Wstęp

Państwo polskie, dostrzegając zalety płynące z funkcjonowania społeczeństwa informacyjnego, jest zaangażowane w jego budowę od wielu lat. Podejmowane działania oraz środki przeznaczone na realizację celów obrazują rolę, jaką odgrywa współcześnie cyberprzestrzeń. Dzięki niej można funkcjonować obecnie zarówno w sferze prywatnej, jak i publicznej. Tak ważne znaczenie cyberprzestrzeni jest spowodowane przede wszystkim rozszerzaniem się globalnej sieci teleinformatycznej, łączącej miliony użytkowników i umożliwiającej komunikowanie się między nimi, oraz korzystanie z zasobów informacyjnych zgromadzonych w systemach. Rozwój ten jest ściśle związany z przeobrażeniami technologicznymi, jakie dokonały się w obszarze komunikacji elektronicznej, a przede wszystkim w technologiach informacyjno-komunikacyjnych, dzięki którym ludzie mogą masowo komunikować się i wymieniać dane. Czynnikami zmian – według P. Fajgielskiego – są: „[...] cyfrowa postać przetwarzania danych, mobilność związana z możliwością bezprzewodowego przekazu informacji, znaczące zwiększenie pojemności nośników danych, integracja w jednym urządzeniu wielu funkcjonalności oraz miniaturyzacja”[1]. Zmiana technologiczna spowodowała wzrost do-

[1] P. Fajgielski, *Rozwój technologii informacyjnych i komunikacyjnych oraz związanych z nimi zagrożeń – wybrane aspekty prawne*, [w:] *Cyberterroryzm zagrożeniem XXI wieku*, red. A. Podraza, P. Potakowski, K. Wiak, Warszawa 2013, s. 142.

stępności i różnorodności usług, co umożliwiła przede wszystkim zaawansowana wymiana informacji.

Rozwój cyberprzestrzeni i coraz powszechniejsze wykorzystywanie technologii informacyjno-komunikacyjnych sprawiło, że przeniknęły do niej także negatywne zjawiska[2]. Głoszenie różnorodnych koncepcji życia godzących w dotychczasowe standardy, tworzenie podziemia cyfrowego, bezwarunkowe wkraczanie monopoli marketingowych w sferę prywatną, monetyzacja danych wspierana potrzebą szybkiego osiągnięcia zysku czy wszelkie inne wysiłki zmieniające uwarunkowania życia społecznego, gospodarczego i politycznego, powodują, że w cyberprzestrzeni pojawiły się zagrożenia już dobrze poznane, np. faszyzm, pornografia, pedofilia, oszustwa, kradzieże, handel ludźmi czy nawet terroryzm. Z roku na rok liczba przestępstw dokonywanych w cyberprzestrzeni rośnie niemal lawinowo. Wiąże się to z zaletami, jakie cyberprzestrzeń oferuje przestępcom. Chodzi tu głównie o globalny charakter i związany z tym brak międzynarodowych granic, a także dostępność, względnie niskie koszty, minimalne możliwości wykrycia przygotowywanego ataku, czego nie ułatwia pozorna jednak anonimowość[3]. Zagrożenia te są ważne ze względu na to, iż wszystkie podmioty w coraz większym stopniu wykorzystują cyberprzestrzeń.

Indywidualni użytkownicy są narażeni na utratę osobistych informacji, takich jak korespondencja czy prywatne treści cyfrowe, a także wykorzystywanie ich danych osobowych przez niepowołane osoby. Może się to wiązać ze szkodami moralnymi, stratami finansowymi czy utratą poczucia bezpieczeństwa, która – w przypadku dotknięcia nią większych grup społecznych – może znacznie opóźnić cyfrowy rozwój zarówno społeczeństwa, jak i samego państwa.

O wiele poważniej są jednak zagrożeni przedsiębiorcy. Cyberprzestrzeń, będąc głównym napędem gospodarki XXI wieku, staje się podstawą funkcjonowania współczesnej gospodarki[4]. Straty wiążą się głównie z utratą reputacji, kosztami finansowymi, co w efekcie może

---

[2] S. Moćkun, *Terroryzm cybernetyczny – zagrożenia dla bezpieczeństwa narodowego i działania amerykańskiej administracji. Raport Biura Bezpieczeństwa Narodowego*, Warszawa 2009, s. 2.

[3] M. Lakomy, *Zagrożenia dla bezpieczeństwa teleinformatycznego państw – przyczynek do typologii*, „E-Politikon" 2013, nr 6, s. 102.

[4] R. Tadeusiewicz, *Zagrożenia w cyberprzestrzeni*, „Nauka" 2004, nr 4, s. 32.

spowodować nawet upadek prowadzonej działalności gospodarczej. Szczególnie narażony jest sektor bankowości, a także sektor teleinformatyczny oraz wszelkie instytucje tworzące infrastrukturę krytyczną państwa, która odnosi się bezpośrednio do bezpieczeństwa całego kraju. Mając zatem na uwadze rangę strategii, która może oddziaływać bezpośrednio na podmioty administracji rządowej, a ze względu na jej umocowanie w przepisach prawa powszechnego – tylko pośrednio na pozostałe podmioty władzy publicznej, przedsiębiorców i obywateli, należy przyjąć, iż jest to dokument niezbędny w związku z rozwojem cyberprzestrzeni i powstawaniem z nią związanych cyberzagrożeń. W skali takich zmian pojawiają się zupełnie nowe wyzwania przed władzami publicznymi w obszarze regulacyjnym, zmierzające do zapewnienia na nowo definiowanego porządku i bezpieczeństwa publicznego.