САЈБЕР НАПАДИТЕ КАКО НАЈСОВРЕМЕНА ЗАКАНА ВРЗ ВОЕНИТЕ ОПЕРАЦИИ И КРИТИЧНАТА ИНФРАСТРУКТУРА

Митко БОГДАНОСКИ, Марјан БОГДАНОСКИ,
Елениор НИКОЛОВ, Драге ПЕТРЕСКИ

Воена академија „Генерал Михаило Апостолски“ – Скопје

Апстракт: Овој труд се фокусира на сајбер нападите како една од најголемите загрижености во светот на глобалните безбедносни закани, со можности за импликации врз сите сфери, почнувајќи од поединците, индустриските системи, владините и државните институции, па сè до големите интернационални организации. Сајбер нападите за многу брзо време прерасnaа во една од водечките закани врз комплетниот безбедносен систем како на национално, така и на глобално ниво. Сè поголема е свеста и кај најмалите познавачи на оваа проблематика дека сајбер закана може да предизвика огромни штети кои не би се разликувале од штетите нанесени со било каква воена операција, а сајбер оружјето, на многу посуптилен начин, може да одземе повеќе животи од било каков конвенционален напад. Владите низ целиот свет, како и сите големи светски организации, се подготвуваат да се справат со овој масивен технолошки повик за закани од глобални размери. Свеста за заканата и ризиците е висока, што условува, и покрај кризната економска ситуација во светски рамки, издвојување на големи финансиски средства со цел подготовка за одговор на нови вонредни состојби кои би биле причинети од глобалните сајбер напади.

Клучни зборови: сајбер, напади, безбедност, војување, мрежи

CYBER ATTACKS AS A CUTTING EDGE THREATS ON MILITARY OPERATIONS

Abstract: This paper focuses on cyber attacks as one of the most imoortant consideration in the world of global security attacks, with possibility of implication for

all spheres, starting from individuals, industrial systems, governmental and state's institutions and international organisations. In a very short period of time, cyber attacks have become one of the leading threats to the complete security system on national as well as global level. The field of utilization of these attacks is increasing day by day, which is primarily caused by the increased computerization of every branch of the industry.
Governments around the world and all major world organizations are preparing to cope with this massive technological call for threats with global scale. Awareness of the threat and risk is high, which requires, despite globalfinancial crisis, allocating a large sum of money in order to prepare against the new emergencies that would be caused by global cyber attacks.

Key words*:* cyber, attacks, security, warfare, networks

Вовед

Во периодот на големиот пораст на употребата на сајбер нападите како еден од главните напади со можности за комплетно блокирање, како на одбранбениот и безбедносниот систем, така и на комплетното функционирање на една држава, заштитата на информацисko-комуникацискиот систем стана една од главните загрижености на глобално ниво. Malware-ите, Тојанците, слабостите на компјутерските системи, повредливостите на мрежите, упади, крадењето на податоци, крадење на идентитет, злонамерни botnet-и и заштитата на критичната инфраструктура сè почесто се главна тема во дискусиите поврзани со безбедносните закани. Компјутерските експерти речиси секојдневно бараат помош за проблеми поврзани со овие безбедносни закани. Сајбер безбедноста секојдневно е главна тема на стотици конференции и истражувачки трудови. Многу јавни дискусии се фокусирани на заканите и методите, сè со цел да се развијат подобри одбранбени механизми. Од друга страна владите воопшто не сакаат да зборуваат не само за методите на сајбер напади и операциите, туку и за тоа која политика ја следат при реализирањето на овие операции. Причина за ова прикривање е можеби стравот дека граѓаните тоа нема да го одобрат.

Поради зголемената употреба на сајбер просторот за напад не само врз еден компјутерски систем или критичен објект, туку и врз комплентото функционирање на една држава, светските велесили и големите организации превземаат соодветни и навремени против мерки. Размислувањето во оваа насока следеше пред сè после сајбер нападите врз Естонија и Грузија, кои комплетно го блокираа функционирање на комплентата критична инфраструктура во овие држави. Една од главните противмерки која ја превземаа САД беше формирњето Сајбер командата која е формирана во 2010 година од Министерството за одбрана со цел да ја координира сајбер одбраната на воените мрежи и да спроведува воен сајбер напад. Слични вакви команди се формирани и од други велесили и организации. Ова е и

прифатливо доколку се свати местото на сајбер нападите во глобалните безбедносни закани. Доколку се погледне во одредени валидни информации кои се неодамна објавени[1,2,3,4], веднаш ќе се забележи местото на овие несиметрични закани во глобалните безбеднисни закани. Истото ќе се случи доколку се погледне и во најновите безбедносни стратегии на сите светски велесилии организации[5,6], каде овие напади ги завземаат највисоките места во набројувањето на главните безбедносни закани.

Во Интернационалната Стратегијата за Сајбер Безбедност и најновата Стратегија за Безбедност на САД, сајбер заканите се третираат на исто ниво како и воените закани[7,8]. Ако се анализира изјавата на Леон Панета, која ја даде додека беше на функцијата Директор на CIA (Central Intelligence Agency), каде истиот наведува дека "сајбер нападите се најголемата национална безбедносна закана на САД",може лесно да се увиди третманот на овие закани од страна на една од најмоќните разузнавачки организации во светот[9]. Истиот, за време на скорешното интервју, но сега во својство на секретар за одбрана на САД, дадено за CBC News[10], ја покажа загриженоста од овие напади и можните последици од истите, кои можат да бидат од „парализирање на финансискиот систем" и „исклучување на електричната мрежа", па сè до „парализирање на државата".

Од друга страна, FBI (Federal Bureau of Investigation) уште во 2009 година ги рангира сајбер нападите како трети по ред најопасни закани, кои следат веднаш по нуклеарната војна и оружјето за масовно уништување[11].

Според најновиот Извештај за глобални ризици за 2012 година[12], кој е годишен извештај на Светскиот Економски Форум, Сајбер заканите се рангирани на четврто место, секако гледано од економски аспект.

---

[1] GCHQ chief reports 'disturbing' cyber-attacks on UK, BBC News UK

[2] Cyber attacks take down two Israeli websites - is cyber warfare the next front in the middle east conflict?, FORBES

[3] Cyberattacks likely to escalate this year, US Today

[4] Cyber-attacks now the most feared EU energy threat, Euractive

[5] Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation, Adopted by Heads of State and Government in Lisbon, November 2010

[6] A Strong Britain in an Age of Uncertainty: The National Security Strategy, United Kingdom, October 2010

[7] National Security Strategy, Unite States of America, May 2010

[8] International Strategy For Cyberpace, Prosperity, Security, and Openness in a Networked World, President of the United States, May 2011

[9] Cyber-Attacks Are the Biggest National Security Threat

[10] Panetta: Cyber warfare could paralyze U.S., CBS News

[11] FBI ranks cyber attacks third most dangerous behind nuclear war and WMDs, TD Daily, 7 January 2009

Во Табела 1 е даден приказ на најпознатите сајбер напади позади кои како напаѓачи се јавуваат држави или непознати групи, а чија цел се важни државни јавни и приватни институции. Најчести последици од овие напади се одбивање на услуга, шпионажа, саботажа и крадење информации[13].

Табела 1: Најпознати напади врз националната/глобалната безбедност и критичната инфраструктура

Година	**Напаѓач**	**Цел**	**Последици**
1982	САД – ЦИА	Логичка бомба насочена кон гасоводот на СССР во Сибир	Деструкција
1999 и 2000	Русија	Пентагон, NASA, Национална Лабараторија	Крадење информации и шпионажа
2004	Кина	Sandia Национална Лабараторија, Lockheed Martin и NASA	Шпионажа
2007	Кина	Компјутерска мрежа на САД (750,000 компјутери)	Одбивање на услуга
2007	Русија	Web сајтови на владата и други важни институции /банки на Естонија	Одбивање на услуга
2008	Непознато	Воена мрежа на САД	Злонамерен код и зомби машини
2008	Кина и/или Русија	Претседателски избори на САД	Упадво email системите
2008	Русија	Web сајтови на владата и други важни институции /банки на Грузија	Одбивање на услуга
2010, 2011	Непознато (неофицијално Израел)	Иранси објект за збогатување на ураниум	Саботажа
2010, 2011, 2012	Anonymous “Operation Avenge Assange”	Повеќе цели во западните земји (јавни и приватни)	Одбивање на услуга

Од нападите претставени во Табела 1 би го издвоиле нападот на воената мрежа на САД во 2008 година, кој долго се прикриваше. Овој напад, според изјавата од 2009 година на заменикот на секретарот за одбрана, Вилијам Лин, се третира како најсериозниот сајбер напад врз воените мрежи на САД кој е иницран од преносен флеш драјв ставен во лаптоп во блискиот исток. Овој драјв содржел злонамерен код кој има можност интелегентно да се шири и низ класифицираните и низ некласифицираните системи, без да биде детектиран и во исто време да има можност да се поврзе со надворешни сервери кои се контролирани од сервери на странската разузнавачка служба

[12] Global Risks 2012 Seventh Edition, An initiative of the Risk Response Network, World Economic Forum, 2012

[13] “Investigating Cyber Security Threats: Exploring National Security and Law Enforcement Perspectives”, Frederic Lemieux, Report GW-CSPRI-2011-2

која го искористила овој код за реализирање на сајбер напад[14]. На сличниот принцип функционираат и Stuxnet и Duqu malware-ите кои се поставени во иранскиот објект за збогатување на ураниум во 2010 и 2011 година[15].

1. Општо за сајбер нападите и сајбер операциите

Сајбер нападот се однесува на спроведени акции против податоци, софтвер или хардвер во компјутерски системи или мрежи. Овие акции можат да го уништат, деградираат или одбијат пристапот. Многу владини воени и разузнавачки агенции активно се подготвуваат да спроведат и да се справат со сајбер нападот, и тоа, најверојатно, заедно со конвенционални напади или контранапади.

Сајбер операцијата, од друга страна, се дефинира на малку поинаков начин. Имено, оваа активност повеќе се однесува на собирање на разузнавачки информации, отколку на деструктивните активности. Сајбер операцијата вообичаено е насочена кон најосетливите компјутерски системи и системите со најмалку детектирачките способности. Целта е да се извлечат податоци без да се регистрира нападот. Операцијата, исто така, се однесува на форензичко враќање на подотоците од уништени (или украдени) лаптопи и медиуми за складирање.

И нападот и операцијата бараат извршување на три работи: пристап кон системот или мрежата, идентификување на повредливостите на системот кон кој се пристапува и вметнување на корисниот товар (payload). Пристапот може да се реализира преку Интернет или преку физички пристап. Повредливоста може да се појави кај системот, софтверот, интерфејсот помеѓу софтверот и хардверот, комуникациските канали, табелите за конфигурирање, корисниците и провајдерите на услуги. Корисниот товар може да биде програм за мониторинг на податоци, вирус, црв, spyware или Тројанец и најверојатно со негова помош може да се пристапи далечински до комуникациските канали на нападнатиот систем. Разликата помеѓу нападот и операцијата пред сè зависи од тоа како е искористен payload-от. За време на нападот payload-от е деструктивен, додека за време на операцијата истиот не е деструктивен. Сепак, многу често нападите се толку слични што жртвата на сајбер операцијата не е во можност да каже кој тип на напад е реализиран.

Сајбер нападот и операцијата се алатки кои нудат нов опсег на способности на владите кои можат да бидат похумани и да нанесат помала колатерална штета од нивните претходници, „кинетичките“ напади. На пример, воените операции може да се зависни од оневозможувањето на радари распоредени околу одреден град; ако со сајбер напад се оневозможат

[14] "Worst cyber attack on US military came via flash drive," PHYSorg.com, 25 Aug 2010

[15] “Индустриски сајбер напади – глобална безбедносна закана”, Интернационална конференција “Лицата на кризата”, Скопје, Март 2012

радарите, во тој случај нема да има потреба од бомбардирање на инсталациите, со што би се предизвикала колатерална штета. Разузнавачките операции кои можат далечински да украдат датотеки од одредена локација со што се овозможува избегнување на губење на животите на тајните агенти. Сепак, овие алатки можат да се искористат и за сосема други потреби, на пример шпионирање на граѓаните од страна на владни агенции.

Во Извештајот на Националниот совет за истражување на САД[16] се дискутираат техничките, политичките и социјалните аспекти на сајбер нападот и операцијата. Во него се идентификуваат комплицирани прашања кои мораат да се решат, како што се правото на воениот конфликт, заплашувањето и динамичноста на сајбер нападот. Додека принципите прифатени од страна на Обединетите Нации во врска со употребата на силите и вооруженият напад нудат добра стартна точка за интернационално дефинирање на сајбер нападите, во многу случаи на употреба на сајбер напади истите се комплетно неискористливи. Традиционалните политики на застрашување со закана за соодветен одговор на нападите во случајот за напади реализирани со искористување на сајбер просторот се проблематични и многу често и неприметливи, пред сè заради ектремно тешките услови за идентификување на напаѓачите. Динамичностите на сајбер нападот, исто така, тешко се разбираат, вклучувајќи го и тоа како да се чува сајбер конфликтот од ескалирање надвор од контролата и како да се одреди сајбер конфликтот.

2. Разгледување на сајбер нападите од технички аспект

Претходно дискутираното се донесуваше пред сè на легалниот, етичкиот и политичките аспекти на сајбер тероризмот, што е работа на правниците, етичарите и политичарите. Нашиот труд пред сè се концентрира на дефинирање на техничките аспекти на сајбер војувањето и предлагање на ефикасни мерки за намалување на ефикасноста на истите, што бара широки познавања од областа на вмрежување, компјутерските системи, безбедноста во мрежните системи и други области поврзани со компјутерските техники и телекомуникациското инженертво. Меѓутоа, нити еден познавач на било која од претходно споменатите области не може самостојно да одговори на предизвиците на сајбер нападите. Предлозите на експертите за развој на ефикасни алатки за сајбер напад или одбрана тешко дека можат да бидат реалзирани без поддршка на политичките авторитети, правниците, но и етичарите.

Сè до 90-тите години соработката помеѓу експертите од ова поле скоро и да не постоела. Во тој период развивачите на контролни системи за одбрана од проектили не биле во можност да развијат сигурен систем. После развојот

[16] National Research Council. Technology, Policy, Law, and Ethics Regarding U. S. Acquisition and Use of Cyberattack Capabilities, National Academic Press, 2009

на дебати поврзани со оваа област и размената на искуства и експертизи поврзани со несигурни големи и комплексни системи, познавањето на проблемите во оваа област значително се зголемија, што предизвика и намалување на ефектите на можните напади на овие контролни систем. Овие дебати придонесоа на подобрување на безбедносните политики, јаки автентикациските механизми и во присуство на Интернет, подобрени криптирачки механизми, технологии за развој на анонимност, предлози за намалување на нелегитимна спам пошта и неутралност на мрежата. Сепак, и покрај ова, сè уште не може да се гарантира целосна безбедност на контролните системи. Иако не е голем бројот на експерти кои можат да развијат ефикасни malware-и, црви, Тројанци и сл., сепак тие се достапни на црниот пазар и оние кои се решени да навлезат во одреден контролен систем би платиле за овие напаѓачки алатки, без разлика колкава е побараната сума за овие механизми за влез во контролните системи.

За надминување на проблемите со сајбер нападот потребно е спроведување на мерки кои се разгледуваат на стратегиско ниво. Комплексните и суптилните проблеми поврзани со сајбер нападот не можат да бидат решени доколку нема активно учество во дискусии од страна на екперти од областа на информациските технологии. Некои од областите каде техничката експериза е неизбежна се:

- Подобрување на способностите за брзо одредување на инволвираните страни во нападот, со цел да се обезбеди навремен и прецизен напад.
- Разбирање и мерење на директните и индиректните ефекти на сајбер нападот; пристапување кон оштетувањата поврзани со директните и индиректните ефекти на сајбер нападите.
- Одредување дали сајбер операцијата е напад или операција – или, поточно кажано, одредување на намерите.
- Обиди да се разбере, преку симулирање на воени игри, како социјалните и техничките системи на Интернет можат да одговорат на различни напади и правокации, како сајбер нападите можат да излезат од контрола.
- Разбирање на релацијата помеѓу времето на обновување и вредноста на нападот – напаѓачот е помалку мотивиран да ја оневозможи мрежата ако жртвата истата многу брзо ја оспособува.
- Пронаоѓање на ефективни мерки за сместување или откривање на Тројанци и други форми на malware-и.
- Искористување на ефектите на виртуелизација во зголемување на способностите за извршување, детектирање и спротиставување на нападот.
- Разбирање и минимизирање на ризиците воведени со развојот или употребата на сајбер напаѓачките и експлоатирачките способности.
- Разбирање и објаснување на импликациите на новите технологии – како тие можат да бидат нападнати или како истите можат да бидат искористени за извршување на напад или експлоатација.

- Одредување на барањата за добивање на добри индикации и предупредувања за сајбер нападот – дали е потребно да се навлезе во мрежата на противникот за да се добие навремена информација за ефикасен и навремен одговор?

Проучувањето на овие области е значајно за подобра одбрана. Не е можно да се изгради јака безбедност без да се разбере во детали функционирањето на еден напад и ефективноста на истиот.

3. Предлог мерки што треба да се превземат од ИТ професионалците

Како што веќе напоменавме, за да се зголемат познавањата во областа на сајбер нападите, експлоатацијата и одбраната потребна е отворена дискусија од страна на ИТ професиналците на дебати кои ги покриваат овие напади од технички, правен, политички и социјален аспект. Ова може да се реализира на неколку начини и тоа:

- Соработка во истражувањето на различните споменати области и публикување на заеднички резултати.
- Развивање и учество во вежби поврзани со сајбер напад и безбедност; осигурување дека сајбер вежбите ги опфаќаат најновите технолошки достигнувања и ограничувања.
- Учествување во групи кои ги адресираат прашањата поврзани со сајбер нападите, на пример, Асоцијацијата за студирање на сајбер конфликтите, која ги спонзорира состаноците и работните групи на различни теми поврзани со сајбер напад и одбрана.
- Учество во online групни дискусии, како што е CSFI-CWD (Cyber Security Forum Initiative's Cyber Warfare Division) на LinkedIn.
- Учество на конференции како што се InfoWarCon (cyberloop.org) или Конференцијата за сабер конфликти спонзорирана од NATO-акредитираниот Кооперативен center of excellence за сајбер одбрана во Естонија (www.ccdcoe.org)
- Учество во работни групи спонзорирани од владата кои ги разгледуваат прашањата поврзани со сајбер нападите.
- Издвојување на вистината од фикцијата во врска со сториите кои се појавуваат во медиумите, кои многу често, заради публицитет, се обидуваат да ја изобличат вистината.

Иако најчесто овие проблеми се разгледуваат на состаноци и дискусии за сајбер конфликтите на кои се пристапува од легален и политички аспект, сепак, од витално значење е на овие состаноци да присуствуваат и ИТ професионалци, со цел, предлозите кои ќе произлезат на овие состаноци да ги земат во предвид и технолошките аспекти на сајбер војувањето. Дополнително, овие состаноци можат да допринесат за ширење на мрежата

на ИТ експерти кои ја покриваат оваа област, што претставува дополнителен ресурс во зголемување на можноста за поефикасен одговор на сајбер нападите.

Заклучок

Разгледувајќи ги сајбер нападите како акт на војување, сеуште не може со сигурност да се каже дека некоја држава во вистинска смисла е нападната од друга држава со примена на сајбер напад, иако сајбер нападите врз Естонија и Грузија беа блиску до дефиницијата на војување. Ефектите на сајбер нападите можат да бидат катастрофални, исти со ефектите на нуклеарниот напад, но, од друга страна, за разлика од конвенционалните нуклеарни напади, сајбер нападот може од друга страна да нанесе и други штети, како на пример економски штети, без притоа да биде предизвикана загуба на човечки животи.

Со цел да се намалат ефектите на овие напади, во овој труд се предложени ефикасни противмерки од технички аспект, како и предлог мерки за учество на јавни дебати, состаноци и работни групи, со цел споделување на проблемите и предлозите на одредени сајбер напади и заеднички одговор на истите.

ЛИТЕРАТУРА

1. “GCHQ chief reports 'disturbing' cyber-attacks on UK”, BBC News UK, 31.10.2011, http://www.bbc.co.uk/news/uk-15516959
2. “Cyber attacks take down two Israeli websites - is cyber warfare the next front in the middle east conflict?”, FORBES, 16.01.2012, http://www.forbes.com/sites/erikkain/2012/01/16/cyber-attacks-take-down-two-israeli-websites-is-cyber-warfare-the-next-front-in-the-middle-east-conflict/
3. “Cyberattacks likely to escalate this year”, US Today, 10.01.2012, http://www.forbes.com/sites/erikkain/2012/01/16/cyber-attacks-take-down-two-israeli-websites-is-cyber-warfare-the-next-front-in-the-middle-east-conflict/
4. “Cyber-attacks now the most feared EU energy threat”, Euractive, 25 January 2011, http://www.euractiv.com/energy/cyber-attacks-feared-eu-energy-threat-news-501547
5. “Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation”, Adopted by Heads of State and Government in Lisbon, November 2010, http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf
6. “A Strong Britain in an Age of Uncertainty: The National Security Strategy, United Kingdom”, October 2010, http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf
7. “National Security Strategy, Unite States of America”, May 2010, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf
8. “International Strategy For Cyberpace, Prosperity, Security, and Openness in a

Networked World", President of the United States, May 2011, http://info.publicintelligence.net/WH-InternationalCyberspace.pdf
9. "Cyber-Attacks Are the Biggest National Security Threat", August 2011, http://www.policymic.com/articles/1519/with-shaky-future-ahead-pakistan-poses-real-danger
10. "Panetta: Cyber warfare could paralyze U.S.", CBS News, 5 January 2012, http://www.cbsnews.com/8301-18563_162-57353420/panetta-cyber-warfare-could-paralyze-u.s/
11. "FBI ranks cyber attacks third most dangerous behind nuclear war and WMDs", TD Daily, 7 January 2009, http://www.tgdaily.com/security-features/40861-fbi-ranks-cyber-attacks-third-most-dangerous-behind-nuclear-war-and-wmds
12. "Global Risks 2012 Seventh Edition, An initiative of the Risk Response Network", World Economic Forum, 2012, http://reports.weforum.org/global-risks-2012/
13. "Investigating Cyber Security Threats: Exploring National Security and Law Enforcement Perspectives", Frederic Lemieux, Report GW-CSPRI-2011-2, 7 April 2011, http://www.cspri.seas.gwu.edu/Seminar%20Abstracts%20and%20Papers/2011-2%20Investigating%20Cyber%20Security%20Threats%20Lemieux.pdf
14. "Worst cyber attack on US military came via flash drive," PHYSorg.com, 25 Aug 2010, http://phys.org/news201978152.html
15. Митко Богданоски, Александар Ристески, Марјан Богданоски "Индустриски сајбер напади – глобална безбедносна закана", Интернационална конференција "Лицата на кризата", Скопје, Март 2012
16. W.A. Owens, K.W. Dam, and H.S. Lin, Eds. "National Research Council. Technology, Policy, Law, and Ethics Regarding U. S. Acquisition and Use of Cyberattack Capabilities", National Academic Press, 2009. http://www.anagram.com/berson/nrcoiw.pdf