Cyberterroryzm w polityce bezpieczeństwa państwa. Problemy ochrony infrastruktury krytycznej.

Streszczenie

Zasadniczym problem badawczym pracy jest próba odpowiedzi na pytanie, jaki wpływ ma zjawisko cyberterroryzmu oraz inne zagrożenia asymetryczne na rozwój regulacji prawnych, chroniących bezpieczeństwo infrastruktury krytycznej w Polsce. W zakresie objętym badaniem mieści się również próba wyodrębnienia najbardziej istotnych problemów ochrony infrastruktury krytycznej przed zagrożeniami o charakterze cyberterrorystycznym.

Do osiągnięcia wytyczonego celu badawczego wykorzystano przede wszystkim teoretyczne metody badawcze, w szczególności analizę instytucjonalno-prawną. Dokonano przeglądu dotychczasowego stanu legislacji związanej z ochroną bezpieczeństwa cyberprzestrzeni w dokumentach strategicznych Unii Europejskiej (rozdział II), Stanów Zjednoczonych Ameryki Północnej (rozdział III) oraz Rzeczpospolitej Polskiej (rozdział IV), zwracając uwagę nie tylko na zależności ściśle chronologiczne w ramach procesu prawotwórczego, lecz także na funkcje wzajemnego wpływu. Znaczący nacisk położono więc szczególnie na analizę problematyki niejednolitości identyfikacyjnej zarówno zjawiska cyberterroryzmu, jak i pojęcia infrastruktury krytycznej.

W rozdziale V poddano analizie fakt, iż precyzyjne zdefiniowanie infrastruktury krytycznej, choć możliwe na poziomie dokumentów strategicznych powstałych w wyniku procedur legislacyjnych, nie zawsze jest osiągalne i możliwe w ujęciach teoretycznym i badawczym. Jedynie uwzględnienie szerokiego kontekstu politycznego, społecznego i gospodarczego otoczenia infrastruktury krytycznej pozwala na prawidłowe definiowanie infrastruktury krytycznej.

W rozdziale VI, z kolei, będącym próbą analizy strategicznych założeń ochrony infrastruktury krytycznej RP, przedstawiono najważniejsze akty prawne regulujące procedury identyfikacji i ochrony infrastruktury krytycznej w Polsce. Z uwagi na bardzo obszerny materiał badawczy dokonano zawężenia analizowanego zakresu do legislacji krajowej w odróżnieniu od przyjętego uprzednio w rozdziałach dotyczących bezpieczeństwa cyberprzestrzeni szerokiego ujęcia uwzględniającego także USA i Unię Europejską. Przyjęcie tej perspektywy pozwoliło ocenić, w jakim stopniu wytworzenie procedur prawnych ochrony infrastruktury krytycznej przed zagrożeniami z cyberprzestrzeni stało się jednym z priorytetów stojących przed państwem, a także zdefiniować trudności, jakie stwarza konieczność realizacji tego priorytetu na poziomie legislacyjnym. Decyzja o poddaniu analizie najważniejszych aktów

prawnych regulujących procedury identyfikacji i ochrony infrastruktury krytycznej w Polsce zaowocowała także zamieszczeniem w pracy (w rozdziale VII) szczegółowego opisu systemów infrastruktury krytycznej RP.

Do najistotniejszych problemów ochrony prawnej infrastruktury krytycznej w Polsce zaliczono: trudności definicyjne pojęcia IK, wady przyjętego podejścia do identyfikacji zasobów infrastruktury krytycznej oraz niejasności w zakresie oceny krytyczności poszczególnych elementów systemu. Jako problemy ochrony zdiagnozowano także: niezgodność zapisów *Narodowego Programu Ochrony Infrastruktury Krytycznej* z obowiązującymi przepisami wyższego rzędu, przyjęte podejście do odpowiedzialności za ochronę systemów IK, wskazano także potrzebę wzmocnienia ochrony prawnej systemu elektroenergetycznego, uznanego za najważniejszy z katalogu zasobów infrastruktury krytycznej.

Słowa kluczowe: cyberterroryzm, cyberprzestępczość, infrastruktura krytyczna, terroryzm, polityka bezpieczeństwa państwa