“Новата стратегическа концепция на НАТО и националната сигурност на България” – 29.11.2010

Красимира Георгиева

НАТО и новите технологии за борба с тероризма

Производството на нови по-мощни и всеобхватни оръжия е приоритет в политиката за сигурност на големите държави по подразбиране. Напоследък, в допълнение, се появяват тенденциите, свързани с организирането и провеждането на нов вид атаки – кибератаките. В изминалите няколко години много страни по света бяха подложени на масивен “щурм“ във виртуалното пространство. До скоро този нов вид тероризъм беше подценяван, но събитията от изминалите няколко години, включително и от настоящата 2010 г., дават повод да се подложи на обсъждане въпросът – заражда ли се нов вид война?

През 2007 г. потресаваща кибератака в Естония доведе до масови безредици. По време на дипломатически спор между Талин и Москва, естонските интернет страници и компютрите бяха подложени на масирани кибератаки, в резултат на което много мрежи бяха блокирани. Шокиращото и обезпокоително в случая е , че подобни атаки могат да сринат компютърните системи в няколко страни едновременно.

САЩ, въпреки че е една от най-развитите страни в икономически и военен план, става жертва на кибервойната и е неспособна да се защити. Според статистика Щатите търпят дневни загуби от няколко милиона долара именно в резултат на честите сривове и пробиви на компютърните системи. Една от американските неправителствени организации провежда експеримент , чиято цел е да докаже , значението и опасността от хакер - атаките. Симулацията показва, че в случай на грамотна атака, 40 млн. американци в източните щати могат да се окажат без електроснабдяване в продължение на половин час след атаката; след още един час 60 милиона.души ще забележат , че техните телефони са се превърнали в обикновени пластмасови кутийки. А след още два часа ще бъде парализиран и финансовият световен център - Wall Street.

Ролята на НАТО в тази нова борба срещу кибератаките е необходима и значима. Алианса е в готовност да окаже подкрепа (помощ) на страните, заплашени с този модерен вид война, чрез подготвен екип за „бърза помощ”.

НАТО, като водеща световна организация призвана да поддържа сигурността, изминава дълъг път в усъвършенстването на защитни механизми и програми за опазването на компютърните системи. През 1989 г. г-н Анил генерира защита на натовските компютри само с един персонален компютър. Днес той ръководи два екипа натоварени със същата задача - единият е в структурите на НАТО в Монс, а другият е в Брюксел. Позицията на НАТО е само отбранителна. САЩ създадоха специално отделно военно командване за реагиране при кибератаки.

На този етап нито една държава не е в състояние да изгради достатъчно добра защитна система срещу атаките във виртуалното пространство. За справяне с подобна криза е

нужна подготовка, субсидирана от много финансови постъпления. Нужно е време страните да изградят съответната отбрана. Единственото, което може да се направи, както казва Лари Клинтън, президент на компанията ISA, занимаваща се с въпросите на интернет безопасността е че „На удара ще отвърнем с удар”, тъй като организирането на една кибератака изисква много по-малко финанси , отколкото защитата от такава.

Кибератаките могат да бъдат много безобидни , но също така биха могли да нанесат непоправими щети. Предвид това, в новата концепция на НАТО се набляга и върху новия тип заплахи. Ако в следващите години Алианса успее да изпълни поставените цели, успешно ще започне да функционира механизма на защита от кибератаки.