

# BEZPIECZNA ŁĄCZNOŚĆ W OCHRONIE INFRASTRUKTURY KRYTYCZNEJ PAŃSTWA

---

Systemy i sieci teleinformatyczne eksploatowane przez administrację rządową, samorządy terytorialne, przedsiębiorstwa świadczące usługi na rzecz obronności podlegać powinny szczególnej ochronie w cyberprzestrzeni - to jeden z głównych wniosków seminarium zorganizowanego przez ASzWoj.

22 października w Akademii Sztuki Wojennej w Rembertowie odbyło się seminarium naukowe pt. "Bezpieczeństwo systemu łączności i sieci teleinformatycznych resortu obrony narodowej w ramach ochrony krytycznej państwa". Organizatorem wydarzenia był Instytut Działań Informacyjnych Wydziału Wojskowego Akademii.

Obszar bezpieczeństwa państwa - militarny i niemilitarny, narażony jest na nowego rodzaju zagrożenia. Cyberataki dotyczą zarówno organizacji publicznych i niepublicznych, państwowych i prywatnych, ale także kluczowych obszarów funkcjonowania państwa i jego infrastruktury krytycznej. Systemy i sieci teleinformatyczne eksploatowane przez administrację rządową, samorządy terytorialne, przedsiębiorstwa świadczące usługi na rzecz obronności podlegać powinny szczególnej ochronie w cyberprzestrzeni.

W wojskowych systemach łączności i informatyki dokonują się przeobrażenia w zakresie rozpoznanych oraz przyszłych, przewidywanych zagrożeń w cyberprzestrzeni. Systemy wspomaganie dowodzenia mają na celu ułatwienie podejmowania decyzji na poszczególnych szczeblach dowodzenia, kierowania i zarządzania w siłach zbrojnych, administracji państwowej oraz w firmach o kluczowym znaczeniu dla obronności państwa.

Zagadnienia z tym związane omawiano podczas sympozjum prowadzonego przez pracowników naukowych i dydaktycznych z zakładów teleinformatyki i cyberbezpieczeństwa Instytutu Działań Informacyjnych ASzWoj. W ramach konferencji odbyły się trzy panele poświęcone militarnemu wymiarowi cyberbezpieczeństwa państwa, systemom łączności i sieciom teleinformatycznym resortu obrony narodowej oraz wsparciu teleinformatycznemu w siłach zbrojnych. Sympozjum było dobrą okazją do wymiany doświadczeń, poglądów i opinii w gronie ekspertów reprezentujących siły zbrojne, administrację państwową w tym m.in. Urząd Komunikacji Elektronicznej oraz polskie i zagraniczne firmy oferujące rozwiązania kluczowe dla zapewnienia bezpieczeństwa teleinformatycznego sił zbrojnych i infrastruktury krytycznej państwa.