

# КРЪГЛА МАСА „СЪСТОЯНИЕ И ПРОБЛЕМИ НА СИГУРНОСТТА В КИБЕРПРОСТРАНСТВОТО НА БЪЛГАРИЯ”

## ВЪВЕДЕНИЕ

*о.р. ген. м-р Стефан Димитров - председател на УС на СОРА*

Развитието, усъвършенстването и разширяването на киберпространството върви с големи темпове. Ако днес потребителите на интернет приближават **2 млрд.**, то в близките години се очаква да се удвоят за сметка на развиващите се страни. В големите страни се обръща особено внимание на научния сектор за интернет. В САЩ са напреднали с развитието на цяла наука - **Computer Science**. Не изостават в тази област Китай и Индия, а малко по-назад са РФ и Израел.

Според **Миша Глени**, е подготвена почвата за **студена война в Интернет**. Повод за това негово заключение са фактите, че правителството на Великобритания е публикувало в своята стратегия за сигурност - стратегия за национална киберсигурност, а САЩ са създали свой щаб по отбрана в киберпространството. По негови прогнози в тази студена война ще бъдат въввлечени РФ, КНР, Индия и Израел.

Има **вече редица примери за големи кибератаки**: 2007г. - срещу **Естония**; 2008г. във войната срещу **Грузия**; 2009г. при терористичните атаки в **Мумбай** са използвани интернет телефони, а вчера съобщи за хакерски атаки срещу ядрените заводи на Иран в Бушер.

По официални данни от САЩ, числото атаки срещу Американския конгрес и правителствените сайтове е около 1.6 млрд. на месец. Атаките са два типа: лов на информация и опити за блокиране на системата.

Да си спомним наскорошния скандал с WikiLeaks, където бяха публикувани 90 хил. документа на американските военни за войната в Афганистан за периода 2004 - 2010 г.

Направено изследване, сред ръководители на компании в САЩ, показва, че 54 % от тях са били подложени на несанкциониран достъп, а на 66% от тях са нанесени вреди на операциите им.

**Накратко, каква е ситуацията в момента в световен мащаб в тази област:**

**В САЩ** киберсигурността е приоритет в националната сигурност. **Работи** се усилено и вече е създадено киберкомандване към Стратегическото командване на Пентагона; кибервойски с щат 1000 човека, провеждат се учения, изготвят се стратегии и тактики на действие; създава се нова версия Интернет (MNP) за военни цели. В рамките на Министерството на националната безопасност действа подразделение с приложение на специална програма „Айнщайн” за пресичане на опити за влизане на хакери в правителствените компютърни мрежи. Споменава се за „кибероръжия” - логически бомби, ботнети, микровълнови излъчватели /изгарящи микросхемите в радиус няколко мили/.

**Великобритания** - създаден е Оперативен център за киберсигурност, подчинен на Щаба за правителствена свръзка, също основен елемент от осъвременената Стратегията за национална сигурност. Освен това, ще бъде създадено агентство за борба с киберпрестъпността, което ще координира правителствената политика в тази област.

**В НАТО има център за киберотбрана, но** защита на компютърните мрежови системи е приоритетна задача и ще залегне в бъдещата Стратегия на НАТО /която ще бъде огласена през м. Ноември, 2010 в Лисабон/.

Повечето страни имат собствени системи за киберотбрана, но те не са обединени в рамките на НАТО. **Повече ще бъде представено в лекцията на ген. Съби Събев.**

### **ЕС**

Има информация, че системите на ЕС са най-слабо защитени. Предстои сериозна работа за обединяване на усилията на държавите членки за съгласувани действия, така както бе направено в областта на енергийната сигурност /газта/.

В същото време, Съвета на Европа е единствената международна институция приела документ против киберпрестъпността. Той влезе в сила през 2004 г. и е подписан от 22 държави, в т.ч. и САЩ.

РФ и Китай отказаха да го подпишат.

### **Китай**

Работи се усилено за поставяне на заграждения срещу хакерските атаки от САЩ и др. За тази цел е разработана специална информационна система **Kylin**, която се монтира на РС от правителствените и армейски подразделения. Китай активно действа в киберпространството с атаки срещу САЩ.

Китай е въвел строга цензура в интернет, която се явява търговска бариера, пречеща на работата на европейските компании в страната.

Неотдавна завърши и спора между САЩ и КНР по работата на Гугъл.

Китай широко практикува и кибертормоза - наети са 280 хил. души, които „работят” под форамата на обикновени участници в чатовете, неудобни на властите. Тяхната задача е да се внесе обръкване в дискусиите между участниците.

### **Русия**

САЩ и Великобритания изнасят данни за кибератаки от руски хакери към правителствените киберсистеми и особено към системите на службите за сигурност. Фирмите на тези държави също се жалват от тези хакери, стремящи се да изземат съвременни технологии.

Кремъл финансира интернет-фирмите, разпращащи съобщения в поддръжка на режима или саботиращи сайтове, критикуващи властта (кибертормоз). Интернетата в РФ се следи непрекъснато и е под контрол на властите.

Използва се и кибершантажа - престъпници срещу замогващи се фирми.

РФ не желае да приеме документът на СЕ, тъй като се опасява от нарушаване на традиционната представа за суверинитет.

### **България**

Има достатъчно данни не само за хакерски атаки, а и за извличане на информация, за копиране на банкови карти, в т.ч. и за детско насилие в интернет.

**Повече** - от нашите докладчици и в дискусията!

\*  
\* \*

В днешно време, **съгласуването на политиката за сигурност в киберпространството** е **изключително** сложно. Това засяга такива проблеми, като цензурата в Интернет, националния суверинитет, както и характера на някои правителствени режими не признаващи редица международни договори и споразумения. Освен това, често не може да се определи кой стои зад атаката - държавата, хакер - свързан ли е с дадено правителство или е „единак“.

\*  
\* \*

**Целта на тази кръгла маса** е да алармираме обществото за необходимостта от ефективни мерки срещу киберпрестъпниците; да се обмени информация между гражданите-експерти и институциите, занимаващи се със киберсигурността; да подскажем на властите за актуалността на проблема и необходимостта: киберсигурността да залегне като един от приоритетите в Стратегията за сигурност; да препоръчаме модел на подход при решаване на проблемите /избор на този на Китай и РФ , или този на Швеция, САЩ или Великобритания/.

София,

28.09 2010 г.