, a nawet – w pewnych okolicznościach – pozbawienia życia ludzkiego.

Współcześnie cyberprzestrzeń nie jest już traktowana jako odrębna kategoria polityki czy działalności oddzielonej od innych elementów władzy krajowej. Cyberprzestrzeń i jej ochrona stały się bowiem stałym elementem systemu ochrony bezpieczeństwa państwa i obronności. Na poziomie ogólnopaństwowym takie ataki mogą przynieść długotrwale odczuwalne skutki finansowe, ekonomiczne i społeczne. Szczelny, ofensywny, sprawnie współpracujący

z podmiotami zewnętrznymi, prowadzący ciągły monitoring i wyposażony w specjalistów w odpowiednich dziedzinach system bezpieczeństwa cybernetycznego może zmniejszać skutki tych ataków, a nawet je uniemożliwić. Dotyczy przede wszystkim najważniejszych systemów cybernetycznych, takich jak: sieci energetyczne, sieci komunikacyjne lub instytucje finansowe, które są tak ważne, że każde zakłócenie może mieć poważne konsekwencje dla bezpieczeństwa publicznego i bezpieczeństwa narodowego. Nie sposób nie docenić wysiłków organów ścigania, które mają na celu zwalczanie cyberprzestępczości przy jednoczesnej ochronie prywatności w cyberprzestrzeni. Powszechnie uznaje się, że cyberbezpieczeństwo służy ochronie danych osobowych, a co za tym idzie – prywatności. Na przykład, Kanadyjczycy wspierają wysiłki na rzecz ochrony swojej prywatności w Internecie oraz przyznają, że organy ścigania stoją przed wyzwaniami związanymi z cyberprzestępczością, i są zaniepokojeni rosnącym zagrożeniem cyberprzestępczością osób fizycznych, organizacji sektora prywatnego i publicznego oraz rządów.

Niniejsza monografia powstała w wyniku realizacji przez Akademię Sztuki Wojennej grantu badawczego na temat: „System cyberbezpieczeństwa RP – model rozwiązań prawnych" – jako projektu w zakresie obronności i bezpieczeństwa państwa, finansowanego ze środków Ministerstwa Obrony Narodowej[1]. Cyberbezpieczeństwo jako zjawisko interdyscyplinarne stało się przedmiotem rozważań Autorów. Badaniom poddano działalność państw jako podmiotów prawa międzynarodowego, skupiając się na wskazaniu prawnych i organizacyjnych rozwiązań przyjętych zarówno w wymiarze indywidualnym, jak i w sposób zorganizowany, aby efektywne przeciwdziałać oraz zwalczać niepożądane i przestępcze zachowania w cyberprzestrzeni. Wyodrębnieniu uległy także relacje pomiędzy

[1] „System cyberbezpieczeństwa RP – model rozwiązań prawnych" – projekt w zakresie obronności i bezpieczeństwa państwa, objęty kodem A.I.1.2.0 i numerem Kwestury 62, finansowany ze środków Ministerstwa Obrony Narodowej na podstawie decyzji nr 5/2018/GB z dnia 7 listopada 2018 r. [umowa MON GB/4/2018/208/2018/DA]. Kierownik projektu: dr hab. Katarzyna Chałubińska-Jentkiewicz, profesor ASzWoj. Zadanie badawcze nr 3: *Diagnoza formalno-prawnych podstaw i stanu organizacji bezpieczeństwa personalnego w aspekcie prywatności i tożsamości w ramach jednolitego i zintegrowanego systemu cyberbezpieczeństwa RP.*

systemem cyberbezpieczeństwa a systemem prawa i związanym z tym działaniem organów władzy publicznej. Odrębna kwestię stanowi analiza prawno-administracyjnych uregulowań w zakresie ochrony danych osobowych jako ochrony prawa do prywatności oraz ochrony informacji w cyberprzestrzeni, a także odpowiedzialności karnej za naruszenie dóbr podlegających ochronie.

Redaktorzy