МИЛОВАН Б. ЈОВАНОВИЋ*
Правни факултет за
привреду и правосуђе
Нови Сад

УДК 004.738.5:316.77
Монографска студија
Примљен: 29.08.2014
Одобрен: 18.09.2014

ИНТЕРНЕТ И ТЕРОРИЗАМ

Сажетак: Медији су данас веома снажан фактор политичке и друштвене моћи али и чинилац који у великој мери обликују светску демократију и јавно мњење. Креирајући политичку вољу, ставове, потребе и навике, медији све више обликују понашање појединаца, група и маса који истину и стварност схватају и виде онако како им медији то сервирају.Сходно томе, данас су све чешће дискусије о односу медија и тероризма, публицитета и пропаганде. Говорећи о масмедијима, не можемо а да се не осврнемо на интернет, његов значај и улогу у животу сваког појединца данас, а која је све већа из дана у дан. Развој технологије за терористе отвара нове могућности у реализацији њихових циљева. У савременим условима глобализације интернет, као један од облика нових комуникационих технологија, постаје моћно оружје у рукама терористичких организација. Интернет и савремене технологије доносе многе погодности савременом човеку али нажалост и терористима.Неопходно је истаћи велику улогу интернета као медија у промовисању тероризма али и интернета као моћног оружја у рукама терориста путем којег се врши регрутовање нових кадрова и прикупљање средстава за нове активности. Мрежа комуникација преко рачунара идеална је за терористе због тога што се интернет, који нема централизовано управљање, не може у потпуности контролисати. Традиционални тероризам замењује полако кибер (cyber)t тероризам који подразумева различите злоупотребе рачунарских система које се односе на: крађу података и „обарање" веб страница, планирање терористичких напада, изазивање насиља и страха код цивила или напад на организационе системе. За кибер-терористу, рачунарска мрежа представља оружје, медијум или циљ. У циљу ефикасније борбе против тероризма, данас се улажу велики напори да се контрола Интернета бар до некле учини могућом. Оно чега морамо бити свесни је да кибернапади постају реална опасност друштву на коју исто нема адекватан одговор.

Кључне речи: медији,интернет, комуникација, технологије, тероризам, кибер-тероризам

---

* miki80miki@gmail.com

Уводна разматрања

Услови глобализације допринели су да било који догађај на једном делу планете готово истовремено постаје познат људима на скроз другом делу планете. Највећи допринос томе дали су медији и савремене технологије без којих све наведено не би било могуће. Пропаганда, као један од најснажнијих инструмената савременог света[1], представља битно оружје којим се служе терористичке организације. Већина грађана никада није у контакту са било којим обликом терористичког насиља, већ га постаје свесна једино посредством медија.[2] Говорећи о масмедијима, не можемо а да се не осврнемо на интернет, његов значај и улогу у животу сваког појединца данас, а која је све већа из дана у дан. Развој технологије за терористе отвара нове могућности у реализацији њихових циљева а у савременим условима глобализације интернет, као један од облика нових комуникационих технологија, постаје моћно оружје у рукама терористичких организација. Поред тога што доносе многе предности савременом човеку, интернет и савремене технологије самим тим доносе и терористима а они који шире екстремистичку пропаганду путем интернета и регрутују нове чланове имају слоган: ‘‘Тастатура = Калашњиков”.[3] Овај слоган говори много тога и може се тумачити на разне начине. Тако, са једне стране, путем интернета терористи *размењују информације* везане за оружје и тактику регрутовања, планирају нападе, врше пропаганду и међусобно кумуницирају. Са друге стране налази се сајбертероризам где уз помоћ интернета терористи могу да ометају авионску контролу и да изазову сударе авиона, могу да оптерете телефонске линије, да искључе електричну енергију, саботирају финансијске системе итд. Информативна револуција је допринела настанку једног новог виртуелног простора чијих могућности и предности су врло брзо постали свесни и сами терористи.

Познато је да је Осама Бин Ладен комуницирао са припадницима Ал Каиде са покретних компјутера и помоћу бежичне мреже путем енкриптованих порука које су заштићене од нежељеног читања. Терористи првенствено користе мејл адресе у својој комуникацији и то на начин да садржаји остану недоступни обавештајним службама. Обавеш-

[1] Савић , А., *Основни концепт пропаганде у савременом свету*, Безбедност бр. 3, 1986., стр. 212.

[2] Ђурић-Атанасиевски, К, *Утицај медијског извештавања о тероризму на јавност и доносиоце политичких одлука*, чланак у часопису Војно дело, vol. 62, бр. 4., Војна академија, Београд, 2010., стр. 357-358.

[3] http://www.muskimagazin.com/2012/01/25/terorizam-i-internet-tastatura-kao-kalasnjikov/, Доступно: 7.7.2012.

тајне службе могу само надзирати промет између тачно одређених адреса, тј. пошту која кружи мрежом. Али ако нема промета ка другим адресама, ове службе су немоћне. Зато терористи отварају мејл налоге; деле шифру међусобно и остављају једни другима поруке у тзв. скицама (драфтс). Како нема слања ка другим адресама, комуникација је сигурна и тајна! Данас се као средство за ширења својих идеја користе сва достигнућа интернета, међу којима се посебно истичу и програми за "чаврљање" (ИРЦ - *Internet Relay Chat*), који омогућавају непосредно комуницирање у реалном времену, чиме се омогућава непосредна повезаност. Ово даље значи да чланови терористичких организација могу синхронизовати своје деловање пред акцију, и/или добити повратну информацију одмах.[4] Интернет као мрежа представља изум војске САД-а из времена хладног рата када је Пентагон тражио метод да усаврши један неуништиви облик комуникације, који ће моћи да одоли атомском нападу и који би преживелим политичким и војним руководиоцима омогућио да међусобно комуницирају и организују против напад. Тај облик комуникације нема централну власт, дизајниран је у виду рибарске мреже, и ако би било који њен део престао да функционише, она се може преусмерити на остатак који би наставио да функционише као целина.[5] Припадници терористичких организација и оперативних група, данас више него икад, у својој међусобној комуникацији, активно користе интернет и разне сервисе доступне на интернету. Њихови терористички, оперативни, односно заповедни центри комуницирају са оперативним групама, које чине углавном по тројица терориста, преко електронске поште која се проверава преко интернет страна (*webmail*) рачуна које отварају на разним бесплатним, анонимним сервисима за пошту (*yahoo, hotmail, gmail* итд). Обавештајне службе данас расположивом технологијом могу надзирати једино промет између појединих тачно одређених електронских адреса, дакле пошту која кружи мрежом.[6]

Интернет као медиј и оружје у служби тероризма

Интернет представља погодно тле за различите облике злоупотреба. Терористима је Интернет доступан, баш као и свима нама. Користе

[4] http://www.muskimagazin.com/2012/01/25/terorizam-i-internet-tastatura-kao-kalasnjikov/, Доступно: 7.7.2012.
[5] Петровић , С, *Компјутерски криминал*, Војноиздавачки завод, Београд, 2001., стр. 64
[6] Опширније видети: Зиројевић Фатић М, Злоупотреба интернета у терористичке сврхе, МП 3, 2011. стр. 417–448.

га као оружје, као начин комуникације и обраћања јавности. Путем Интернета терористи регрутују нове чланове и прикупљају финансијска средства за финансирање својих терористичких активности а интернет је и бојно поље у коме је могуће извођење терористичких активности.Оно што је посебна предност интернета као медија у односу на друге облике масмедија је и чињеница да интернет кориснике снабдева визуелним предностима телевизије са једне стране, али и интерактивним погодностима телефонског система, као облика директне комуникације, са друге стране. То га, дакле, чини веома привлачним за терористе, који користећи предности и телевизије и телефонске комуникације успевају брже и непосредније доћи до жељене публике. Терористи тако користећи неограничен простор, пропагирају своје идеје, објављују приручнике за деловање, упутства за акције и саопштења за јавност, чиме интернет стављају у службу ширења страха и панике, као што су то одавно телевизија, радио и штампани медији. Бројне терористичке организације су укључене на Интернет и имају своје веб стране а међу њима су: Хамас, Хезболах, ЕТА, Исламска група, Албанска национална армија (АНА), Ирска организација (ИРА), Ослободилачка војска Прешева, Бујановца и Медвеђе итд. Ослободилачка војска Прешева, Бујановца и Медвеђе, која је огранак „ОВК" и тежи отцепљењу тог дела Србије и његовом припајању Косову и Метохији, нема независан сајт, већ се информације о тој организацији могу наћи на сајтовима других терористичких организација које делују на том простору.[7] Албански терористи на Интернет мрежи имају око хиљаду петстотина веб страница, већина њих се крије иза веб страница различитих хуманитарних организација. Да бисте дошли до веб странице АНА, треба да отворите страницу хуманитарне организације „Албанци заједно" и да преко ње дођете до албанске терористичке организације. Најпопуларније веб странице којима албански терористи врше пропаганду својих идеја о политичком насиљу су „Бали комбетар", АСХК и „Алабанско-америчка лига" (веб страница албанског лобија у САД).

Креатори интернет презентација терористичких организација осим текста, обилато користе и графику и визуелни елементе (слике, филмови...). Све организације имају амблеме на својим почетним странама (тзв. Home page). Неки сајтови посетиоцима чак нуде да „скину" амблеме (Download). Иако интернет стране уобичајно скривају насилну природу терористичких организација и наглашавају њихову наводну мирољубиву природу, пацифистички приступ проблему није приказан

[7] Зиројевић, М, *Терористичке организације и интернет*, Војно дело бр. 1, Војна академија, Београд, 2004., стр.94

на амблемима. Симболи приказују оружје или друге елементе који означавају насиље. На интернет страни Хезболаха можемо видети нож са кога капље крв. „Обасјана путања" и ИРА приказују маскиране војнике који витлају оружјем, Кахане има подигнуту песницу. Интернет презентација Ослободилачке војске Косова је у црној и црвеној боји, са сликама наоружаних војника уз звуке корачнице, док интернет презентација Тупак Амару и Националне армије ослобођења Колумбије показују подигнуту пушку. Неки од ових симбола су постојали пре него што се појавио интернет и зато се њихово значење не може представити као ненасилно. Заставе организација (или слични национални симболи) се, такође, редовно појављују на овим странама. Пракса да се преводе садржаји који имају најмање елемената насиља, може се тумачити као улагивање западној јавности. Нетекстуални делови, као на пример песме и говори, ипак су намењени домаћој јавности.

Редован елемент интернет страна терористичких организација представља одељак са говорима и текстовима лидера, оснивача и идеолога. Овде можемо запазити обиље званичних докумената који се могу и претраживати по наслову у датуму. Интернет презентације Тупак Амару и запатиста омогућавају овакво претраживање. Они чак и позивају посетиоце да копирају, преводе, штампају и деле ове материјале уз образложење да „они представљају рад главне команде и сајт нема апсолутна право на ауторска права". Презентација турске Народне револуционарне партије/Фронта ослобођења нуди говоре и преводе одељака из књиге једног од лидера. Сајт Хамаса обезбеђује и линкове на којима се може наћи превод интервјуа шеика Јасина (*Yassina*) арапској радио станици и новинама. „Обасјана путања" дозвољава приступ памфлетима, а ФАРЦ има и писма.[8] Кахане садржи недељне колумне у којима Бенџамин Зејев Кахана тумачи Тору. Уопште, креатори интернет страница терористичких организација се труде да на овај начин поделе материјале кроз медије и да допру до најшире јавности. Поједине презентације постају праве кућне продавнице преко којих се могу наручити књиге, видео и аудиокасете, налепнице, штампане мајце и беџеви са знацима организације.

Једна студија овог феномена, на коју се позива Ројтерс, наводи преко 5000 Интернет сајтова који шире идеологију Ал Каиде. Интернет провајдери затварају џихадистичке веб сајтове кад год их лоцирају, али они се појављују негде другде, под другим именом.Иначе, данас најпознатија терористичка организација на свету, интернет је открила мало

[8] http://www.csrp.org/index.html, Доступно: 7.7.2012.

касније, тек када је протерана из Авганистана. Под талибанском страховладавином у овој земљи једва да је било и струје, па је можда и разумљиво кашњење Ал Каиде да препозна овај медиј као користан. А онда постављају многе пропагандне филмове и снимке, од којих је најшокантнији онај на ком се види одрубљивање главе Американца, Ника Берга. Слање снимака арапској телевизији Ал Џазира сада мења постављање на сопствене интернет стране. Синоним за Ал Каиду на интернету биле су интернет странице Alheda.com и Jehad.net.[9] Главни штаб Ал Каиде, шаље своје редовне видео „билтене" на којима маскирани џихадиста у студију набраја постигнућа са многих фронтова, од Ирака до Чеченије, уз навођење броја убијених Американаца.Сајтови терористичких организација не садрже само текст, већ користе и графику и визуелне елементе (слике, филмове...). Схвативши важност слика Абу Мусаб Ал Заркави (лидер Ал Каиде у Ираку, убијен 2006.) је својевремено издао наредбу да свака група снима своју операцију и да снимке што пре постави на Интернет. „Више од пола битке се води на бојишту медија", поручивао је он у једном пресретнутом писму. „Будите свесни да је сваки кадар који снимите подједнако добар колико и ракета испаљена у нашег непријатеља и његове марионете".Интернет терористичким групама нуди могућност директне контроле садржаја порука које они желе да проследе јавности. Добро дизајниран веб сајт терористичкој организацији пружа ауру легитимности, посредством сајта терористи промовишу своје активности са отвореним позивом на деловање. У вези са Интернетом, неопходно је поменути и то да данас постоји мноштво Интернет страница које садрже упутства о начину прављења бомби, и то тако да се користе безопасни материјали, чија комбинација резултира бомбом.

Ови сајтови су помогли многим активистима терористичких организација широм света у извођењу својих активности. Поред овога, интернет се широко користи и за регрутовање нових кадрова па терористичке групе развијају различите методе за регрутовање путем мреже. Просек постојања једне терористичке групе је мањи од једне године. Њихов број чланова се смањује услед хапшења, смрти и напуштања терористичке организације. Посредством Интернета терористи привлаче потенцијалне кандидате. Посебно су усмерени на врбовање младих путем компјутерских игрица, цртаних филмова и Интернет причаоница у којима шире своје идеје.

---

[9] http://www.muskimagazin.com/2012/01/25/terorizam-i-internet-tastatura-kao-kalasnjikov/, Доступно: 7.7.2012.

Такозвани „Џихадистички веб портали" и „собе за четовање " погодни су за регрутовање младих муслимана. Поједине веб странице садрже компјутерске игрице за децу које подржавају циљеве појединих терористичких организација. На тај начин, игрице припремају регрутовање нових чланова. Хезболах данас регрутује људе широм европских земаља, циљ је да реорганизују и ревитализују терористичке мреже које је Иран некада имао у Европи. Ако неки од њихових планова успе то може да изазове велике људске жртве. Колика опасност прети, види се у нападу на мадридску приградску железницу 2004. године када је убијено више од сто деведесет људи. Тај напад су извели муслимански досељеници који су полицији били познати као шверцери дроге и ситни криминалци, а нису имали никакве формалне везе са Осамом бин Ладеном. У Великој Британији је први пут у историји њиховог правосуђа изречена казна затвора кибер-терористима. Они су посредством Интернета позивали муслимане широм света да започну свети рат против свих неверника.[10]

Интернет као средство комуникације

У својим активностима терористи интернет користе као средство комуникације а при томе интернет се користи као веза између ћелија често међусобно неповезаних и раширених на великом географском простору. Оваква структура захтева одређен степен заштите група приликом потребе да се комуницира на даљину. Комуникација је неопходна како би припадници терористичких организација испланирали и извршили напад. У комуникацији терористи користе електронску пошту веома често. Разлог томе је и чињеница да ако са одређене електронске адресе нема промета ка споља, ка мрежи, односно према трећим адресама, обавештајне службе данас једноставно немају начина надзирати што се догађа на тим отвореним виртуелним поштанским сандучићима. Корисничке податке, дакле корисничко име и лозинку након отварања такве интернет поште добијају припадници одређене терористичке оперативне групе, те преко поште која се чита искључиво у самом интернет простору (webmail) комуницирају на начин да се та адреса не користи за слање порука трећим особама или на друге адресе, него тројица или више корисника међусобно размењују поруке на начин да поруке остављају у фолдеру означеном као „скице" („drafts"). Како сва тројица има-

[10] Опширније у: Малетић, И, *Допринос медија развоју савременог тероризма и антитероризма*, Криминалистичко-полицијска академија, Београд, 2009.

ју корисничко име и лозинку исте електронске поште која се проверава преко мреже они користе ту адресу и у том фолдеру могу прочитати поруку која им је остављена, а која представља оперативна упутства за поступање или акције те терористичке групе. Ово је данас најчешћи начин на који терористичке групе избегавају надзор обавештајних служби над комуникацијом њихових припадника, а вероватност да ће сигурносне службе открити ову комуникацију је врло мала, с обзиром да би за то службе требале знати тачну адресу, корисничко име и лозинку преко којег се таква комуникација одвија. Други начин, данас врло уобичајен у комуникацији терористичких организација, је комуникација шифрираним порукама преко различитих интернет форума, где терористичке организације у облику шифрираних текстова остављају поруке својим терористичким ћелијама, које их могу тада јавно прочитати. За разбијање и откривање ове комуникације такође је потребно набавити шифрарнике сваке поједине групе како би се такве поруке могле идентификовати и дешифровати. Следећи ниво, односно идентификација корисника који се на одређеним интернет форумима користе таквом комуникацијом у терористичке сврхе је готово немогућа. Као средство за ширења својих идеја користе се сва достигнућа интернета, међу којима морамо посебно истакнути и програме за четовање (ИРЦ) који за сада једини омогућавају непосредно комуницирање међу тачно одређеним корисницима у реалном времену, чиме се омогућава непосредна повезаност. Ово даље значи да чланови терористичких организација могу синхронизовати своје деловање пред акцију, и/или добити повратну информацију одмах (fidbek). Овај метод је релативно сигуран јер безбедносне агенције не могу пратити ове истовремене разговоре на интернету (нема препознавања гласа као код телефона, сви трагови се бришу одмах). Такође, развој посебних типографија који се развијају пре свега међу младим Арапима отежава рад обавештајних агенција. Наиме, користе се посебни знакови (ASCII знакови) који су визуелно веома слични арапским словима, што омогућава споразумевање на рачунарима који не подупиру арапски језик, али исто тако се не приказују као арапски знакови чиме избегавају програмско За размену информација користе заштитни алат у виду дигиталне криптографије. Криптографска техника заштите података треба да обезбеди следеће захтеве:

- Тајност-захтев који обезбеђује да информациони садржај криптографски заштићене поруке буде доступан само овлашћеним корисницима.
- Интегритет-захтев који се односи на могућност откривања неовлашћене промене информационог садржаја поруке.

- Аутентичност-захтев који се односи на могућност утврђивања идентитета учесника у комуникацији.
- Непорицање-захтев којим се спречава могућност порицања реализације одређених активности корисника који учествују у комуникацији.

Коришћење криптоване комуникације путем јавних Интернет сервиса пружа члановима терористичких организација могућност да буду у сталном контакту чинећи њихово откривање и тумачење веома тешким.[11]Постоје две врсте система за криптовање: симетрични и асиметрични систем, при чему је код симетричног система кључ за шифровање идентичан кључу за дешифровање, или се једноставном трансформацијом кључа за шифровање може извести кључ за дешифровање. За асиметрични систем карактеристично је постојање различитих кључева за шифровање и дешифровање тзв. јавни и тајни кључ. Сваки корисник који поседује јавни кључ може да изврши шифровање поруке, док само власник тајног асиметричног кључа може да изврши дешифровање поруке.Чак и мање напредне рачунарске технологије су веома погодне за терористе. Они могу да користе и метод који се назива стеганографија („скривена писмена") да би упаковали поруке у дигиталне слике или мелодије. Те слике и мелодије се постављају на јавно доступне сајтове. Најбаналнији пример стеганографије би био слика преко слике у Power Point презентацији.[12] Говорећи о могућностима интернета у комуникацији, морамо нагласити да он пружа могућност комуникације не само између припадника исте терористичке организације, него и између чланова различитих терористичких група, што омогућава терористима из различитих делова света, као што су Авганистан, Турска, Ирак, Чеченија, Палестина, Индонезија...да размењују идеје, сугестије и практична искуства. То омогућава терористичким организацијама да ојачају и своје дејство глобално прошире а да при томе остану у великој мери латентни. [13]

Интернет и прикупљање средстава за финансирање тероризма

Поред улоге интернета као средства комуникације, овај медиј се веома често користи и за прикупљање ф*инансијских средстава* неопхо-

[11] http://www.doiserbia.nb.rs/img/doi/0025-8555/2011/0025-85551103417Z.pdf, Доступно 8.7.2012.

[12] Кешетовић, Ж, *Интернет као оруђе терориста*, Ревија за безбедност бр. 4, 2008., стр. 40.

[13] Опширније у: Малетић, И, *Допринос медија развоју савременог тероризма и антитероризма*, Криминалистичко-полицијска академија, Београд, 2009.

дних свакој терористичкој организацији како би она уопште могла да постоји и да спроводи своје акције. Интерактивна природа интернет комуникација омогућава терористима да на различите начине дођу до финансијске потпоре, неопходне за извођење активности и свакодневно функционисање. Начини на који то раде су заиста различити али се терористи најчешће путем сопствених веб страница обраћају посетиоцима сајта, али и својим присталицама, упорно их молећи да у најскоријем року донирају њихову организацију - било тако што ће оставити податке банковног рачуна како би организација наплатила донацију, било да изврше уплату посредством интернета. Од оних којима је због неког разлога неугодно да организацију помогну новчано, или то нису у могућности, очекује се да уместо новца доставе неке друге предмете који им могу послужити приликом терористичких напада, укључујући чак и заштитне, војне прслуке и другу опрему. Такође, терористи посредством Интернета продају књиге, аудио и видео касете, заставе, мајице и друге сличне ствари. Познат је случај када је терористичка организација Права ИРА поставила „линк" на једној веб страници истичући да посетиоци који изврше куповину преко овог „линка" помажу затворенике организације Права ИРА. Свака куповина је терористичкој организацији доносила 3%-5% од продајне цене, а сајт је био у обавези да тај износ проследи власницима постављеног „линка". „Линк" је уклоњен новембра 2000. године, врло брзо након што је постављен. Портпарол малопродаје тог сајта је изјавио да ни једна куповина није извршена и да самим тим ова организација нема право на провизију. Албански терористи продају своје књиге посредством књижаре Тоекса. Ове албанске књижаре се налазе на Косову и Метохији, у Македонији, Црној Гори, Албанији и Грчкој, издања ове књижаре се продају и посредством претходно навођеног сајта. Добротворне установе као покриће веома су чест начин долажења до средстава а многе терористичке организације (нарочито класичне исламистичке) се служе управо овим методом. Разлог томе је и обавеза за муслимане да врше донације у добротворне сврхе. У појединим случајевима терористичке организације поседују добротворне установе чија је наводна сврха постојања искључиво хуманитарна. Овакве добротворне установе се, уз саосећајну конотацију, рекламирају - како у новинама, тако и на веб страницама и собама за четовање. Постоје случајеви и када терористичка организација оформи огранак у некој већ постојећој добротворној установи како би на тај начин, тајно скупљала новчана средства па тако донатори веома често и нису упознати са тим где иде њихов новац. Многа истраживања су указала на везу између дечије порнографије на Интернету и терористичких организација. По

неким проценама чак 75% дечије порнографије се дистрибуира путем Интернета, а око 90% свих међународних потерница Интерпола везаних за компјутерски криминал односе се на педофилију. Свака интернет страна са дечијом порнографијом просечно зарађује око 30.000 долара месечно. Финансијска средства добијена на овакав начин користе се за финансирање терористичких организација.[14]

Интернет у борби против кибер-тероризма

Убрзани развој интернета праћен је често и убрзаним развојем начина његове злоупотребе. Тако бројне слабости интернета чине заштиту кључних система тешком, а остављају „широм отворена врата" за различите злоупотребе. Све ово нам говори да је откривање извршилаца терористичких напада у виртуелном простору, веома тешко, јер постоји висок степен дигиталне анонимности, због чега је немогуће утврдити да ли је кибер напад починио терориста, или непријатељски настројена држава, или пак неки дечко.Надгледање електронске поште, репресивни закони и цензура веб страница се пооштравају посебно након 11. септембра 2001. Тада у Америци питање националне безбедности постаје горуће питање информатичког друштва. Донет је закон по ком су провајдери у обавези да чувају све податке о Интернет саобраћају, пошиљаоцу и адресанту електронске поште, посетама веб страницама и по неколико месеци. Међутим, проблем представља општа сигурност коју треба успоставити, која се налази са једне стране, и право на приватност свих грађана које треба поштовати, са друге стране. Постоји опасност увођења репресије услед претеране контроле грађана и драстичних казнених мера. Што се тиче борбе против кибер-тероризма,Министарство унутрашње безбедности САД окреће се заштити критичне инфраструктуре од потенционалних кибер напада након 2001. године и већ поменутог терористичког напада на Њујорк. Одмах након првих телевизијских извештаја многи су похрлили на Интернет како би сазнали више детаља. Поред оних који су били само радознали, хиљаде људи желело је да успостави контакт са својим најближима или пријатељима јер телефонске везе, како мобилне тако и фиксне, није било могуће успоставити. У тим тренуцима дошло је до великог загушења најпознатијих информационих сајтова. *CNN*, MS *NBC* и други били су буквално затрпани посетом тако да се све одвијало веома успорено.Наредних дана, као ваљда и

[14] Опширније у: Малетић, И, *Допринос медија развоју савременог тероризма и антитероризма*, Криминалистичко-полицијска академија, Београд, 2009.

целокупна светска штампа, сајтови су били препуни извештаја са лица места, тужних судбина и оштрих изјава. Могле су се видети стотине слика које су сведочиле о ономе шта се десило: прашина, рушевине, 3-Д прикази причињене штете па чак и сателитски снимци пре и после напада. Међутим, ни на једној од тих слика није се могао видети теже повређен човек или неко од погинулих. Влада САД увела је цензуру која није заобишла ни Интернет. Слике погинулих људи могли сте добити само директно од неког другог корисника Мреже. Колико је то различит принцип од онога што се види на холивудским филмовима и од онога шта смо ми имали прилику да гледамо на нашим програмима током протекле деценије...Наравно, да би се терористи онемогућили у даљим акцијама и прикрили пропусти обавештајних служби, спроведене су опсежне мере које нису заобишле ни Интернет. Из разлога безбедности забрањено је отварање нових налога на свим web е-маил сајтовима (!) а на сајтовима за аукције укинута је продаја било чега што се могло довести у везу са нападима (разлог је вероватно то што су почеле продаје делова WTC-а, баш као што су се некада продавали делови Берлинског зида).У оквиру опсежне истраге једно од првих места на које су агенти закуцали били су Интернет провајдери. И поред тога што су на неким серверима већ били инсталирани озлоглашени програми за праћење електронске поште DCS1000 (некадашњи *Carnivore*), истражитељима су били потребни детаљни дневници (логови) свих активности. Овим је по ко зна који пут нарушена приватност корисника тих провајдера, али и свих који комуницирају с њима. Међутим, многи стручњаци не верују да ће то директно помоћи у проналажењу трагова јер је у питању огромна количина података коју треба анализирати. Само AOL са 31 милионом и Earthlink са 5 милиона корисника чине велики залогај за истражитеље. Занимљиво је да је провајдерима и телефонским компанијама у Уједињеном Краљевству наложено да сачувају све лог-фајлове почев од 11. септембра. Неко ко је био способан да изведе тако синхронизовану и компликовану акцију сигурно је способан и да прикрива комуникацију. Чак и ако разне обавештајне службе успеју да лоцирају потенцијалне терористе и прате њихове комуникације, могу наићи на проблем шифрованих података па чак и говора.Америчке службе располажу подацима да се терористичке организаије са Блиског истока служе управо овим методама.

Тако је Вадих Ел Хаге, један од осумњичених за бомбашке нападе на две амбасаде САД 1998. године, слао криптоване е-маил поруке под разним именима другим припадницима групе Ал Каида за коју се верује да је заправо организација Осаме бин Ладена. Он ће то вероватно разја-

снити пред судом, док ће Калил Дик, терориста ухапшен у Пакистану 1999. године, тешко убедити судије да у свом рачунару није скривао скице бомбашког напада на Јордан. Наиме, његов рачунар је пренет у САД где су математичари уз помоћ суперкомпјутера дешифровали фајлове. Слично њима, Ремзи Јусеф, мозак бомбашке операције у WTC 1993. године, у рачунару је чувао криптоване фајлове у којима су се налазили детаљи планова за уништење једанаест америчких путничких авиона. Рачунар је нађен у његовом апартману у Манили 1995. године, али ФБИ је на декриптовању два фајла радио више од годину дана.Међутим, терористи већ пет година (нарочито од када Американци покушавају да открију локацију Бина Ладена праћењем сателитског телефона који он користи), употребљавају један друкчији начин скривања информација: познате програме чији су аутори борци за слободу приватности и који се могу бесплатно скинути са Мреже. Ови програми криптују податке у оквиру графичких или звучних фајлова не нарушавајући њихову структуру, па чак не мењајући им ни дужину. Тако криптоване информације може прочитати само онај ко зна да такав фајл носи информацију и поседује одговарајући кључ. *iDEFENCE, cyber* обавештајна компанија, сматра да терористи користе овај начин криптовања података, а да „филоване" слике размењују на неком од добро посећених сајтова или чак на неким порно сајтовима. Потенцијално, где год се може послати слика може се пренети и скривена информација. Проблем је у томе што данас на Интернету на две милијарде сајтова има преко 28 милијарди слика! [15]

Године 2003. почиње са радом Дивизија за националну кибербезбедност која функционише у складу са циљевима одређеним Националном стратегијом за обезбеђење кибер простора која је усвојена 2003. године, а садржи основне смернице које се односе на заштиту јавности и привреде од напада на рачунарске системе и телекомуникационе мреже. Ова стратегија одређује пет основних националних приоритета. Први приоритет се односи на унапређење могућности САД да одговори на потенцијалне кибер инциденте, као и на свођење потенцијалне штете која би тим инцидентима настала. Други, трећи и четврти приоритет се односе на смањивање претњи од кибер напада, као и на смањивање укупне рањивости САД услед таквих напада. Пети приоритет се односи на превенцију кибер напада који би угрозили националну безбедност.Оружане снаге САД обезбеђују заштиту својих информационих система стратегијом избегавања ризика. Мрежна структура оружаних снага САД је одвојена од јавног Интернета, приступ средствима се стро-

[15] http://www.sk.rs/2001/10/skin01.html, Доступно 8.7.2012.

го ограничава „закључавањем просторија", омогућава се физички приступ само провереном људству, постоје уређаји за криптозаштиту а САД су такође формирале и Центар за заштиту националне инфраструктуре који запошљава више од 500 експерата из ЦИА, НАСА, НСА. Под њиховом присмотром се налазе телекомуникације, енергија, банкарство и финансије, системи за снабдевање водом, систем за контролу ваздушног саобраћаја и владин сервис и сервис за ванредне ситуације.Исто тако, поједине владине организације у САД су формирале своје групе да се баве кибер-тероризмом.[16] ЦИА је формирала сопствену групу Центар за информационо ратовање са око хиљаду људи и двадесет четворочасовним радом. ФБИ истражује хакере и сличне случајеве. Увелико се ради и на развоју кибер-оружја.Владе многих држава схватају значај контроле својих грађана и њихових интересовања. У томе веома често имају и подршку Интернет компанија. Најчешћи облици контроле Интернета су постављање филтера против субверзивног материјала, увођења цензуре за веб странице са опасним садржајем по власт и инсталирање посебних програма који читају електронску пошту.Потпредседник Европске комисије Франко Фратини изјавио је да Европска унија мора да уложи додатне напоре како би повећала безбедност становника свих њених чланица. Једна од мера које је предложио јесте затварање свих веб локација на којима екстремне групе објављују своје пропагандне материјале и размењују информације о методама терористичких напада. „Тероризам представља претњу не само политичким основама Европске уније, него и свакодневном животу наших суграђана" изјавио је Фратини. „Нове мере треба да олакшају сарадњу компанија давалаца Интернет услуга и одговарајућих државних служби, како би се спречили терористички напади и идентификовали нападачи , додао је Фратини. Овим мерама се предвиђа лакши приступ базама података давалаца Интернет услуга.Аустријска влада је од ове године почела са контролом Интернета и праћењем кретања појединаца на светској мрежи са циљем улажења у траг терористичким организацијама. Канцеларка Немачке истиче да Немачка треба да дозволи службама безбедности контролу Интернета због сузбијања тероризма, у супротном постоји могућност да се створи простор у ком ће терористи бити безбедни, а да држава у њега неће моћи да уђе.Ускоро ће се у оквиру руске војно обавештајне службе ГРУ оформити ново одељење које ће се искључиво бавити сакупљањем информација преко Интернета. Ово све је у складу са борбом против тероризма, али с друге стране ради се о потезима којима се у многоме угрожава приватност.У нашој земљи,

[16] Петровић , С, *Компјутерски криминал*, Војноиздавачки завод, Београд, 2001., стр. 362.

Републичка агенција за телекомуникације усвојила је правилник под називом „Технички услови за подсистеме, уређаје, опрему и инсталације Интернет мреже." Овим правилником се предвиђа да Интернет оператери о свом трошку оформе део система за законом дозвољен надзор телекомуникација и да државним органима пруже информације о претплатницима и омогуће им да пресрећу разговоре и електронску пошту. Интернет провајдери су обавезни да надлежним службама, полицији или Безбедносно-информативној агенцији омогуће потпуно аутономно посматрање Интернет активности претплатника и преусмерење долазног и одлазног саобраћаја.Овај правилник је изазвао негодовање јавности при чему се истицало да правилник у многоме крши људска права, пре свега што у моменту његовог доношења Србија није имала Закон о заштити података о личности. Овај правилник је привремено стављен ван снаге, до доношења поменутог закона. С обзиром да је Закон о заштити података о личности усвојен у Народној скупштини Србије видећемо да ли ће спорни правилник ступити на снагу у изворном или нешто измењеном издању.Стручњаци се слажу да до сада у Републици Србији није извршен ни један напад који би могао да се окарактерише као кибер-тероризам. Разлог што је мала вероватноћа да Република Србија постане мета кибер-терориста јесте низак ниво интеграције рачунарских система, али и то што Република Србија, није чланица евроатланских организација које су главна мета екстремних исламистичких група. У складу са развојем нове информационо-комуникационе технологије, национална инфраструктура Републике Србије биће све више аутоматизована и међусобно повезана. Суштински ресурси базираће се на информацоно-комуникационој технологији, укључујући одбрамбене системе, системе државне управе, комплексне управљачке системе и инфраструктуре које обухватају контролу електричне енергије, телефонског система, токова новца, ваздушног саобраћаја, нафте, гаса и других информационо-зависних области.[17] Ове мере ће посебно бити значајне у будућности када се очекује приближавање Србије Европској унији и евроатланским интеграцијама, које би са собом, осим мноштва погодности, Србији донеле и нове непријатеље а са њима и могућност мноштва сајбер али и других терористичких напада. С тога се искуства других земаља морају узети у обзир и применити у систему безбедности наше земље. Колики је значај ове борбе говори и податак да се читава међународна заједница је почела да се бори против неких видова злоупотребе интернета. На пример, Европска Унија је створила систем раз-

[17] Вулетић, Д, *Угрожавање безбедности Републике Србије сајбер тероризмом*, Безбедност бр. 6, 2006., стр.956

мене информација о овој врсти претње. Португалија је предложила усвајање система размена информација прикупљених на интернету („Interchange of Open Information Collected on the Internet"). Наведени систем требало би да обезбеди свим чланицама „ефикасно оруђе у откривању информација, а све у контексту борбе против тероризма". У оквиру ове организације донет је и Закон о заштити електронских података („Rules of protection of electronic data"). И друге важне међународне организације укључиле су се у ову борбу: Уједињене Нације су донеле Резолуцију 1373 о борби против тероризма. Амерички Конгрес је донео Патриотски акт (USA Patriot Act). Закон о надзору страних обавештајних служби, познат као FISA, осигурава кључни правни оквир који омогућује обавештајној заједници да, надзирући комуникације терориста, прикупља информације за заштиту цивилних слобода Американаца. Закон 9/11, како је колоквијално назван, предвиђа преусмеравање средстава на високо ризичне савезне државе и градове, проширује надзор зрачног и поморског терета који улази у САД и финансирање нових програма који ће осигурати међусобну комуникацију различитих обавештајних и сигурносних служби ангажованих у борби против тероризма. Осим поменутих постоје и препоруке осам најразвијенијих земаља света Г-8 и Европског полицијског тела Европола.[18]

Закључна разматрања

У савременим условима глобализације, тероризам представља озбиљан глобални проблем који угрожава савремено друштво. Тероризам је један од највећих изазова савременој цивилизацији и један од најопаснијих облика политичког насиља а као такав обележен је застрашујућим физичким и психолошким методама политичке борбе. Иако корени тероризма сежу далеко у прошлост, тероризам је производ модерног доба а његови узроци и мотиви су различити. Циљ терористичких аката је скретање пажње јавности на стање, положај и проблеме неке друштвене групе и њихово стављање у први план у односу на све друге проблеме у држави, региону, па чак и свету, слање поруке (политичке) о тежњи и намерама те групе. Како би изазвали страх и постигли политичке циљеве терористичке организације употребљавају различите облике насиља зависно од области у којој се испољавања а при томе теже саморекламирању и добијању публицитета, тако да је за терористе вео-

[18] Опирније у: Зиројевић Фатић М, *Злоупотреба интернета у терористичке сврхе*, МП 3, 2011. стр. 443–444.

ма важна могућност јавног обраћања и пропаганде. С обзиром да су одавно постали свесни значаја медија, терористи посредством медија, веома вешто, промовишу своје идеје и активности. На тај начин медији постају важна полуга у пропаганди терористичких идеја. Терористи користе пропаганду како би себе описали као борце за слободу, револуционарне хероје и оне који доносе ослобођење. За пропаганду је карактеристично пласирање одабраних елемената истине који су вешто помешани са неистином.Тероризам можемо посматрати и као својеврсно средство комуникације.Претварањем својих акција у велики медијски догађај, коме ће уредници медијских кућа посветити свој програм и бирањем атрактивних мета о којима ће извештавати медији- шаљу својеврсну поруку и постају средство комуникације. Исто тако, између медија и терориста успостављен је интерактиван однос. Масовни медији тероризму дају глобалан значај. Насиље које терористичке групе спроводе представља њихов пут да информација стигне до „публике". Исто тако и трендови медијске индустрије данас се крећу у правцу преферирања садржаја сензационалистичког типа, због чега терористи себи могу осигурати максималну присутност у медијима. Потреба за сензационализмом надвладала је потребу за супростављањем терористичким актима чиме се ствара простор за даље активности терориста.Оно на шта посебно морамо указати је и чињеница да развој технологије за терористе отвара нове могућности у реализацији њихових циљева а у савременим условима глобализације. При томе интернет, као један од облика нових комуникационих технологија, постаје моћно оружје у рукама терористичких организација.Интернет технологије су терористичким организацијама пружиле могућност лакшег и слободнијег преноса порука. Мрежа комуникација преко рачунара идеална је за терористе због тога што се интернет, који нема централизовано управљање, не може у потпуности контролисати. Методе контратероризма у многоме ће морати да се промене према терористима који делују у том новом, виртуелном простору.Улога и значај интернета је данас све већа а интернет се појављује како као средство кумуникације и средство за прикупљање финансија терористичким организацијама, тако и средтво путем којег се регрутују нови чланови и изводе терористички напади. Традиционални тероризам замењује полако кибер (*cyber*) тероризам који подразумева различите злоупотребе рачунарских система које се односе на: крађу података и „обарање" веб страница, планирање терористичких напада, изазивање насиља и страха код цивила или напад на организационе системе. Као потенцијалне мете кибер-тероризма, издвајају се: електрична постројења, водовод, складишта гаса и нафте, као и њихов транспорт,

службе за ванредне ситуације, фармацеутске установе, болничке архиве, веб странице, тржиште акција, банкарске трансакције, железнички, речни и авио саобрај, државни органи, и др. Оволика раширеност мета напада је последица чињенице да је откривање кибер-терористa веома тешко, јер Интернет пружа висок степен дигиталне анонимности.

У циљу ефикације борбе против тероризма, данас се улажу велики напори да се контрола интернета бар до некле учини могућом, јер интернет у стању и облику у ком се сада налази, још увек представља неразрешиву енигму за државе, али и рај за терористе, који своје активности полако, али сигурно пресељавају у јефтинији, али знатно ефикаснији виртуелни свет.

Литература:

1. Savić, A., Osnovni koncept propagande u savremenom svetu, Bezbednost br. 3, 1986.
2. Vuletić, D., Ugrožavanje bezbednosti Republike Srbije sajber terorizmom, Bezbednost br. 6, 2006.
3. Zirojević, M., Terorističke organizacije i internet, Vojno delo br. 1, Vojna akademija, Beograd, 2004.
4. Đurić-Atanasievski, K., Uticaj medijskog izveštavanja o terorizmu na javnost i donosioce političkih odluka, članak u časopisu Vojno delo, vol. 62, br. 4., Vojna akademija, Beograd, 2010.
5. Zirojević Fatić M., Zloupotreba interneta u terorističke svrhe, MP 3, 2011.
6. Kešetović, Ž., Internet kao oruđe terorista, Revija za bezbednost br. 4, 2008.
7. Maletić, I., Doprinos medija razvoju savremenog terorizma i antiterorizma, Kriminalističko-policijska akademija, Beograd, 2009.
8. Petrović , S., Kompjuterski kriminal, Vojnoizdavački zavod, Beograd, 2001.
9. http://www.muskimagazin.com/2012/01/25/terorizam-i-internet-tastatura-kao-kalasnjikov/, Доступно: 7.7.2012.
10. http://www.csrp.org/index.html, Доступно: 7.7.2012.
11. http://www.sk.rs/2001/10/skin01.html, Доступно 8.7.2012.

INTERNET AND TERRORISM

Summary: The media today are very powerful factor of political and social power but also a factor that largely shape the world democracy and public opinion. Creating political will, attitudes, needs and habits, the media increasingly shape the behavior of individuals, groups and masses of truth and reality and realize they see as their media to serve. Consequently that, today more and more discussion about the relationship between media and terrorism, publicity and propaganda. Speaking of

mass media, one can not look at the internet, its importance and role in the life of every individual today, which is growing by the day. Development of technology for the terrorists opens up new opportunities to realize their goals. In modern conditions of globalization internet as a form of new communication technologies, it becomes a powerful weapon in the hands of terrorist organizations. Internet and modern technology brings many benefits to modern man but unfortunately terrorists. It is necessary to emphasize the great role of the Internet as a medium to promote terrorism and the Internet as a powerful weapon in the hands of terrorists through which conducted the recruitment of new staff and raise funds for new activities. Network communication via computer is ideal for terrorists because of the internet, which has no centralized control, can not be fully controlled. Traditional cyber terrorism replaced slowly (cyber) t terrorism that involves a variety of misuse of computer systems related to: data theft and the „overthrow" of web pages, planning terrorist attacks, inciting violence and fear among civilians or an attack on the organizational systems. For cyber-terrorist , computer network is a weapon, medium or goal. In order to effectively combat terrorism, now efforts are made to control the internet bar to some extent make it possible. thing which we must be aware that cyber-attacks are becoming a real danger to society that the same does not adequate response.

Key words: media, internet, communication, technology, terrorism, cyber-terrorism