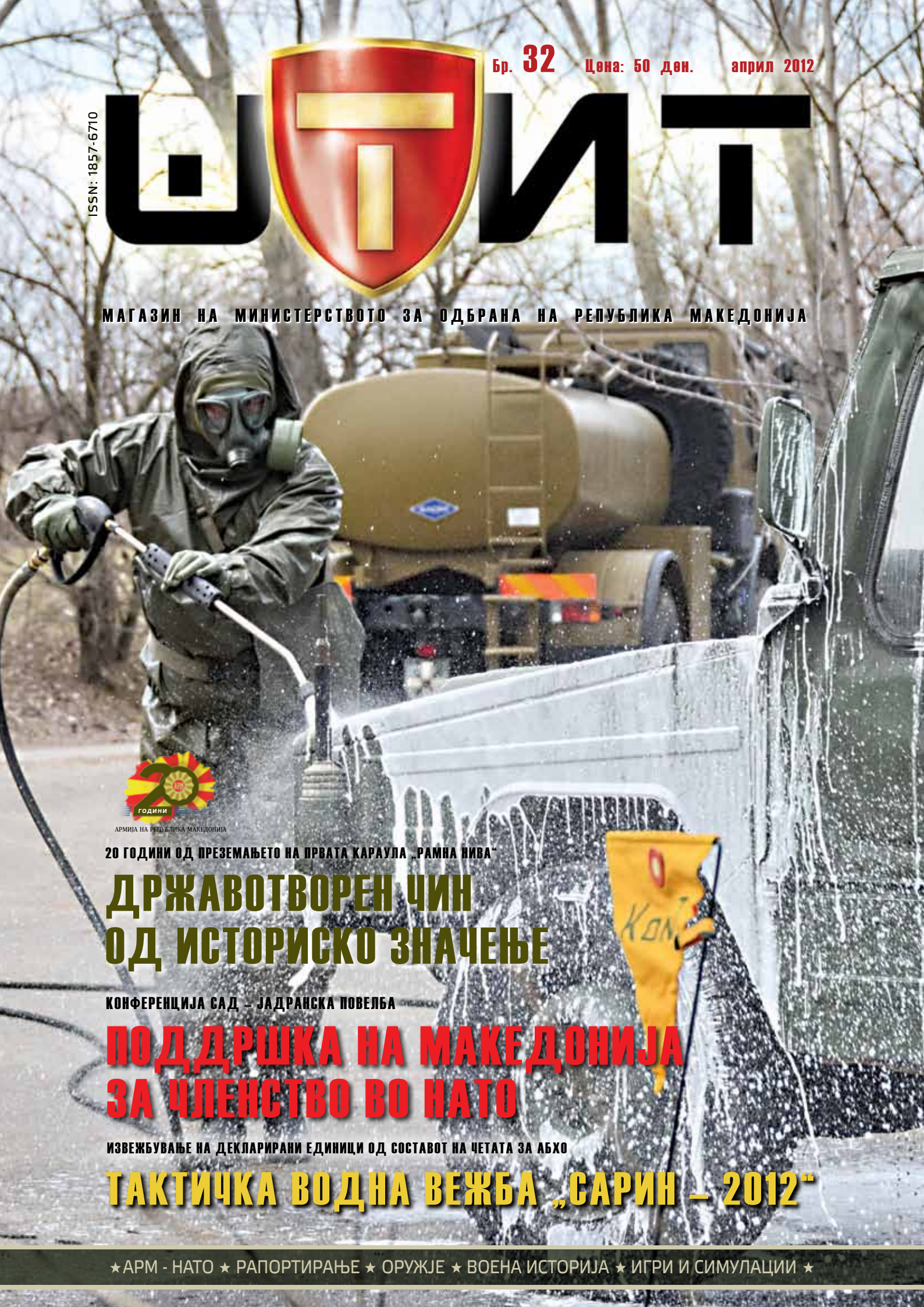
Бр. 32 Цена: 50 ден. април 2012

ISSN: 1857-6710

ОДИТ

МАГАЗИН НА МИНИСТЕРСТВОТО ЗА ОДБРАНА НА РЕПУБЛИКА МАКЕДОНИЈА



20 ГОДИНИ АРМИЈА НА РЕПУБЛИКА МАКЕДОНИЈА

20 ГОДИНИ ОД ПРЕЗЕМАЊЕТО НА ПРВАТА КАРАУЛА „РАМНА НИВА“

ДРЖАВОТВОРЕН ЧИН ОД ИСТОРИСКО ЗНАЧЕЊЕ

КОНФЕРЕНЦИЈА САД – ЈАДРАНСКА ПОВЕЛБА

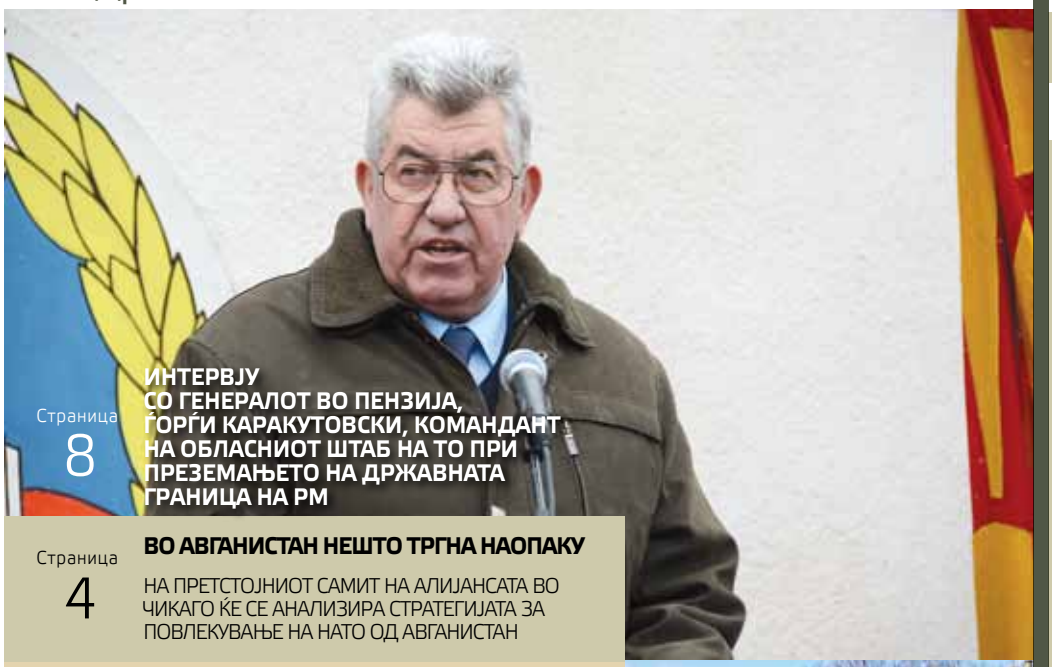
ПОДДРШКА НА МАКЕДОНИЈА ЗА ЧЛЕНСТВО ВО НАТО

ИЗВЕЖБУВАЊЕ НА ДЕКЛАРИРАНИ ЕДИНИЦИ ОД СОСТАВОТ НА ЧЕТАТА ЗА АБХО

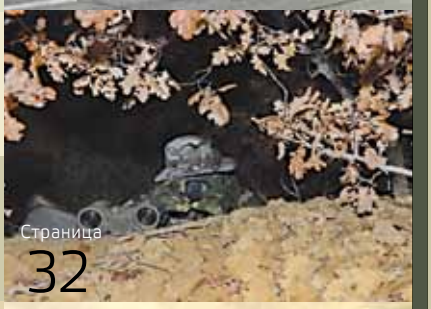
ТАКТИЧКА ВОДНА ВЕЖБА „САРИН – 2012“

★АРМ - НАТО ★ РАПОРТИРАЊЕ ★ ОРУЖЈЕ ★ ВОЕНА ИСТОРИЈА ★ ИГРИ И СИМУЛАЦИИ ★

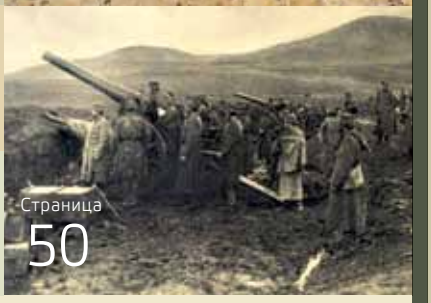
Содржина:



Страница 11



Страница 32



Страница 50

ШТИТ - Година IV, број 32, април 2012 година, излегува еднаш месечно
ИЗДАВАЧ - МИНИСТЕРСТВО ЗА ОДБРАНА НА РЕПУБЛИКА МАКЕДОНИЈА

ИЗДАВАЧКИ СОВЕТ
Емил Димитриев (претседател)
Генерал-мајор Насер Сејдини, Селвет Барути, полковник Мирче Ѓоргоски, потполковник Здравко Ризовски, потполковник Мери Ринџова, проф. д-р Ѓорѓи Малковски

ГЛАВЕН И ОДГОВОРЕН УРЕДНИК
Здравко Ризовски, потполковник

РЕДАКЦИЈА
Васил Дичевски (новинар-уредник), Кристина Илиевска (новинар-уредник), Билјана Иванова (технички, ликовно-графички уредник); Иван Петрушевски (новинар); Ксенија Митева-Котеска (лектор); Александар Атанасов (фотографии)

Печати: „СТЕДА ГРАФИКА“ – Скопје

АДРЕСА НА РЕДАКЦИЈАТА
МИНИСТЕРСТВО ЗА ОДБРАНА - СПИСАНИЕ „ШТИТ“
ул. „Орце Николов“ бб 1000 Скопје
Телефони: 02 328 24 17; 02 3128 276
Факс: 02 3113 527
www.morm.gov.mk; E-mail: stit@morm.gov.mk

ЦЕНАТА НА ЕДЕН ПРИМЕРОК Е 50 ДЕНАРИ
ГОДИШНА ПРЕТПЛАТА 600 ДЕНАРИ

жиро с-ка 0500100116787 20
(повикување на број: 725939-10)
даночен број: 4030990271748
ТС 100000000063095

ВАЛОРИЗАЦИЈА НА СРАБОТЕНОТО

Во пресрет на претстојниот Самит на НАТО во Чикаго, Владата на Република Македонија преку ресорните министри за одбрана и за надворешни работи, Фатмир Бесими и Никола Попоски, ја интензивираше дипломатската активност со цел на претстојниот самит на Алијансата нашата земја конечно да добие валоризација на досега сработеното, односно полноправно членство во северноатлантското семејство.

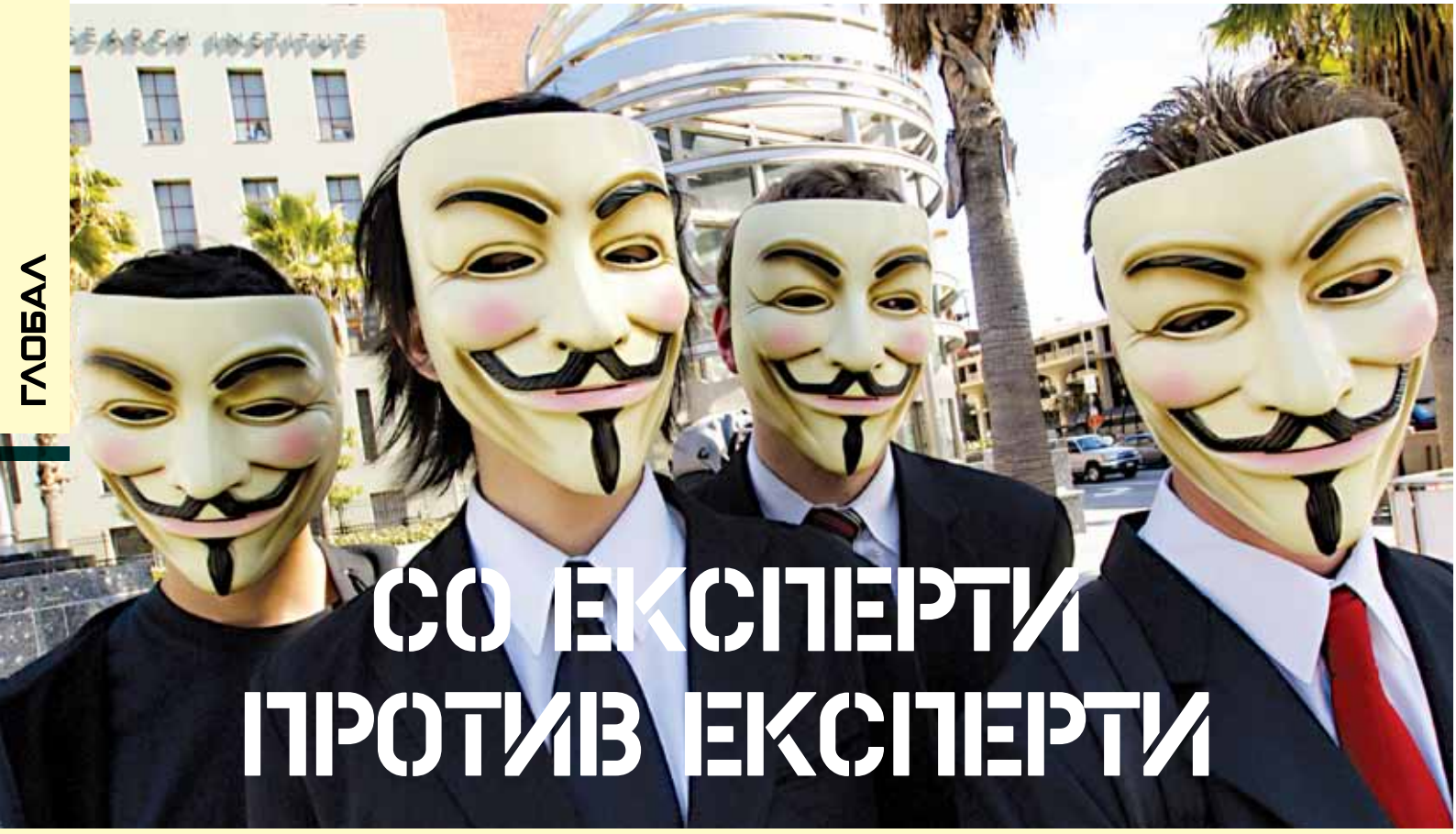
„Нашата основна порака е да ги информираме нашите партнери дека не отстапуваме од нашата стратегиска определба и цел за која постои широк политички консензус – да станеме полноправна членка на НАТО-алијансата“, истакна министерот за одбрана Бесими, оценувајќи ги досегашните и идните активности кои треба да дадат придонес кон евроатлантските интегративни процеси со кои уште еднаш ќе се укаже на придонесот кој Република Македонија го дава кон глобалната безбедност.

Сепак, очите на главните играчи на светската и на европската мапа се вперени кон надминувањето на спорот за името со нашиот сосед. Со неодамнешната пресуда на Меѓународниот суд во Хаг недвосмислено беше потврдено дека Република Грција неоправдано го попречува нашето членство во евроатлантското семејство под привремената референца со која сме примени во ООН. Затоа Република Македонија со право лобира кај своите партнери и поддржувачи на претстојниот Самит на НАТО да биде валоризирана хашката пресуда и со тоа нашата земја да го добие своето заслужено место во Алијансата. Оценувајќи го овој неоправдано наметнат спор за името со нашиот јужен сосед, македонскиот министер за одбрана, користејќи се со спортски речник, оцени: „Ова е маратон кој бара кондиција и истрчување до крај. Ние треба да сме доследни на нашите цели и не треба да се откажеме, бидејќи забрзувањето на процесот на интеграција е добар за целиот регион“, додавајќи дека токму тоа е видливо и преку фактот дека минатата декада НАТО во голема мера бил присутен во регионот, но во исто време преку активностите на групата А-3, односно А-5 под покровителство на САД, од нејзиното формирање до денес земјите-членки од регионот континуирано придонесуваат кон глобалната безбедност во светот.

Доказ за тоа дека Република Македонија е целосно посветена на реформите за исполнување на критериумите и стандардите за членство во НАТО е и почетокот на практичната имплементација на новата организациско–формациска структура на АРМ според стандардите на Алијансата. Имено, со указ на претседателот на Република Македонија и врховен командант на вооружените сили, д-р Ѓорге Иванов, во согласност со новата организациско-формациска структура на АРМ, за нов директор на ГШ на АРМ е поставен бригадниот генерал Димче Петровски, нов командант на Здружената оперативна команда е бригадниот генерал Методија Величковски, а началник на штабот во ЗОК е полковникот Мухамет Рацај, додека за нов командант на Првата механизирана пешадиска бригада е поставен полковникот Стојан Димчов.

Засилените активности за промоција на значењето на евроатлантските интеграции за регионот продолжуваат со ненамален интензитет. Покрај другите, една од главните активности беше и Конференцијата на министрите за одбрана на земјите од Јадранската група каде домаќин беше нашата земја и на која стана збор за глобалната економска криза и нејзините импликации врз регионалната безбедност, енергетската безбедност, имплементацијата на концептот „паметна одбрана“и сл.

Здравко Ризовски



СО ЕКСПЕРТИ ПРОТИВ ЕКСПЕРТИ

ОДБРАНАТА ОД САЈБЕР-ЗАКАНИ Е НА ВРВОТ НА БЕЗБЕДНОСНИТЕ АГЕНДИ НА ДРЖАВИТЕ-ЧЛЕНКИ НА НАТО

Најновите национални стратегии за безбедност на повеќето државичленки на НАТО, покрај заканите од тероризам, војни и случајни или елементарни непогоди, на врвот на своите безбедносни агенди ги поставуваат сајбер-заканите, како закани по безбедноста на своите влади. Меѓутоа, во однос на степенот на сајбер-заканите, многу од државите не се во можност да одвојат доволно ресурси за справување со нив.

Тоа е новата технологија на дваесет и првиот век која се шири со неверојатна брзина. Веќе во многу аспекти модерниот живот се потпира на сајбер-просторот. Во текот на изминатата деценија компјутерските системи и интернетот станаа од витално значење за непречено функционирање на владите, индустријата, финансиите и на нашите секојдневни животи како индивидуи. Тие се користат за комуникација, за контрола на критичната национална инфраструктура и за справување со глобалните финансиски трансакции.

Затоа, обезбедувањето на сајбер-просторот е многу важно. Во изминатите години како ризик беше на пониско ниво на безбедносните приоритети, но сега со право е префрлен во врвот, на ниво заедно со тероризмот, меѓународна воjна, хаварија или опасности како што се поплави или пандемија на грип.

Во многу погледи сајбер-заканата е попредвидлива во однос на другите закани и истата може да се реши. Она што е потребно се експерти со врвен компјутерски квалитет. Меѓутоа, и огромните финансиски средства кои ги издвојуваат европските држави (како, на пример, Велика Британија којашто издвојува 500 милиони евра), не можат да бидат доволни. Тоа е мала сума во споредба со милијардите долари кои САД ги инвестира секоја година во сајбер-безбедноста.

САД веќе има стотици на високо ниво обучени компјутерски експерти кои работат на решавање на проблеми од сајбер-безбедноста. Велика Британија сајбер-безбедноста ја менаџира со неколку десетици вработени во Управата за сајбер-безбедност во владиниот кабинет и од страна на Оперативен центар за сајбер-безбедност (OSOC). Наскоро во Велика Британија ќе се формира Национална агенција за сузбивање на криминал во која ќе има сајбер-тим кој ќе се користи за обезбедување на критичната национална инфраструктура, на пример, на централи и транспортни системи.

ДОЛГОРОЧНИ САЈБЕР-ЗАКАНИ

На скалата на ризици непобитен е фактот дека сајбер-заканите се наоѓаат на врвот. Постојат силни докази дека групи на криминалци, терористи и шпиони имаат сè повеќе можност стручно да го користат сајбер-просторот, во време кога многу земји сè повеќе се зависни од користење и функционирање во сајбер-просторот.

Денис Блер, директор на американското национално разузнавање ја предупреди комисијата на Сенатот на САД дека оваа година „има појава на сомнителни интернет-активности од невиден размер со извонредна софистицираност". Тој, исто така, предупреди дека „Ал Каеда" интернетот го користи како оружје, но дека има и докази за широко распространет, државно спонзориран сајбер-напад, со цел здобивање економски и индустриски предности.

Шефот на британскиот владин штаб за комуникации (GCHQ), Јан Лобан, предупреди дека Велика Британија се соочува со „вистинска и веродостојна" закана од сајбер-напад, со акцент дека не се работи само за прашања од интерес за националната безбедност и одбраната. Тој изјави дека заканата оди до срцето на економската благосостојба и највисокиот национален интерес на Велика Британија. Според него, секој месец на владините мрежи има повеќе од 20.000 „злобни" e-mail од кои 1.000 се намерно насочени против нив. Дури 80 проценти од заканата за владините компјутерски системи би можеле да се решат со стручни и искусни експерти, но 20 проценти од заканите се покомплексни и не можат да се решат толку едноставно поради што е потребна надградба на повисока безбедност сајбер-ѕидови.

Директорот на Управата за сајбер-безбедност, Нил Томпсон, предупреди дека „траекторијата на ризикот на сајбер-безбедноста се движи во погрешна насока", нагласувајќи дека криминалците напаѓаат онаму каде што се парите – бесконечно користејќи го интернетот за бизнисизмами кон поединци за стекнување на готови пари преку непостоечки лажни идентитети.

Клучна точка се 90 проценти од корисниците коишто користат кредитни и други картички и кои работат низ сајбер-просторот.

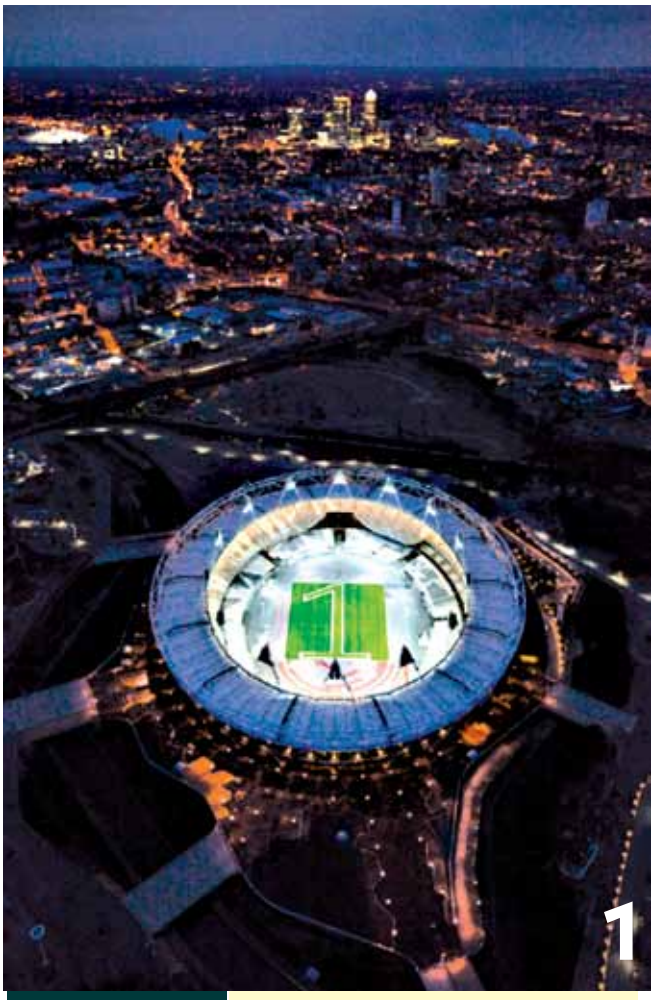
Речиси 65 отсто од семејствата се поврзани на интернет. Бизниси и енергија, храна и други ланци на снабдување сè повеќе се потпираат на сајбер-комуникации и трансакции. Сајбер-кражбите (како што е крадење пари со замена на идентитетот на луѓето со цел префрлање и трансакција на пари од големите компании) се проценува дека изнесува 52.000.000.000 евра годишно на глобално ниво.

Намалувањето на сајбер-криминалот ќе донесе значителни економски придобивки. Просечната цена за безбедноста на информациите во една мала фирма е од 10.000 – 20.000 евра. За една голема компанија, со повеќе од 500 вработени, тоа може да биде 1-2 милиони евра.

САЈБЕР-ШПИОНАЖА

Заканите одат пошироко. Бројот на обидите да се пробие во владиниот, во воениот или во индустрискиот сајбер-систем се зголемува. Ова се должи на државите-спонзори на сајбер-шпионажата. Во 2007 година, кога на чело на Британската разузнавачка служба МИ5 беше Џонатан Еванс, тој предупреди дека во тоа време во Велика Британија околу 300 индустриски бизнис-тајни биле нападнати од страна на Кина. Веб-сајтот на МИ5 предупредува дека денес Велика Британија сè уште е „висок приоритет и цел на шпионажа" на странски разузнавачки служби кои се фокусирани на трговските претпријатија многу повеќе отколку во минатото. Се проценува дека најмалку дваесет странски разузнавачки служби работат до одреден степен против интересите на Велика Британија. МИ5 најмногу е загрижена од делувањето на руски и на кинески шпиони.

Се претпоставува дека во текот на следните пет до десет години НАТО-сојузниците ќе станат многу чувствителни на сајбер-криминалот и на сајбер-нападите кои можат да бидат извршени од страна на државни или недржавни актери, а ќе биде многу тешко да се следи нивната трага. Притоа, се претпоставува дека доколку се изведе успешен сајбер-напад од големи димензии врз сојузник на НАТО, последиците и нанесената штета од овој напад би можеле да доведат до финансиска катастрофа како при нападите од 11 септември. Денес инцидентите од сајбер-нападите се сè повеќе видливи. Кина неодамна ги обвини САД за поттикнување на немирите во Иран преку сајбер-активности – преку интернет-сајтови како што се Facebook и Twitter. Работата во една од нуклеарните централи во Иран неодамна беше нарушена низ сајбер-напад – во британскиот весник „RUSI" се шпекулира дека тоа е дело на сајбер-специјалисти на САД и на Израел. Како што забележува весникот, зголемените сајбер-активности насочени кон одредени држави, го зголемуваат стравот дека таквите напади ќе предизвикаат сајбер-војна – државите ќе се сведат на одбрана од заканите применувајќи контра сајбер-напади.



1. КРИМИНАЛЦИТЕ СЕ ПОДГОТВУВААТ ЗА ОЛИМПИСКИТЕ ИГРИ ВО ЛОНДОН, А НЕКОЛКУ ВЕБ-САЈТОВИ ВЕЌЕ ВЕТУВААТ БИЛЕТИ ШТО НЕ ПОСТОЈАТ

2. ДЕНЕС ИНЦИДЕНТИТЕ ОД САЈБЕР-НАПАДИТЕ СЕ СÈ ПОВЕЌЕ ВИДЛИВИ, ПОСЕБНО ВО АРАПСКИОТ СВЕТ

САЈБЕР-ЗАКАНА ЗА ОЛИМПИСКИТЕ ИГРИ

За Владата на Велика Британија постои уште една, многу голема причина зошто е крајно време да се фокусира на сајбер-заканите. Нејзината сајбер-безбедност мора да биде флексибилна во пресрет на Олимписките игри во Лондон 2012 година. Извршување на терористички и на криминални напади, како и евентуални природни катастрофи, би можеле да предизвикаат значителни сајбер-проблеми. Успешен непријателски сајбер-напад во целост може да го попречи контролирањето на билетите и на транспортната мрежа за опслужување, како и да ја спречи доставата на храната и на енергијата и да ги блокира патиштата за снабдување. Нападот би можел да има негативен ефект и би можел да влијае на компјутерските системи кои се занимаваат со функцијата на спортски настани, а тоа би можело да го фрли Лондон во темнина. Дури и некои планови за контрола на црвеното светло на семафорите, за непречено движење на спортистите и олимпискиот факел, би можеле да бидат загрозени.

Најверојатниот ризик е компјутерската сајбер-измама со билетите за игрите. Во ноември 2009 година британското списание „Which? Computing" објави: „Криминалците се подготвуваат за настанот Олимписки игри, а неколку веб-сајтови веќе ветуваат билети што не постојат." Очигледно е дека една силна држава како што е Велика Британија не е во можност да ги спречи овие несакани сајбер -криминални дејства. Треба да се има многу посилна законска регулатива во оваа област за да се запре сајбер-криминалот.

ЗАКЛУЧОК

Предупредувањата за зголемување на сајбер-заканите биле сфатени многу несериозно во изминатите години. Владите во современите општества веќе го истакнуваат овој проблем и одвојуваат дополнителни ресурси за решавање на истиот. Исто така се предупредува и приватниот сектор, не само поради приватните бизниси, бидејќи внесувањето на нови познавања за сајбер-просторот во приватниот сектор ќе биде од витално значење за одржување на безбедноста.

Предизвик ќе биде да се убедат приватните бизнисмени да склучуваат договори со владите, без да се поткопуваат сопствените комерцијални интереси, а притоа заеднички да ги надминуваат заканите од сајбер-криминалците. Исто така, владите треба да остваруваат меѓусебна интензивна соработка и размена на разузнавачки информации за што поефикасно справување со злонамерните хакери кои ги контролираат сајбер-мрежите низ цела Европа. Исто така ова би требало да вклучи дипломатска акција од страна на земјите-потенцијални поддржувачи на сајбер-криминалот и нивно убедување да станат рамноправни партнери во борбата на овој фронт.

м-р Ненад Танески