АФСЕА СЕКЦИЯ СОФИЯ
БЪЛГАРСКА СЕКЦИЯ НА AFCEA INTERNATIONAL ЗА МОДЕРНИЗАЦИЯ НА ВЪОРЪЖЕНИЕТО, ТЕХНИКАТА, ИНФОРМАЦИОННИТЕ И КОМУНИКАЦИОННИТЕ ТЕХНОЛОГИИ ЗА НАЦИОНАЛНАТА СИГУРНОСТ

СТАНОВИЩЕ НА АФСЕА СЕКЦИЯ „СОФИЯ” ПО ТЕМАТИЧНОТО НАПРАВЛЕНИЕ” „МОДЕРНАТА ПОЛИТИКА ЗА СИГУРНОСТ И ОТБРАНА В 21 ВЕК“

Като атрибут на модерна политика за сигурност АФСЕА СЕКЦИЯ "СОФИЯ" смята изграждането на надеждна и съвместима с натовските стандарти система за кибернетична сигурност. Точния превод оставям на филолозите. Става дума за “cyber security”.

Българското правителство и Министерството на отбраната са длъжни да подкрепят не само на думи плана за действие на НАТО по киберсигурността, като

- **Споделя информация и активно сътрудничи с държавите-членки по киберсигурността ;**
- **Способства за включване на български компании в проекти по киберсигурност на НАТО;**
- **Работи по създаване на способи за идентификация;**
- **Периодично оценява кибернетичната заплаха;**
- **Работи по създаването на общи стандарти;**
- **Работейки по киберсигурността, спазва принципите за „интелигентна отбрана” т.е. да не се дублират усилията и да се пестят средства („споделени разходи”).**

Известно е, че е се полагат усилия в тези направления. Те водят ли обаче до някакви практически резултати? Изминаха почти две години, откакто е била създадена Междуведомствена работна група по киберсигурността към прословутия БОРКОР, която е излязла с предложения, които не изглеждат зле. По финансови причини обаче проектът е отхвърлен. По-късно работата е продължила междуведомствена група под ръководството на

секретар по националната сигурност към МС. Политическите сътресения, очевидно спират или забавят съвместната дейност.

Налага се извода, че първо МО като една стабилна институция, боравеща с преобладаващ обем от чувствителна информация и най-отговорни задължения по отношение на НАТО, без да спира участието в съвместни дейности, да работи активно и самостоятелно в това отношение. За целта следва да се проучат внимателно и задълбочено възможностите на български компании, които предлагат техники и технологии в сферата на киберсигурността. Преди всичко обаче, МО следва да огледа и оцени структурите си, които функционално работят в IT – сектора. В състояние ли са те да се справят с тези задачи?

На форуми на АФСЕА в последните години не еднократно тази тема е била обект на внимание и наши фирми са представяли подобни продукти. Нещо повече, секцията готви голяма конференция, съвместно с NCIA, с участието на наши и чужди компании. Проведени са предварителни разговори с МО, МТИТС, ДАНС, ДКСИ и др. ведомства.

На второ място, МО следва да се включи в инициативата на НАТО за придобиване на способности за киберзащита. То е изразило и потвърдило интереса си чрез подписване на Statement of Interest, но все още не е подписала меморандум за разбирателство (Memorandum of Understanding) и не е потвърдила участие в някой от пакетите на проекта. Проектът на агенцията CI, в който Република България. за сега не се е включила влизат: Канада, Холандия, Великобритания, Германия, Франция, Италия, Полша, Румъния, Турция. Организиран е на принципа на Smart Defense за споделени разходи – плащат всички общата сума, резултатите се ползват от всички. Задължително е да се направи възможното – български компании да участват в проекта.

ПРЕДСЕДАТЕЛ НА УС НА АФСЕА СОФИЯ

ДОКТОР СИМЕОН КРАЛИКОВ О.З. ПОЛК.