Bucureşti, 14 octombrie 2015

RĂZBOIUL HIBRID. AMENINȚAREA CIBERNETICĂ

Asociaţia **New Strategy Center** a organizat miercuri, 14 octombrie a.c., la Cercul Militar Naţional, dezbaterea cu titlul: „***Războiul hibrid. Amenințarea cibernetică***". Aceasta este prima dintr-o serie de dezbateri dedicate războiului hibrid şi multiplelor sale forme de manifestare. În acest sens, personalități marcante din țară și din străinătate vor împărtăși experiența și viziunea lor privind războiul hibrid, amenințarea cibernetică, războiul informațional, precum şi noile forme de amenințare militară.

Criza de securitate din Ucraina a arătat forța şi eficiența războiului hibrid readucând în prim plan multiplele sale de manifestare. Războiul hibrid este o formă de conflict interstatal nedeclarat, care încorporează capabilități convenționale și nonconvenționale, militare și nonmilitare, tactici combinate și acțiuni teroriste, agresorul urmând exploatarea vulnerabilităților inamicului său.

Conştientizarea crescândă a seriozității amenințării cibernetice s-a accentuat din ce în ce mai mult în ultimii ani. Într-o lume globalizată și puternic dependentă de comunicațiile electronice, statele au devenit din ce în ce mai vulnerabile pe frontul cibernetic, cu atât mai mult cu cât unele grupări teroriste sau de criminalitate organizată dispun în prezent de capabilități ofensive serioase în acest domeniu. În condițiile în care se așteaptă ca atacurile cibernetice să cunoască un trend ascendent, multe țări occidentale și-au sporit considerabil capabilitățile apărării cibernetice pentru a preveni și combate eficient agresiunile în mediul virtual la adresa infrastructurilor critice ale statului, sistemelor de comunicații sau organismelor guvernamentale, precum și la adresa cetățenilor. În acest sens, dezvoltarea unei strategii pe termen lung vizând dezvoltarea capacității defensive a României în acest domeniu devine de o importanță critică. Astfel, consolidarea securității și protecției în domeniul cibernetic, prin asigurarea mecanismelor de prevenire și contracarare a atacurilor cibernetice la adresa infrastructurilor informaționale de interes strategic, reprezintă unul din obiectivele naționale de securitate ale României, cuprinse în strategia Națională de Apărare a Țării 2015 – 2019.

Unul din subiectele principale ale discuțiilor l-a reprezentat dimensiunea cibernetică a războiului hibrid și modul în care NATO încearcă să răspundă în mod eficient unor astfel de amenințări. În acest sens, Domnul Sorin Ducaru, asistent al secretarului general NATO, a subliniat cu tărie caracterul defensiv al mandatului NATO în combaterea acestui fenomen,

punând accent pe capacitatea de reziliență a sistemelor informatice. Mai mult decât atât, domnul Ducaru a identificat multiplele provocări și amenințări la adresa securității internaționale care pot apărea în urma utilizării cu rea intenție a tehnologiei informației și a internetului. Astfel, atât actorii statali cât și cei nonstatali pot folosi mijloacele informatice pentru a afecta în mod negativ infrastructura critică, pentru a prelua controlul asupra unor instalații militare, pentru a extrage informații clasificate, cât și pentru alte tipuri de acțiuni care pot oferi un avantaj strategic celui ce se folosește de astfel de mijloace.

Un alt subiect abordat în cadrul acestei dezbateri a fost propus de domnul general-locotenent Dumitru Cocoru, adjunct al directorului SRI și a privit modul în care România face față amenințării cibernetice. Domnul General Cocoru a subliniat faptul că România este, în mod clar, ținta unor atacuri cibernetice complexe ce au vizat infrastructurile critice, infrastructura din domeniul energetic, sistemele de comunicații din cadrul Ministerului Afacerilor Externe, precum și infrastructura din domeniul cercetării științifice și a apărării. În România, acțiunile cu cel mai mare impact și cu cea mai mare probabilitate de manifestare sunt reprezentate de spionajul cibernetic, urmat la scurtă distanță de criminalitatea cibernetică.

În completarea expunerii celor doi invitați, domnul Ionel Nițu, Președinte New Strategy Center, a adus în discuție părerea mai multor analiști care consideră faptul că în momentul de față marile puteri doar își măsoară limitele și capabilitățile între ele, neexistând până în momentul de față un război cibernetic real. În abordarea temei privind rolul spațiului cibernetic în desfășurarea operațiunilor hibride, domnul Nițu a subliniat schimbarea mediului strategic în care se desfășoară operațiuni militare, susținând ideea apariției unui nou mediu de lupta – cel cibernetic – care are capacitatea de a influența fundamental modul în care se desfășoară operațiuniile militare în celelalte medii – cel terestru, cel aerian, cel maritim și spațiul cosmic.

În urma acestei dezbateri, o serie de întrebări își vor găsi răspunsul în dezbaterile viitoare organizate de **New Strategy Center**: În ce măsură se poate aplica articolul 5 al NATO în domeniul apărării din domeniul cibernetic? În ce măsură legislația poate ajuta la crearea unui cadru care să susțină în mod eficient dezvoltarea unor capabilități de apărare în domeniul atacurilor cibernetice? Cum se pot contracara acțiunile ostile ce fac parte din războiul informațional? În zona războiului informațional cine sunt cei responsabili de apărarea Românei?