

НАТО И КИБЕРСИГУРНОСТТА

ГЕН. МАЙОР О.Р. С. СЪБЕВ



СЪДЪРЖАНИЕ

- **ВЪВЕДЕНИЕ**
- **КИБЕРЗАПЛАХИТЕ И ОТГОВОРА НА НАТО**
- **КИБЕРСИГУРНОСТТА В АРМИИТЕ НА
НЯКОИ СТРАНИ-ЧЛЕНКИ**
- **ЗАКЛЮЧЕНИЕ**



ВЪВЕДЕНИЕ

- **“Today you don’t need an Army; all you need is a keystroke” – EST President;**
- **Най-вероятният следващ регионален или световен конфликт – кибервойна;**
- **Една от най-вероятните опасности за НАТО – кибератаките;**
- **Над 120 страни притежават или разработват настъпателни киберспособности**
- **Днес и в бъдеще кибератаките ще нарастват по интензивност и сложност**

КИБЕРЗАПЛАХИТЕ И ОТГОВОРА НА НАТО

- 1999 г. – първи кибератаки преди началото и в хода на въздушната кампания на НАТО над бивша Югославия;
- 2002 г. – САС одобри триетапна Програма за киберзащита;
 - I етап - Съюзна способност за отговор на компютърни инциденти (NCIRC);
 - II етап – Достигане на пълни оперативни способности на Центъра на NCIRC;
 - III етап – Елиминиране/намаляване на слаби места в киберзащитата и използване на нови технологии за намаляване на киберрисковете

NCIRC

- **Правомощията на NCIRC са делегирани от страните-членки в решенията на САС**
- **Способност за киберзащита/отбрана**
 - да отговаря на заплахи и уязвимости на компютърната сигурност;
 - да обработва и докладва инцидентите и разпространява свързаната с тях информация;
 - да концентрира управлението на инцидентите чрез едно централизирано и координирано усилие;
 - да смекчава ефектите от проблемите свързани с компютърната сигурност.
- **Сътрудничество на всички цивилни и военни органи на НАТО, както и на крайните потребители**
- **NCIRC е инструмент за намаляване на рисковете в компютърната сигурност на НАТО.**

Някои NCIRC услуги

- NCIRC Бюлетени и доклади
- Мениджмънт на анти–злонамерен софтуер
 - Предоставяне обновени антивирусни програми;
 - Управление на антивирусна поддръжка и заявки;
 - Визити за полева поддръжка на компютърни системи;
- Мониторинг на съдържанието на съобщения
- Защита на Уеб-сайтове



ПРОДЪЛЖЕНИЕ

- 2007 г. – Кибератаките срещу Естония и помощта на НАТО;
- **2008 г. (януари)** – Одобрена от САС официална политика на НАТО по киберсигурността и утвърдена в Букурещ на срещата на високо равнище на НАТО;
- 2008 г. (април) – Одобрена съвместна съюзна концепция за киберзащита;
- 2008 г. (май) - Сертифициране на Център по компетентност за сътрудничество в киберзащитата/киберотбраната;



ПРОДЪЛЖЕНИЕ

- **Създаване на нов орган за ръководство на киберзащитата (NATO Cyber Defence Management Authority – NCDMA) с борд;**
- 2008 г. (август) – САС утвърди указания за сътрудничество в киберзащитата с партньори и международни организации;
- 2009 г. (април) – САС прие рамка за сътрудничество на НАТО със страните-партньори в областта на киберзащитата;
- 2009 г. – Учение на НАТО по киберзащита (Cyber Coalition 2009)

ПРОДЪЛЖЕНИЕ

- 2010 г. (май) – 13-ти работен семинар на НАТО по киберзащита (Талин, Естония);
- **2010 г. (август)** – Нова дирекция в Международния секретариат на НАТО (**Ново възникващи предизвикателства пред сигурността – Emerging Security Challenges Division**) – фокусира дейността си върху тероризма, разпространението на ОМП, енергийната сигурност и **киберотбраната.**

ОРГАНИ ЗА РЪКОВОДСТВО И ИЗПЪЛНЕНИЕ

- САС;
- Дирекция “Нововъзникващи предизвикателства пред сигурността”
- НСЗВ / НСЗА;
- Военните органи на НАТО;
- Агенцията на НАТО за КИС (NCSA)
- Органът за ръководство на кибер защитата/отбраната (CDMB);
- Технически център на НАТО за информационна сигурност;
- Център за отговор на компютърни инциденти;
- Център по компетентност за сътрудничество в киберзащитата/киберотбраната (COE CCD)



КИБЕРЗАЩИТАТА В СТРАНИ-ЧЛЕНКИ НА НАТО

- **САЩ** – приоритетна национална задача; 2010 г. – активиране на Киберкомандване; първи експедиционни подразделения за киберзащита
- **Великобритания** – Център за безопасност на виртуални операции;
- **Италия** – изграждане на командна и контролна структура за противодействие на киберзаплахи; предложение за формиране на хакерски полк



ПРОДЪЛЖЕНИЕ

- **Германия** – Департамент по информационни и компютърни мрежови операции; подготвя военни хакери;
- **България** (на национално ниво)
 - Назначен национален координатор по киберсигурността (2008 г.)
 - Акредитиран Център за действие при кризисни ситуации в компютърната сигурност (2009 г.)



ЗАКЛЮЧЕНИЕ

- Кибератаките нарастват по интензивност и сложност;
- На национално ниво България е изградила основите на киберзащитата.
- Военното ведомство все още е на етап на концептуално изясняване и предприемане на практически мерки за киберзащита на своите компютърни мрежи.
- Неотложен приоритет за МО – придобиване на надеждни способности за киберзащита.

