

# КИБЕРАТАКИТЕ – НОВИЯТ ИНСТРУМЕНТ В АРСЕНАЛА НА АРМИИТЕ

**Николай Т. Стоянов, Стоян М. Балабанов**

ИНСТИТУТ ПО ОТБРАНА, СОФИЯ, БУЛ. ТОТЛЕБЕН 34,  
ТЕЛ. +359(2) 92 21827, E-MAIL: N.STOIANOV@DI.MOD.BG  
ИНСТИТУТ ПО ОТБРАНА, СОФИЯ, БУЛ. ТОТЛЕБЕН 34,  
ТЕЛ. +359(2) 92 21800, E-MAIL: S.BALABANOV@DI.MOD.BG

## CYBER ATTACK – NEW TOOL IN ARMYS' ARSENAL

**Nikolai T. Stoianov, Stoian M. Balabanov**

*ABSTRACT: In this paper basic definitions of cyber attacks, cyber war, and information warfare and information superiority are presented. Some useful examples of using cyber attacks are pointed. Short overview of national and international structures that have responsibility for cyber defense is made. Future directions for science development in Bulgarian MoD are proposed.*

*KEY WORDS: cyber wars, cyber attacks, information warfare, information superiority;*

Достиженията в областта на електрониката и информационните технологии поставиха съвременната цивилизация в състояние, при което информацията се превръща във важен елемент за развитието на обществото, носеща в себе си значим социален елемент. Ето защо защитата на националните информационни ресурси, в това число и с използване на специално създадени за целта информационни технологии, е от особено значение за националната сигурност. Това налага икономическата, военната и научната политика на държавата да се разглеждат и през призмата на информационната сигурност. В този ред на мисли не може да се изключи и военната компонента на националната сигурност, която е в съществена зависимост от защитата на информационните ресурси [1],[5]. Нарасналата роля на нетрадиционните силови въздействия, в това число и информационни, ни кара да подходим към въпросите на военното строителство от определено нетрадиционни позиции. Един от тези нетрадиционни подходи е свързан с кибер-въздействия и защитата от тях.

Важни инструменти, определящи достигането на стратегически информационни преимущества, се явяват арсеналът от сили и средства за информационни въздействия. развитието на днешната цивилизация е създадо редица исторически предпоставки за формиране на качеството и ролята на тези сили и средства. Бързото усъвършенстване на средствата и методите за целенасочени информационни въздействия позволява не само да се влияе върху установилия се баланс на силите, но и да се изменят сега съществуващите

критерии за неговата оценка на основата на съотношение на геополитически, икономически, военни и информационни фактори.

Информационната революция променя из основи естеството на бойните действия. За да се печелят войни днес, трябва първо да се спечели информационната война. Съвременните опити потвърждават това. Всички военни успехи през последните години имат общ елемент: способността за постигане на информационно превъзходство над противника [2]. Всеки военен провал е резултат главно на неуспеха да се осигури това превъзходство. Успехът в информационните войни често зависи не само от творчеството и изобретателността на командирите, а и от прилагането на съвременни технологии.

Бъдещите войни ще се водят не само по бойните полета, но и в световните компютърни и комуникационни системи. Воюващите страни често ще бъдат познатите военни сили, но ще има и други, които почти нямат военни способности.

Информационните технологии стават толкова важни за определяне на военната мощ, че почти преобладават над всичко друго.

Самото притежаване на по-добрите технологии не гарантира успех. Побеждава тази страна, която разбира как да използва информационните технологии по-ефективно.

Информационните технологии създават днес съществена разлика между победата и загубата. По-добрата технология означава по-прецизна армия. И тъй като армиите стават все по-зависими от информационните технологии, те ще стават уязвими по нови начини. Във войните на информационния век победата обикновено е на страната на онези, които имат по-голямо влияние върху технологиите и по-добър достъп до световната електронна инфраструктура.

Натрупан е и е систематизиран значим опит за водене на информационни войни, провеждане на информационни операции, разработени са и са използвани на практика широк спектър от средства и методи за организиране, планиране и провеждане на информационни операции и оценка на постигнатия от тях резултат. Практически всички страни осъществяват или се опитват да осъществяват информационни въздействия, далеч не само в условия на войни и военни конфликти. Заедно с това информационните операции продължават да остават едно от полетата на усилено изучаване в методологичен, организационен и технически план.

„Пустинна буря” е първата война, в която една армия се приближава до използване на истинска мрежова комуникационна система. Коалицията има надградени слой след слой от комуникации: местно радио, военен сателит, търговски сателит и др [3],[4].

За първи път термина „кибервойна” се използван от Аркуила един месец след края на войната. Това изглежда е първият път, когато на някой му хрумва идеята за свързаните чрез мрежа армии.

Бойните мрежи имат два начина за атака. Те могат да нападат или да се групират. Разликата е в това дали информационната технология е приложена в оръжието или в организацията.

Следващите четири идеи определят най-важните особености на съвременната война:

- Асиметричните заплахи;
- Информационните технологии променят природата на войната;
- Разбиването на цикъла за вземане на решение на противника определя победителя в бойните действия;
- Взаимосвързаните цифрови комуникации променят начина на организация на военната сила.

Ясно се вижда, че нашата национална сигурност зависи от политиката за популяризиране, регулиране и контрол върху информационните технологии. Кибервойната ще зависи до голяма степен от това кой може да атакува и да отбранява комуникационните и компютърни системи. Най-големия проблем е просто, че кибернападателя е неизвестен. Понякога е невъзможно да се разбере, че има кибер-атака.

Кибервойната е „оръжие за масово разрушение, а не оръжие за масово унищожение”. – Питър Уилсън.

Особено място сред методите и способите за информационни атаки заемат различни технологични решения, реализирани с използване на специализиран софтуер и специални технически средства. В резултат на предприети атаки могат да бъдат осъществени: неоторизиран достъп и извличане на информация, разрушаване на информация, блокиране на системи и др. Всяка информационна атака може да се класифицира в следната последователност: цели на атаката; атакуващи; средства за атаки; достъп до информационни ресурси; постигнати резултати. Като пример за такива атаки през последните 4-5 години могат да се посочат действията срещу правителствата и техните официални сайтове в Киргизстан, Южна Корея, Естония и др.

Следва да се отбележи, че няма утвърдена дефиниция за това какво представлява “акт на война” в кибернетичното пространство. Министерството на отбраната на САЩ дава следното определение за целта: “Използване на компютърни мрежови операции с цел да се възпрепятства ефективното използване на противниковите компютри, информационни системи и мрежи, като се запази боеспособността и ефективността на собствените такива”. Днес над 120 държави използват Internet за политически, военни и икономически шпионаж и въздействия върху информационните ресурси на своите конкуренти и противници. Ето няколко примера [1][2][3][4][5]:

През 1998 г. като отговор на провежданите в Индонезия антикитайски бунтове около 3000 хакери атакуват организирано индонезийски правителствени сайтове.

През 2001 г., след като китайски военен самолет се сблъсква с разузнавателен самолет на САЩ над Южнокитайско море, над 80 000 хакера са ангажирани в “самозащитна кибер война” срещу САЩ. Оттогава Китайската Народна Република използва кибер шпионаж в съответствие с военната си стратегия, насочена срещу намаляване на технологичното превъзходство на САЩ.

През 2008 г. Израел започва операция “Лято олово” срещу Палестина. В киберпространството бързо избухва война между Израел и арабски хакери.

Правителствените естонски Web сайтове са атакувани организирано от руски хакери през 2007 г.

Организираны кибер атаки са извършени от руска страна, координирано с наземните, въздушни и морски операции на Русия срещу Грузия във войната в Южна Осетия през 2009 г. Високо организираната и координирана кампания е насочена срещу предварително определени Web сайтове на правителството на Грузия, както и на други стратегически обекти, в това число посолствата на САЩ и Великобритания.

В резултат на проведени учения в Министерство на отбраната на САЩ във връзка с установяване на потенциални опасности в резултат на кибератаки е направено заключение, че слаби страни не са само уязвимостта на мрежите и хаосът, който може да бъде предизвикан, а и опасността от несвоевременно установяване на факта, че нещо се е случило, както и произходът му.

Важно внимание на кибератаки и войни отделят както научните, така и чисто военните организации. В редица държави се създават кибер-командвания (САЩ, Русия, Китай, Германия, Иран и др.). Важно е да се отбележи, че в повечето случаи тези командвания са на стратегическо ниво, което показва и придаваната значимост на очакваните резултати. Съществуват редица проекти свързани с кибератаки и защитата от тях, като:

- Проектът на Research and Technologies Organization (RTO) на НАТО за защита от кибератаки;
- НАТО Cooperative Cyber Defence Centre of Excellence (CCD COE) със седалище в Талин, Естония основан през 2008 г.
- Последният доклад, свързан с развитието на Северноатлантическия съюз, създаден от т.нар. „група на мъдреците”, определя борбата с киберпрестъпленията като един от основните фокуси, върху който трябва да се фокусира Алианса

- Европейската агенция за сигурност (European Defense Agency-EDA) също определя като една от основните си цели борбата с кибератаките.

Политиката на Алианса в областта на киберзащитата цели осигуряване на единен и координиран подход при защитата от кибератаки на ключовите информационни системи на НАТО и отделните страни-членки, както и споделяне на най-добрите практики и предоставяне на способности за подпомагане на съюзниците при отправяне на молба за взаимопомощ. Структурите и органите за осъществяване на тази политика са в процес на изграждане.

Въпросите, свързани с кибератаките в специфичните условия на Българската армия, са застъпени и в научната политика на Министерството на отбраната. Основно научно звено в тази област е Институтът по отбрана. В създадения сектор „Защита на информацията” в състава на Института, едно от основните направления, в които работят специалистите е „Кибератаки и защита от тях”.

Стремежът на изследователите е обхващането на всички компоненти на проблема информационна сигурност, който на съвременния етап на развитие на научните знания включва:

- Методология на защитата на информационното пространство, представено като съвкупност от възгледи, модели и противоборство;
  - Действащите в информационното пространство основни фактори във вид на закономерности, в това число и представящи се в условия на априорна неопределеност;
  - Изучаване на непрекъснато променящата се методология на обработка и обмен на информация, технологичните средства за тяхната реализация и влиянието им върху методите и способите за информационни въздействия в организационен и технологичен план;
  - Същност, съдържание и развитие на информационните конфликти и технологичната страна на информационното противоборство;
  - Определяне на закономерностите на развитие на информационното пространство и търсене на слабите му страни от гледна точка на информационната сигурност;
  - Научен инструментариум във вид на технологии за осигуряване на скритост на информацията и ограничаване на възможностите от неоторизиран достъп до нея.
- На тази база се организира системата от научни изследвания, свързани с информационната сигурност, която обхваща:
- Научен инструментариум за работа в информационното пространство във вид на технологии, осигуряващи скритост на информацията;
  - Методология за обработка на информация и вземане на решения в условия на информационни конфликти, кризи и при война във вид на технологии за ефективно управление на информационните процеси с осигуряване на тяхната скритост.

Обект на изследване са широк спектър от проблеми, отнасящи се до създаване и защитата от кибернетични атаки, които обхващат организационни, програмни и технически методи. Подходът за разглеждането на информационната среда и средствата за нейното осигуряване, като възможни направления за атаки и използването им като нелетални оръжия, поставят изучаваните въпроси на едно от водещите иновационни места. За осъществяването на тези изследвания в началото на 2010 г. Министерството на отбраната на Република България одобри темата за научно-изследователска и развойна дейност „Кибератаки и защита от тях”.

В Министерство на отбраната и Българската армия, структурите отговорни за киберзащита са Дирекция „Сигурност на информацията” и Дирекция „КИС”.

В изпълнение на Цел на въоръжените сили за придобиване на способности в областта на киберзащитата е създаден Център за Управление и Реагиране при Компютърни Инциденти (ЦУРКИ), който е съвместим с NCIRC на НАТО. Центърът е изграден в съответствие с регламентиращите документи на НАТО и е предназначен за защита на

критични за сигурността на информацията данни и сървери в Автоматизирани информационни системи (АИС) и мрежи на МО и БА в мирно време, война или кризи. Непосредствено изпълнява задачи по защита, откриване, реакция и възстановяване на аномалии или кибератаки срещу комуникационните и информационните системи на МО и БА. Планира се достигане на пълната функционалност на ЦУРКИ през 2012 г.

През 2011 г. се планира участието на експерти от МО и ЦУРКИ в учението по киберзащита на НАТО като Играеща страна. Преките ползи от участието на български представители в учението по киберзащита на НАТО се изразяват в придобиването на практически умения по планиране, подготовка и участие в международни учения по киберзащита.

Структури от състава на МО активно участват в междуведомствена работна група по подготовка на Меморандум за разбирателство между Република България и НАТО, създаващ правната рамка за сътрудничество в областта на киберзащитата.

Целта на Меморандума е да формализира споделянето на информация и обмена на услуги за киберзащита, както и участието в свързани с тях дейности между Република България и органа на НАТО за киберзащита NCDMA (NATO Cyber Defence Management Authority). С неговото подписване ще бъде постигнато:

- разширяване на националните възможности за киберзащита;
- повишаване на оперативната съвместимост между Националния орган за киберзащита и този на НАТО (NCDMA);
- подобряване на възможностите за предсказване, откриване и реагиране срещу кибератаки;
- обмен на информация за киберзащита на реципрочна и балансирана основа.

В заключение може да се каже, че Министерство на отбраната на Република България възстановява традициите на научни изследвания в областта на информационната сигурност и съобразявайки се с новите реалности в Европа и света предприема иновационни програми за изследване и изучаване на новите методи и средства за водене на съвременни информационни операции и кибервойни и начините за защита от тях.

В този смисъл, всички водещи решения в тази област представляват за нас особен интерес и ние ги изучаваме и изследваме.

#### Литература:

- [1]. Goodman S., Lin H., Toward a Safer and More Secure Cyberspace, THE NATIONAL ACADEMIES PRESS, USA, 2007, ISBN 978-0-309-10395-4
- [2]. Janczewski L., Colarik A., Cyber Warfare and Cyber Terrorism, Information science reference, IGI Global, 2008, ISBN 978-1-59140-991-5
- [3]. Karatzogianni A., Cyber Conflict and Global Politics, Contemporary security studies, Routledge, 2009. ISBN 10: 0-415-45970-2
- [4]. Knapp K., Boulton W., Cyber Warfare: Raising information security to a top priority, Auburn University, The Department of Air Force, USA, 2004
- [5]. Libicki M., Cyberdeterrence and cyberwar, RAND Corporation, 2009, ISBN 978-0-8330-4734-2