RĂZBOI ȘI APĂRARE ÎN SPAȚIUL VIRTUAL

WAR AND DEFENSE IN VIRTUAL SPACE

Colonel (ret.) prof. univ. dr. Gheorghe BOARU*

Rezumat: *În societatea informaţională, informaţia - ca armă, ţintă şi materie primă strategică stă la baza tuturor deciziilor.*

Războiul informaţional a devenit o zonă de cercetare şi dezvoltare excepţională, pentru care se acordă o atenţie sporită dar şi resursele necesare pentru cercetare şi implementare, datorită progreselor rapide ale tehnologiei informaţiei din ultimele decenii.

Conflictul din mediul cibernetic sau războiul cibernetic a devenit un fenomen la confluenţa mai multor forme de confruntare dintre aceşti actori, cum ar fi războiul imagistic, războiul psihologic, războiul informaţiilor/contra-informaţiilor, terorismul cibernetic, războiul bazat pe reţea, războiul electronic, criminalitatea informatică etc.

Spaţiul virtual a devenit a cincea dimensiune a confruntării militare, astfel încât în cadrul războiului informaţional putem defini, în funcţie de stările de pace, criză, conflict (război) sau perioada postconflict, anumite faze specifice ale confruntării cibernetice.

Caracteristica comună a confruntărilor din spaţiul cibernetic este raportul antagonic continuu stabilit între ameninţările care se manifestă în spaţiul cibernetic (terorism, spionaj, sabotaj, subversiune şi crimă organizată) şi securitatea informaţională.

NATO a dezvoltat politici şi strategii, a înfiinţat organisme şi instituţii, în domeniul apărării cibernetice. România a acţionat în conformitate cu măsurile europene şi ale NATO elaborând documente similare şi creând structuri naţionale specifice de securitate cibernetică.

Cuvinte-cheie*: războiul informaţional; războiul cibernetic; spaţiul virtual; securitatea cibernetică; terorismul cibernetic; războiul electronic; securitatea informaţională.*

Abstract: *Within the information society, information - as a weapon, target and strategic raw material is the starting point from which all decisions are made.*

Information warfare has therefore become an area of exceptional research and development, generating a lot of interest and attention as well as involving a lot of resources needed for research and implementation, due to the rapid advances in information technology in recent decades.

The conflict in cyberspace or cyber warfare has become a phenomenon at the confluence of several forms of confrontation between these actors, such as imagistic warfare, psychological warfare, information / counter-information warfare, cyber-terrorism, network-based warfare, electronic war, cybercrime, etc.

* Membru corespondent al Academiei Oamenilor de Ştiinţă din România, Membru al Academiei de Ştiințe ale Securității Naționale, e-mail: boarugheorghe@yahoo.com

Cyberspace has become the fifth dimension of the military confrontation so that in the information warfare, we can define, depending on the states of peace, crisis, conflict (war) or the post-conflict period, some specific phases of cyber confrontation.

The common feature in the cyber-space confrontations is the continual antagonistic ratio established between cyber threats (terrorism, espionage, sabotage, subversion and organized crime) and information security.

NATO has developed policies and strategies, set up bodies and institutions in the field of cyber defense. Romania has acted in accordance with European and NATO measures by developing similar documents and creating specific national cyber security structures.

Keywords: *information warfare; cyber war; virtual space; cyber security; cyber terrorism; electronic warfare; information security.*