UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Borut Poljšak

Kibernetska mimikrija spletnih strani

Diplomsko delo

Ljubljana, 2009

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Borut Poljšak

Mentor: doc. dr. Gregor Petrič
Somentor: izr. prof. dr. Marjan Smrke

Kibernetska mimikrija spletnih strani

Diplomsko delo

Ljubljana, 2009

Kibernetska mimikrija spletnih strani

Kibernetski prostor je prostor poln svobode in s tem tudi prevar in poneverb spletnih strani. Diplomska naloga obravnava kibernetsko mimikrijo, ki se pojavlja na svetovnem spletu. Kibernetska mimikrija je pojav, ki temelji na posnemanju kredibilnih spletnih strani. Najbolj pogost znak kibernetsko mimikretične strani je ponarejanje drugih spletnih strani, ki so širše prepoznavne po svoji obliki in vsebini. V diplomski nalogi poskušam prikazati, kako odkriti kibernetsko mimikrijo na spletnih straneh, ki jih obiskujemo. V nalogi so obravnavani določeni primeri pojavnih oblik mimikrije, ki se pojavljajo na spletu. Prikazan je tudi sam potek evalvacij spletnih strani, ki temelji na strokovni shemi za lažje odkrivanje mimikretičnih spletnih strani. Tako je glavni namen naloge predstavitev in ovrednotenje kriterijev, po katerih je moč zaznati in oceniti mimikretičnost spletne strani.
Diplomsko delo je sestavljeno iz teoretičnega dela, iz katerega v drugem delu izpeljujem empirični del, ki je tehnično-evalvacijske narave. Celoten empirični del se nanaša na evalvacijo spletnih strani ter s tem na ugotavljanje kibernetske mimikrije.
Ugotavlja se, da je kibernetska mimikrija spletnih strani resen problem na internetu in da je področje (do zdaj) premalo raziskano.

Ključne besede: Kibernetska mimikrija, prevare, izmišljene strani, ponarejene strani, samoocena spletne strani.

Cybernetic mimicry of web pages

Cybernetic space is space full of freedom and with that comes deception and embezzlement of web pages. Dissertation speaks about cybernetic mimicry and how it occurs on the world web. Cybernetic mimicry is a phenomenon which is based on imitation of credible web pages. The most frequent signal of cybernetic mimicry pages is forgery of other web pages, which is recognized by its own shapes and contents. Dissertation tries to show how to discover cybernetic mimicry on web pages, which we are visiting every day. In dissertation are also discussed and defined examples of the phenomenon of mimicry, which are shown on web. Dissertation represents evaluations of web pages, which are based on expert scheme for easily discovering of mimicry on web pages. The main purpose of task is represented on perceived and estimated mimicry of web pages. Dissertation is combined from theoretical part, from which in second part follows out empirical part. The whole empirical part is related to evaluation of web pages. The main finding is that cybernetic mimicry of web pages is a serious problem on the internet and that this area is not enough discovered yet.

Key words: Cybernetic mimicry, deceptions, untrue sites, counterfeited sites, self-evaluation of web page.

KAZALO

1 UVOD

Danes se v vsakodnevnem življenju uporabniki interneta srečujemo z mnogimi informacijami, ki jih potrebujemo za svoje delovanje. Vendar pa se ob iskanju želenih informacij včasih srečamo s spletnimi stranmi, ki ne vsebujejo pravih, relevantnih oziroma pristnih informacij. Gre za spletne strani, ki nam jih spletni iskalniki ponudijo kot zanesljive vire informacij za naše iskalne potrebe, a dejansko se izkaže, da tovrstne spletne strani ne ponujajo samo relevantnih informacij ali pa gre celo za zavajajoče oziroma zlonamerne informacije. Take strani imenujemo *mimikretične spletne strani*. Njihova najpogostejša lastnost je, da nam podajajo lažne informacije. Lažne informacije so tiste, ki nam ponudijo podatek, ki ni relevanten za našo uporabo v vsakdanjem življenju ali pa nam lahko celo škodi.

V diplomskem delu me zanima predvsem, kako takšne strani odkrijemo, ali obstajajo kriteriji, s katerimi določimo mimikretično spletno stran, ali obstaja ocena, koliko je takšnih strani na spletu. Glavni namen naloge je predstavitev kriterijev, na podlagi katerih je moč zaznati in oceniti mimikretičnost spletne strani na manjšem vzorcu spletnih strani.

Kibernetska mimikrija spletnih strani se pojavlja v širšem na področju računalništva. V diplomski nalogi se bom osredotočil na spletne strani. Prevare, ki se pojavljajo v računalništvu, lahko uvrstimo na področje kibernetske mimikrije, ki posamezniku ali uporabniku spleta najpogosteje povzroča težave. Uporabniki morajo biti pazljivi pri uporabi samih spletnih strani ter pri uporabljanju informacij, ki jih le-te vsebujejo. Želim prikazati, kako se lahko uporabniki sami najbolje zaščitijo pred prevarami na spletnih straneh, ki se pri natančnem preučevanju izkažejo kot del kibernetske mimikrije.

Uporabniki vseh starosti so lahko tarče za druge organizacije ali posameznike, kot omenja Maria Bakardjieva (2005), ki vidi internetnega uporabnika kot model igrače med tehnologijo in družbo. Z uporabnikom misli na navadnega uporabnika, ki ne deluje v profesionalnem okolju (npr. kot inženir, programer, oblikovalec), temveč kot uporabnik v vsakdanjem življenju. S tem je mišljen uporabnik spletnih strani, ki pri razvoju tehnologije nima neposrednega vpliva, vendar pa ima osrednjo vlogo pri uporabi tehnologije (Bakardjieva 2005, 13). Uporabniki spletnih strani ponavadi ne

poznajo tehničnega ozadja izgradnje spletnih strani in možnosti njihovih zlorab, zato so zaradi pojava kibernetske mimikrije še posebej ranljivi.

Kibernetska mimikrija je pojav, ki temelji na posnemanju kredibilnih spletnih strani. V diplomski nalogi bom poskusil prikazati, kako odkriti kibernetsko mimikrijo na spletnih straneh, ki jih pogosto obiskujemo. Uporabil bom kriterije za ocenjevanje spletnih strani, ki so jih razvili na Univerzi Britanska Kolumbija (Lesley University webpage 2008). Izbral sem si pet spletnih strani, za katere sem dobil ideje v knjigi *Web of deception: Misinformation on the internet* (2002). V knjigi so navedene spletne strani, ki naj bi bile kibernetsko mimikretične.
Pri tem je treba poudariti, da v nalogi prevar na internetu ne bom obravnaval kot kriminal, ki se pojavlja znotraj kibernetske mimikrije, temveč z vidika manipulativne moči, ki jo imajo nad uporabniki, ki niso dovolj pazljivi pri uporabi spletnih strani.
Kibernetska mimikrija lahko ogroža človekovo varnost in s tem povzroča negotovost na spletnih straneh. Tako uporabniki izgubljajo zaupanje v varnost spletnih strani. Največji problem pri kibernetski mimikriji je, da jo uporabniki spleta težko ugotavljajo in prepoznavajo, saj so prevare vse bolj pogost pojav na spletnih straneh.

Diplomsko delo je torej sestavljeno iz teoretičnega dela, iz katerega bom nato v drugem delu izpeljal empirični del, ki bo tehnično-evalvacijske narave. Bistvo diplomske naloge je predstavitev, kaj kibernetska mimikrija je in kje se najpogosteje pojavlja.
Celoten empirični del se bo nanašal na evalvacijo spletnih strani ter s tem na ugotavljanje kibernetske mimikrije na obravnavanih spletnih straneh z uporabo sheme.
V sklepu tako podajam ključne ugotovitve iz empiričnega dela in predloge za nadaljnjo raziskovanje kibernetske mimikrije spletnih strani.

Cilj diplomske naloge je prispevati k jasnejšemu zavedanju problema kibernetske mimikrije spletnih strani ter pozvati sorodne strokovnjake k širšemu raziskovanju tega pojava.

2 TEORETIČNI DEL

2.1 KAJ JE MIMIKRIJA?

Pojem mimikrija se v moderni znanosti najprej pojavi v zoologiji. Po Batesu (v Smrke 2007, 14) je dobila ime prva opisana oblika mimikrije dobila ime pri metuljih, in sicer kot oblika biološke podobnosti, v kateri nenevaren in užiten organizem oponaša neužiten organizem zato, da bi se zavaroval pred plenilcem. Mimikrija je velika podobnost enega organizma drugemu organizmu, kar tretji organizem zavede v napačno prepoznavo. Mimikrija je povezana tudi z lažjo in prevaro.

Sama mimikrija prinaša tudi uspeh za tistega, ki je mimik. Pri mimikriji bitja posnemajo druga bitja, da dosežejo določen uspeh. V živalskem svetu je uspeh preživetje, za človeka pa je uspeh bolj kompleksno definiran. Lahko gre za ugled, denar, material itd.

Za mimikrijo lahko rečemo, da proizvaja laž, saj predstavlja nekaj, kar v resnici ne obstaja. Posnemanje v mimikriji je prisotno v sami predstavitvi človeka in nato pri govoru ter navsezadnje pri uporabi tehnologije. Posnemanje neke osebe lahko prinaša tudi koristi za mimika (Gambetta 2005, 229).

Poznamo tudi prevarantsko mimikrijo (deception mimicry) in identitetno mimikrijo (identity mimicry). S tema izrazoma Diego Gambetta (2005) označuje pojav igranja drugega posameznika ali člana skupine, ki ji igralec v resnici ne pripada. Izkoriščevalska mimikrija (exploitive mimicry) je po Edwardu Hagenu (v Smrke 2007) strategija varanja, ki ima za cilj je izsiljevanje družbenih koristi. Človeško oziroma družbeno mimikrijo tu opredeljujemo kot mimikrijo, pri kateri je mimik človek. V človeški mimikriji gre za delovanje posameznika ali družbenih skupin, v katerih se skuša z različnimi oblikami pretvarjanja povečati možnosti uspeha oziroma zmanjšati možnosti neuspeha v družbenem ali naravnem okolju. Mimikretična dejavnost ni nujno zavestno dejanje, saj gre za rutinski vedenjski obrazec, ki je nastal v preteklosti in se priuči s socializacijo (Smrke 2007).

Michael Lachmann in Carl T. Bergstrom (Lachmann in Bergstrom 2004, 2337) razlikujeta med kompleksnimi komunikacijami pri živalih in človeku. Ugotavljata, da so prevare že del naše komunikacije in s tem tudi, da je človeška rasa nagnjena k mimikretičnim prevaram. Bolj ko je komunikacija pri določeni vrsti kompleksna, večje so možnosti za nastanek prevar in mimikrij. V glavnem se mimikrija pojavlja pri bolj kompleksnih strukturah jezika, kar tudi dokazujeta v svojem članku.

Človeška oziroma družbena mimikrija se uveljavlja v mimikretičnem odnosu. Mimikretičen odnos je družbena interakcija med mimikom in operatorjem, v kateri se izvrši mimikretična akcija. Mimikretična akcija je potek mimikretičnega odnosa od njegove vzpostavitve do konca. Ta mimikretičen odnos velja tudi za kibernetsko mimikrijo, saj je *mimik* tisti, ki ponareja spletne strani, *operator* pa je uporabnik interneta, na katerem se nato izvede *mimikretična akcija*, ki prinese posledice. Mimik skuša vzbuditi vtis o svoji drugačnosti od dejanskosti z oponašanjem določenega modela. Model, ki ga mimik posnema je lahko stvaren ali nestvaren pojav. Da bi mimik vzbudil vtis enakosti z modelom, mora operatorju prikazati določene informacije. Celoto prikazanih informacij poimenujemo mimem. Mimem je torej mimikov izdelek, ki posnema model, s katerim skuša mimik pri operatorju vzbuditi zamenjavo z modelom. Pri kibernetski mimikriji lahko mimem opredelimo kot obliko ponarejenih spletnih strani ali programov v obliki trojanskih konj. Ta oblika predstavlja model, s katerim skuša mimik zavesti operatorja. Poznamo tudi namerno ali nenamerno mimikrijo. Nenamerna mimikrija nastopi spontano, ne da bi mimik tak odnos načrtoval. O namerni mimikriji pa govorimo, ko je mimikretična akcija načrtovana in premišljeno vodena. Kibernetska mimikrija je le eno izmed področij človeške mimikrije (Smrke 2007, 15-50).

2.2 OPREDELITEV KIBERNETSKE MIMIKRIJE

Kibernetska mimikrija spada v t. i. človeško oziroma družbeno mimikrijo, ki pa dokončno nastane z uporabo informacijsko-komunikacijskih tehnologij v računalništvu. Mimik je človek, ki to prenese na splet in spoji z računalniško tehnologijo ter s tem ustvari kibernetsko mimikrijo (Gambetta 2005, 223). S kibernetsko mimikrijo mislimo na raznoliko mimikrijo, ki se pojavlja v razraščajočem se kibernetskem prostoru. Tu se uporablja izraz prevara (deception) (Smrke 2007, 131). Prevare so povezane predvsem z novo tehnologijo, vključno z internetom v kibernetskem prostoru (Mintz 2002, 53).

Pri prevari v računalništvu se neka oseba ali program zamaskira kot nekdo drug s ponarejanjem podatkov in tako dobi neko legitimno prednost ali korist. Kibernetsko mimikrijo lahko razdelimo na več področij. Najbolj pomembno področje je poneverba spletnih strani, iz tega izhaja kraja identitete posameznika in na koncu še poneverba elektronske pošte (Dokl 2006, 41).

Zavestne prevare so tudi del kibernetske mimikrije, saj gre za premišljeno fabriciranje oziroma ponarejanje eksperimentov z namenom ogoljufati ali napačno informirati znanstveno javnost. S tem se je ukvarjal Charles Babbage (v Mali, 2002), ki je ločil fabriciranje ali ponarejanje podatkov, manipulacijo podatkov in utajo podatkov. Predvsem utaja ali prekrivanje podatkov velja za manj nevarno goljufijo, medtem ko je ponarejanje podatkov najbolj nevarna prevara. Prikrivanje podatkov je težko odkriti, saj je odločitev, kateri znanstveni podatki in analize so pomembni za javnost, prepuščena individualni presoji raziskovalca (Gruban 2003, 46).

2.2.1 Poneverba spletnih strani

Glavni medij kibernetske mimikrije je splet ali internet, na katerem so spletne strani, ki jih lahko poimenujemo tudi *model*, saj predstavljajo okolje, ki ga *mimik* posnema. Internet omogoča vsakemu uporabniku, da ustvari lastne strani, ki se tičejo katerekoli vsebine. Omogoča različne možnosti skrivanja identitete izvora (dez)informacij. V vlogi *operatorja* oziroma sprejemnika je predvsem običajen, razmeroma nevešč in naiven uporabnik spleta, medtem ko *mimikretično akcijo* vodi tehnološko bolj vešča oseba, ki ga na področju kibernetske mimikrije lahko imenujemo mimik, saj je tisti, ki izvaja mimikrijo.

Eden očitnejših primerov kibernetske mimikrije je ponarejena stran (counterfeit site) ali hlinjena stran. Gre za stran, ki se predstavlja kot pristna stran, v resnici pa le-to oponaša z določenim prikritim namenom. Paul Piper (v Smrke 2007, 131) ugotavlja, da se ponarejene strani predstavljajo v preobleki kot legitimne strani, da bi razširjale dezinformacije. S tem postane jasno, da kibernetska mimikrija na spletnih straneh deluje legitimno, vendar se kibernetsko mimikretično kaže v pridobivanju informacij v nelegitimnem smislu. Očitno parodična je pornografska spletna stran Booble (www.booble.com), ki je posnema spletno stran Google (www.google.com), najpopularnejši spletni iskalnik. Oponašanje neke dejanske strani ima poleg škodljivih namenov lahko tudi parodične, humorne (parody, spoof sites) in neškodljive namene, pri tem je dezinformacija očitna, meni Piper.

Učinkovite so lahko tudi fiktivne spletne strani, ki predstavljajo povsem izmišljene strani. Ne oponašajo nekega modela, ampak v celoti ustvarijo pojav, ki ne obstaja. Izmišljene ali fiktivne strani vseeno vplivajo na posameznika in ga zavajajo. Primer tega

je lahko domača stran Ruritranija[1]. Te izmišljene strani so ustvarjene zato, da zavajajo in/ali zabavajo uporabnike (Mintz 2002, 13).

Ponarejene spletne strani so najbolj problematične potegavščine na internetu. Kot primer lahko omenimo spletno stran Martina Luthra Kinga. Kopija spletne strani predstavlja človeka, ki pa to v resnici sploh ni Martin Luther King. Na spletni strani so izmišljene in lažne informacije.

Ponarejene strani se največkrat kažejo kot legitimne strani pod krinko zato, da širijo napačne informacije, da zavedejo končnega uporabnika. Namene ponarejenih spletnih strani lahko razdelimo na politične namene in za zabavo oziroma za zabavništvo[2] (Mintz 2002, 6).

Napačne informacije na spletnih straneh so produkt kibernetske mimikrije. Anton Vedder (2001) ponuja dve strategiji, kako se izogniti napačnim informacijam na internetu. Prva je razviti kritično vedenje do sprejemanje informacij. Uporabniki ne smejo verjeti vsemu, kar vidijo na internetu, ampak morajo obdržati neko intelektualno distanco do tega, kar najdejo na spletni strani. Obdržati moramo neko razmerje med tem, kar nam spletna stran prinaša pozitivnega in negativnega ter s tem povečati samo veljavnost spletne strani. Druga strategija pa je, da ocenimo samo objavo na spletni strani ter ugotovimo, od kod prihaja informacija, ki je na spletni strani predstavljena kot pristna. Pomembno je tudi samo ozadje spletne strani, ki nam nekaj sporoča. Za odkrivanje napačnih informacij v kibernetski mimikriji je pomembno kritično ocenjevanje spletne strani, ki jo uporabnik uporablja. Odkrivanje napačnih informacij po Vedderju ni samo globlji vpogled v kvaliteto spletne strani, temveč je treba oceniti tudi samo veljavnost informacije, ki nam jo ponuja spletna stran.

2.2.2 Kraja identitete posameznika

Kraja identitete je zlonamerna uporaba identitete neke druge osebe. Sem sodijo zloraba imena, davčne številke, enotne matične številke občana ali elektronskih naslovov. S temi podatki je mogoče pravi osebi narediti določeno škodo oziroma se okoristiti s

[1] To naj bi bila država med Norveško in Švedsko in naj bi imela 4 milijone prebivalcev ter svojo zgodovino, kulturo in politični sistem.

[2] Ena od prvih ponarejenih strani, ki je pritegnila pozornost javnosti, je bila stran www.makah.org, ki je objavljala, kako lovijo kite, ki so zaščiteni. To stran so si izmislile protestne skupine proti lovu na kite. Ta stran je vsebovala pozive, da je Makah morilec, da bi ljudem ali uporabnikom prikazali, da lov na kite izvajajo hladnokrvni morilci živali. Ta stran je bila kmalu za tem ukinjena.

podatki. Najbolj so privlačne kraje številk kreditnih kartic, ki v kombinaciji z drugimi osebnimi podatki na določenih internetnih straneh omogočajo nakup (Dokl 2006, 41).
Identitete nimajo le posamezniki, ampak tudi institucije, podjetja. V »kiberskvotanje« spada ustanavljanje fiktivnih kibernetskih podjetij, ki so zelo podobna izvornim resničnim podjetjem, ki so ponavadi znana in uspešna. Ko se iz tega navideznega, mimikretičnega podjetja iztrži nekaj denarja, se le-to ukine. Poleg ustvarjanja fiktivnih podjetij je pogost tudi t. i. »grooming«[3]. Tako se v spletnih klepetalnicah npr. starejši moški pretvarja, da je najstnik, zato da bi lažje navezal stik z mlajšo žensko (Smrke 2007, 134).
Pod krajo identitete spada tudi »ribarjenje« v kibernetskem prostoru. To je pošiljanje elektronske pošte, ki se uporabniku lažno predstavlja kot pošta uveljavljenega podjetja z namenom, da bi se od uporabnika pridobilo zasebne informacije, ki bi se jih uporabilo za krajo identitete. Elektronsko pismo uporabnika usmeri na spletno stran, na katerih je naprošen, naj obnovi svoje osebne podatke, kot je geslo, podatke o bančni kartici, zavarovalno in bančno številko. Spletna stran je lažna, saj je postavljena le zato, da ukrade informacije (Smrke 2007, 133). Tako mimikretična spletna stran kot elektronsko pismo sta lahko na pogled popolnoma enaka spletni strani ali pismu legitimnega podjetja. Vendar bosta uporabnikove finančne podatke posredovala tretjim osebam, ki se bodo z njimi okoristile (Hafner 2006, 13).

2.2.3 Poneverba elektronske pošte

Poneverba elektronske pošte se lahko pojavi v različnih oblikah, vendar imajo vse isti rezultat. Uporabnik dobi elektronsko pošto, ki se zdi, kot da je prišla od določenega znanega vira, vendar je bila poslana z drugega, ponarejenega. Tovrstne poneverbe se pogosto uporabljajo zato, da bi uporabnika pripravili v škodljivo izjavo, ki jo nato uporabijo proti njemu v medijih ali drugi zainteresirani javnosti ali za izdajo zaupnih podatkov, kot so gesla, številke kreditnih kartic in podobno. Primer ponarejenega elektronskega sporočila, ki bi škodoval, lahko poteka tako, da sistemski administrator sporoči, da je treba spremeniti geslo na določeno zaporedje črk ali številk, ki ga navede, in v istem sporočilu zagrozi, da bo ukinil elektronski predal, če to ne bo storjeno (Dokl 2006, 43).

[3] Pojav grooming pomeni, da odrasla oseba psihološko ali fizično manipulira z otrokom za spolne namene: obravnavan je v poročilu 23. člena konvencije Sveta Evrope (SK EUR-Lex 2009).

2.3 PRIMER KIBERNETSKE MIMIKRIJE SPLETNIH STRANI

V zadnjem času se mimikrija spletnih strani vse bolj pojavlja tudi v Sloveniji, zato bom navedel primer s spleta, ki nam je vsem dostopen in redno uporabljan.

Poneverbe spletnih strani so bile močno odmevne tudi v Sloveniji, ko so na spletni strani banke NLB (www.nlb.si) opozarjali na ponarejeno vstopno stran na njihovi strani, na kateri je posameznik vnesel osebne podatke, od koder je potem imel dostop do njegovega računa nekdo drug. Na strani NLB so objavili tudi primer ponarejene strani. Čeprav je bil oškodovan le en posameznik in še to ne veliko, je to resno opozorilo, da je tudi Slovenijo ogroža ponarejanje spletnih strani na kibernetsko mimikretičen način (RTVSLO 2006).

Na strani Akademske in raziskovalne mreže Slovenije (ARNES) opozarjajo, da je število poskusov prevar (predvsem kraj denarja preko internetu) z uporabo nenaročene oglasne pošte (t.i. spam) v kombinaciji s ponarejenimi spletnimi stranmi v zadnjem letu poraslo. Pojav primerjajo z epidemijo računalniških virusov. Navajajo celo, kako se prevaram izogniti in kako se zavarujemo. Najbolj pomembno pa je, kako te prevare prepoznamo. Navajajo dva primera eBaya[4] (www.ebay.com) in podjetja Visa (www.visa.com), v katerih so določeni akterji ali posamezniki ustvarili mimikretične spletne strani, ki so simulirale prave spletne strani. V obeh primerih opozarjajo, da podjetja popolnoma ponaredijo logotipe, besedilo, barvne sheme in celotno spletno podobo izvirnega podjetja. Bolj napredne spletne strani, ki vam želijo izprazniti račune, pogosto ponaredijo celo videz vašega brskalnika. Tako je mogoče ponarediti naslovno vrstico, katerih bo na prvi pogled izpisan »pravi« spletni naslov, vključno s predpono »https« in »varno ključavnico« v statusni vrstici (ARNES 2004).

[4] Spletna dražbena stran www.ebay.com je največja spletna tržnica na svetu, ki uporabniku omogoča dostop do obsežne spletne strani s široko ponudbo storitev in do svetovne baze z ogromno uporabnikov. Kupcem ponuja mnogo koristnih nasvetov za varno spletno trgovanje ter skrbi za obsežne varnostne informacije o trgovanju, overitvah, reševanju sporov, načinih plačila, kontroli in zaščiti.

3 EMPIRIČNI DEL

3.1 OCENA SPLETNE STRANI

Svetovni splet ponuja ogromno informacij, med njimi tudi možnosti za uporabnike, da izrazijo sami sebe in izmenjajo ideje. Če uporabljamo spletne strani, potrebujemo tudi razvoj naših veščin za oceno strani in namembnosti, zakaj jih iščemo (Microsoft 2009). Posebej pomembno je, da kritično ocenimo spletno stran, ki se nam zdi neprava oziroma kibernetsko mimikretična. Na začetku je dobro biti skeptičen. Nikoli ne smemo verjeti informacijam, ki jih preberemo ali vidimo prvič. Najbolj pomembno pa je, da ne odpremo takoj spletne strani (in njenih aplikacij, dokumentov idr.), ki je ne poznamo. Spodaj so navedeni kriteriji za ocenitev spletne strani, ki jih Anna Mintz v svoji knjigi *Deception of web* (Mintz 2002) navede kot ključne za ugotavljanje kibernetske mimikrije. Uporabnik interneta se mora vprašati:

1. Kdo je administrator ali lastnik spletne strani?

Spletni avtorji potrebujejo za ustvarjanje storitev le malo veščin iz informacijskih tehnologij in malo denarja. Včasih sploh ni popolnoma jasno, kdo je avtor te strani, zato se je treba pozanimati na spletni strani. Domnevno avtorji spletnih strani ne poznajo pogledov uporabnikov. Tukaj je s kibernetsko mimikretične perspektive pomembno, da je avtor spletne strani mimik, ki išče operatorje in jih spremeni v mimikretične žrtve (Smrke 2007).

2. Kdo je objavil spletno stran?

Nekatere objave na spletni strani imajo odličen ugled. Uporabljajo veščine in primerne avtorje. Nekatere zelo uporabne spletne strani z zelo kvalitetnimi informacijami so objavljene pri vladnih agencijah, univerzah in trgovskih združenjih. Večina vladnih informacij je javno dostopnih ter so zastonj. Bolj ko so relevantne informacije na spletni strani, večji ugled ima določena spletna stran.

3. Ali je informacija na strani relevantna?

Ko pregledujemo spletno stran, moramo sami sebe vprašati, ali je informacija relevantna za našo uporabo. Zelo pomembni so tudi viri na spletnih straneh, saj dajejo vtis večje kvalitete. Če na spletni strani ni znanih virov, so lahko informacije nenatančne in nepravilne. Namen spletne strani mora biti samoumeven. Informacije in

vsebina strani ne smejo biti sumljive. Čeprav je bistvo kibernetske mimikrije, da stran v nobenem pogledu ni videti sumljiva, jo moramo vseeno razkrinkati, preden nas mimikrija zavede kot uporabnike. Če je informacija na spletni strani sumljiva in ta stran omogoča povezavo tudi na druge strani, ne smemo nikoli odpirati takih povezav, ker nam bi bile lahko škodljive.

4. Kako pogosto je stran osvežena ali ažurirana?

Zelo pomembno je, da so na spletni strani datumi. Idealno je, da so datumi sprotno objavljeni od prve do zadnje objave, ko je bila stran osvežena. Običajno je na prevaranih ali ponarejenih spletnih straneh redko objavljen datum, ki bi bil starejši od enega meseca. Če se informacije podjetij ne ažurirajo ravno pogosto, je treba pregledati vse datume ažuriranja.

Pri oceni spletnih strani je zelo pomembno, da vemo, kdo so pokrovitelji spletne strani. Pregledati je treba tudi razširjenost URL[5]. Če je končnica nekomercialnega okolja na spletu *.org* (oznaka za organizacijo ali združenje), *.edu* (oznaka za izobraževalno ustanovo) ali *.gov* (oznaka za vladno ustanovo), potem so informacije relevantne. V Sloveniji se za vsemi oznakami vladnih ustanov, organizacij in izobraževalnih ustanov uporablja končnica *.si*. Če so na spletni strani prisotne spletne hipertekstualne povezave (hyperlinks) na notranjo spletno stran, moramo biti pazljivi na to, da ne zapustimo gostiteljeve strani. Izogibati se je treba tudi stranem, ki vključujejo nedokumentirane zgodovinske primere, kot je neverjeten rezultat ali neverjetna zgodba (Mintz 2002 ,157-160).

Anton Vedder (2001) tudi omenja, da mora biti pri ocenjevanju spletnih strani dejavna morala posameznika, kaj je dovoljeno za uporabo in kaj naj ne bi bilo dobro za uporabo. Zato poudarja naslednja vprašanja, kaj bi moral uporabnik sam sebe vprašati, zakaj potrebuje informacije. Prvo je, ali so vse slabe informacije na internetu vedno zanesljive za uporabo. Naslednje je, kako je informacija različna od drugih informacij, ki so dosegljive prek vira. Za Veddra so reševanja moralnih vprašanj bistvo ocenjevanja spletnih strani.

[5] URL (Uniform Resource Locators) je naslov spletnih strani v svetovnem spletu. Vsaka spletna stran ima edinstven naslov, ki jo enolično določa, prav tako, kot telefonska številka enolično določa telefonskega naročnika. URL naslov je sestavljen iz treh delov: določnika vrste protokola, označevalnika gostitelja oziroma računalnika, njegov bistveni del je IP naslov ali domensko ime (DNS), in označevalnika datoteke (E-uspeh.com 2009).

V empiričnem delu se pri evalvaciji spletnih strani osredotočam na kriterije za ocenjevanje internetnih virov, ki so jih objavili na Univerzi Britanska Kolumbija (Greenwood in Steyn 2009). Ti kriteriji kritično ocenjujejo spletne strani, ki se jim zdijo kibernetsko mimikretično sumljive. Tukaj lahko poudarim, da obstajajo tudi druge evalvacijske sheme, ki omogočajo ocenjevanje spletnih strani z uporabo kriterijev. Podobne inštrumente so razvili na Lesley University Library - razvita je bila leta 2008 (Lesley University webpage 2008) in Cornell University - razvita je bila leta 1998 (McMillin 1998).
Ti dve shemi sta premalo obsežni pri samih kriterijih, zato ju nisem uporabil, poleg tega je tudi veliko prekrivanj v sami vsebini evalvacijskih shem. Drugače bi bilo shemi koristno uporabiti sočasno z evalvacijsko shemo, ki sem jo uporabil v svoji analizi.

Evalvacijska shema, ki sem jo uporabil v svoji analizi, je razdeljena v šest kriterijev, glede na podana vprašanja, ki jih na originalni strani naj ne bi bilo, bi jih pa vsebovala samo kibernetsko mimikretična stran. Naj omenim, da s kibernetsko mimikretično spletno stranjo mislim na vse tiste lastnosti, ki jih spletna stran posnema ali preuredi v svojo korist. Več ko je vprašanj na katere lahko odgovorimo pritrdilno, manj je možnosti, da je stran narejena z namenom zlorabe, ter obratno, na več vprašanj ko odgovorimo negativno, več je možnosti, da je spletna stran narejena z namenom zlorabe.
V svoji empiriji bom po evalvacijski shemi evalviral pet (5) izbranih spletnih strani, so navedene v knjigi *Deception of Web* (Mintz 2005). V knjigi bralce nagovarjajo, naj poskušajo ugotoviti, ali so strani narejene za namen zlorabe.
Evalvacijsko shemo, ki jo bom uporabil, sta ustvarila Aleteia Greenwood in profesor Douw Steyn[6] (evalvacijska shema je v prilogi 7.1). Kriteriji evalvacijske sheme so: (1) avtorstvo ali vir spletne strani, (2) natančnost ali skrbnost pripravljene strani, (3) veljavnost spletne strani, (4) ne/pristranskost informacij na spletni strani, (5) zavarovanje spletne strani in (6) sam namen spletne strani.
Evalvacijska shema je tudi odličen priročnik za vsakega uporabnika, ki redno obiskuje splet, saj se lahko s tem izogne mnogim težavam, ki se pojavljajo na kibernetskem mimikretičnem področju spletnih strani. Vsak kriterij je tudi natančneje opredeljen, za kaj se ta kriterij uporabi pri evalvaciji spletne strani in kje se to pojavlja na spletu. Vsak

[6] Na univerzi Britanska Kolumbija Greenwood predava o znanosti in inženirstvu. Steyn pa poučuje okoljske znanstvene programe in atmosferski znanstveni program.

kriterij je temeljito utemeljen, zakaj se uporablja. Problem kriterijev je, da so premalo pojasnjeni kako naj kritično ocenimo, saj ne vemo, kateri so tisti znaki mimikrije na spletni strani, ki nas lahko zavedejo, saj jih ne opazimo. Zato sem se osredotočil le na tisti del kriterijev, ki naj bi najbolje pojasnili, kako naj kritično obravnavamo spletno stran.

Kriterij avtorja ali virov (1) je pomemben, če ne najdemo avtorja ali organizacije, ki nas povezuje na želeno stran takrat lahko hitro posumimo na mimikretično stran. Tudi če najdemo organizacijo ali avtorja, moramo biti še zmeraj previdni in poskušati najti informacije, ki so za nas relevantne. Če administrator spletne strani ni znan, je velika verjetnost, da je spletna stran kibernetsko mimikretična.
Kriterij natančnosti ali skrbnosti (2) je pomemben za kontrolo enakosti med objavljanjem v tradicionalnem tisku in objavljanjem na internetu. Ti vrsti objavljanja morata biti vsaj malo podobna druga drugi. Tukaj je predvsem mišljeno, da je spletna stran natančno opredeljena z informacijami, ki spletno stran bolje kvalitetno in bolj verjetno predstavijo. Izdelki za časopise, revije in periodični tisk so postali množično dostopni na internetu, kjer tudi dokazujejo natančnost ali skrbnost. Ta kriterij je tudi močno povezan z avtorjem spletne strani, saj je prav njegova lastnost ta, da skrbi za natančnost svoje predstavljene spletne strani.
Pod kriterij veljavnosti spletne strani (3) spada že sama vsebina strani, tako da bi ta kriterij lahko opredelili kot vsebinsko veljavnost. Za vsebinsko veljavnost je pomembno predvsem to, da ni mogoče natančno določiti, koliko je neka informacija na spletni strani sploh veljavna in relevantna. Iz same vsebine spletne strani ne moremo vedeti ali je na spletni strani kibernetska mimikrija, zato je treba informacije oceniti ali so relevantne za našo uporabo (Greenwood in Steyn 2009).
Relevantnost kot produkt veljavnosti je pomembna zato, da iščemo informacije ali podatke na spletni strani, ki so za uporabnika pomembni. Kriterij veljavnosti je pomemben zaradi veljavnosti informacij na spletni strani, saj je uporabnik določeno spletno stran obiskal zaradi želene vsebine (Ferligoj, Leskošek, Kogovšek 1995, 70-71). Veljavnost spletne strani je pomembna tudi zato, ker moramo pri informacijah vedeti, ali je posamezna informacija sploh veljavna za našo uporabo. To pomeni, da če informacija ni veljavna, potem obstaja možnost, da spletna stran ni narejena z namenom koristnosti za uporabnika.

Pomemben kriterij je tudi ne/pristranskost (4), ki nam pove, koliko so informacije, ki jih iščemo na želeni spletni strani, ne/pristransko relevantne. Ne/pristranskost je neke vrste že lahko prevara, vendar v latentnem smislu. Prevara v latentnem smislu pomeni predvsem napačne informacije za uporabnika. Ne/pristranskost je prevara predvsem takrat kadar je narejena z namenom prevare. Z ne/pristranskostjo mislim na to, koliko spletna stran vsebuje propagandnih sporočil, provokativnih izrazov in pristranskih informacij vsebuje spletna stran.

Kriterij obsega delovanja (5) na spletni strani deluje na principu, da v časovnem poteku ugotavljamo, kako se stran dopolnjuje in dograjuje. Obseg delovanja sem najtežje evalviral, saj bi bila zato potrebna nova shema, ki bi spremljala spletne strani skozi čas in ocenjevala njihovo konsistentnost in morebitno prisotnost kibernetske mimikrije.

Iz kriterija namena (6) spletne strani je razvidno ali je stran pozitivno ali negativno usmerjena. Če ima spletna stran pozitiven namen, je to lahko razvidno iz prodaje izdelkov, podane literature na strani, vizualne predstavitve spletne strani, dostopnih virov in objave člankov ali knjig. Če se pa se nam dozdeva, da so nameni spletne strani negativni, potem pa lahko predvidevamo, da je na spletni strani prisotna potegavščina ali prevara. Negativni namen lahko zaznamo predvsem s stališča, da se lahko prodajajo določeni izdelki, vendar prinašajo negativni namen (Greenwood in Steyn 2009).

S spletno evalvacijo želim ugotoviti, kako se pojavlja kibernetska mimikrija na obravnavanih spletnih straneh.

3.2 EMPIRIČNA EVALVACIJA SPLETNIH STRANI

V empirični del bom vključil pet (5) spletnih strani, na katerih bom opravil evalvacijo po shemi, ki sem si jo izbral za preverjanje kibernetske mimikrije teh spletnih strani. Glavno raziskovalno vprašanje je, kako se izoblikujejo veljavni in zanesljivi kriteriji z uporabo sheme za njihovo zaznavo, ki se kaže kot kibernetska mimikrija na spletnih straneh. Kot že omenjeno, so izbrane spletne strani navedene v knjigi *Deception of Web* (Mintz 2002). V knjigi so predlagane kot primeri spletnih strani, ki bi lahko bili olajšali razumevanje kibernetske mimikrije na spletu. Vendar moram poudariti, da teh spletnih strani ni še nihče kibernetsko mimikretično ocenil. Primer slovenske spletne strani nisem izbral, saj o tem obstaja malo virov in literature, tako da sem ostal le pri ameriških spletnih straneh. Spletne strani, ki so obenem enote opazovanja, so:

- American Cancer Society, dostopna na www.cancer.org (10. avgust 2009)
- Martin Luther King, Jr, dostopna na www.martinlutherking.org (10. avgust 2009)
- The White House, dostopna na www.whitehouse.net (10. avgust 2009)
- Halloween, its origins and customs, dostopna na www.jeremiahproject.com/halloween.html (10. avgust 2009)
- The White House, dostopna na www.whitehouse.gov (10. avgust 2009)

Teh pet (5) spletnih strani bom razporedil v tabelo (glej prilogo 7.2) in vsako posebej ocenil po omenjeni evalvacijski shemi. Vsaka trditev, ki je stran ne bo vsebovala, bo dobila vrednost nič (0), če pa jo bo vsebovala, bo dobila vrednost ena (1). Več ko bo imela stran vrednosti nič (0), bolj bo pripadala kibernetsko mimikretični strani in bo s tem bolj sumljiva za uporabo. Več kot bo pozitivnih vrednosti, bolj bo stran pristna in relevantna za uporabo ter s tem manj kibernetsko mimikretična. Nato bom med seboj primerjal posamezne kriterije in poskušal ugotoviti, kateri kriteriji so najbolj kibernetsko mimikretični in kateri najmanj. Izračunal bom tudi povprečja in ugotovil, kateri kriterij je najbolj kibernetsko mimikretičen. Iz povprečja bom lahko sklepal, kako in kje se kibernetsko mimikrijo najhitreje zazna in opredeli. Poskušal bom ugotoviti, ali si lahko s to shemo pomagamo kot uporabniki spletnih strani. S tem bom na koncu odgovoril na svoje glavno raziskovalno vprašanje ter to povezal s teorijo, iz katere sem črpal ideje za empirični del (Greenwood in Steyn 2009).

3.2.1 Sklep evalvacije spletne strani American Cancer Society

Spletna stran *'American Cancer Society'* ima v večini pozitivne odgovore (Tabela 7.6 v prilogi), tako da lahko sklepam, da spletna stran ni kibernetsko mimikretična. Informacije so relevantne. Avtorji so omenjeni pod vsakim člankom in vključeni v razne organizacije in društva. Povezave se dogajajo v večini samo znotraj strani, tako da nas ne povezuje na druge spletne strani, ki jih ne poznamo. Za spletno stran je odgovorno samo društvo, ki je tudi avtor te spletne strani. Stran je celotno objavljena in viri so dostopni. Na koncu vsakega članka na spletni strani je objavljen datum in stran je redno osvežena, kar pomeni, da jo predstavniki tega društva redno vzdržujejo. Na druge spletne strani se ne moremo povezovati, temveč samo med notranjimi stranmi. Na strani

ni reklamne propagande in neprimernih izrazov. Izrazoslovje je strokovno, saj vsebuje strokovne izraze iz medicine. Namen strani je pozitiven, daje občutek zaupanja, saj so članki aktualni glede na čas nastanka. Na strani je veliko informacij in virov, ki jih objavljajo tudi ugledne ustanove, kot je The American Cancer Society University. Spletna stran je varna za uporabo, saj iz dane sheme ni razvidno, da bi bila nevarna za uporabnika (podrobnejši predogled tabele v prilogi 7.1).

3.2.2 Sklep evalvacije spletne strani 'Martin Luther King, Jr.

Spletna stran *Martin Luther King, Jr.* je na prvi pogled zelo zavajajoča, saj ne poznamo točnih avtorjev ali institucij, ki bi jamčile za to, kar je napisano na strani. Na spletni strani ne najdemo niti avtorja niti kakšnih posebnih institucij. Opazimo nerelevantne vire in informacije, saj ne moremo preverjati ali so te informacije resnične, ker ni navedenih nobenih virov. Spletna stran nas zelo hitro preusmeri na drugo spletno stran, ki nima povezave z izvorno stranjo. Veliko je tudi rasističnega izražanja[7]. Na spletni strani ni enega datuma objave in elektronskega naslova. Spletna stran je videti kot propaganda, ki poveličuje rasizem in diskriminacijo. Veliko je tudi neresničnih podatkov o Martinu Luthru Kingu. Drugi viri, ki so na voljo za povezavo na druge spletne strani, so nerelevantni, saj so strani prav tako kibernetsko mimikretične. Iz tega lahko sklepam, da so spletne strani, ki so kibernetsko mimikretične, med seboj povezane, saj s tem prikazujejo svojo podobo spletne strani bolj pristno, čeprav to v resnici ne velja. To bi lahko poimenovali tudi podporni mimikretični signali. Ti posameznika zavedejo v svoji podobnosti in prekritosti spletne strani. Spletna stran je zelo sumljiva za uporabo ter za uporabnike. Stran je kibernetsko mimikretična, saj prikriva bistvo spletne strani in širi informacije, ki niso popolnoma resnične, saj ne govorijo o dokazih, ki so dostopni prek uradnih virov, kot so npr. knjige o Martinu Luthru Kingu. Spletna stran kot je *Martin Luther King, Jr.* je neugodna predvsem za tiste uporabnike, ki so manj izobraženi ali naivni (podrobnejši predogled tabele v prilogi 7.2).

[7] Npr. da je Martin Luther King ml. širil neresnice o belcih in želel črnsko prevlado v ZDA.

3.2.3 Sklep evalvacije spletne strani 'The White House.net'

Spletna stran *The White House.net* je značilna ponarejena spletna stran, ki sporoča provokativna in žaljiva sporočila. Spletna stran je kibernetsko mimikretična, saj uporabnikom prikaže, kako lahko pridejo na vladno stran tuji hekerji in jo oponašajo. Spletna stran nima niti znanih avtorjev niti povezave s katerokoli drugo stranjo, ki bi jo povezovala. Namen strani je skrajno negativen in že na meji komičnosti. Sam namen strani je, da sporoča provokativnost, poleg tega kaže na to, da so spletne strani močno podvržene prevaram. Spletna stran tudi ni dokončana, saj je nekako 'ukradena'. Zanimivo je, da se iz te spletne strani zelo lahko dostopa do originalne spletne strani vlade. Ta spletna stran ni dobra za uporabo in tudi ne za sam splet. Hekerji so na njej sporočali svojo prisotnost. Na strani so vidni tudi drugi kibernetsko mimikretični znaki. Znaki so, da spletna stran ni celotno objavljena, temveč delno ter delno ponarejena, vsebuje propagandna sporočila in je pristranska pri informacijah. Na spletni strani so tudi lažne informacije in žalitve (podrobnejši predogled tabele v prilogi 7.3).

3.2.4 Sklep evalvacije spletne strani Halloween, its origins and customs

Spletna stran *Halloween, its origins and customs* je dobila večino pozitivnih odgovorov, kar nakazuje, da stran ni kibernetsko mimikretična, temveč pristna za uporabo. Tudi članki na strani so zelo uporabni in nam nakazujejo, da si lahko več o tem preberemo na drugih dostopnih virih. Avtorji so jasno določeni za vsak članek kot tudi avtorji strani. Informacije na strani so relevantne in zanimive za uporabo. Informacije tudi niso zgodovinsko sporne glede na točno objavljanje iz strani v knjigah. Stran ima ogromno dostopnih virov, članki so aktualni in sam namen strani je pozitiven. Spletna stran ne vsebuje provokativnih jezikovnih izrazov in propagandnih sporočil. Vsebuje veliko vizualnih predstavitev, ki kažejo na pozitivno usmerjenost spletne strani. Sama predstavitev spletne strani je aktualna. Vendar spletna stran vseeno vsebuje nekaj kibernetsko mimikretičnih znakov. Mimikretični znaki so, da ni popolnoma jasno, kdo sproti vzdržuje spletno stran in objavlja novice ni popolnoma jasno, ali to stran vzdržuje in osvežuje več avtorjev ali kdo drug, ki ni popolnoma znan. A kljub temu je spletna stran še varna za uporabo, saj ne vsebuje glavnih kibernetskih mimikretičnih lastnosti (podrobnejši predogled tabele v prilogi 7.4).

3.2.5 Sklep evalvacije spletne strani The White House.gov

Spletna stran *'The White House.gov'* ne kaže znakov kibernetske mimikrije. Nasprotno je od *The White House.net*, zelo kibernetsko mimikretična. Spletna stran nima nobenih znakov, da bi bila sumljiva, saj vsebuje vse kriterije, ki so nakazani v obravnavani shemi. Spletna stran je pristna in varna za uporabnike in iskalce informacij na spletu. Predstavniki takih strani bi naredili splet varnejši za uporabo, vendar to dejansko ni mogoče, zato morajo uporabniki paziti, kaj počnejo na določenih kibernetsko mimikretičnih straneh. Če to spletno stran primerjamo s spletno stranjo *The White House.net,* lahko ugotovimo, da je ta stran ponarejena znotraj vladne strani. Kot je očitno, lahko kateri koli spletni heker v nekaj korakih vdre na katerokoli spletno stran. Očitno je spletna stran slabo varovana ter zato lahka tarča za hekerje z vsega sveta. Čeprav hekerji direktno ne povzročajo negativnih posledic, lahko vseeno vdirajo in spreminjajo spletne strani v kibernetsko mimikretične. Ta spletna stran je primer nekibernetske mimikretične spletne strani in s tem pozitivno naravnane strani. Tudi take strani, ki v bistvu niso kibernetsko mimikretične in so pristne glede informacij in namenov, lahko hitro postanejo tarča kibernetsko mimikretičnih spletnih strani. To sem tudi ugotovil iz same analize spletnih strani, ko sem evalviral spletno stran *The White House.net* (podrobnejši predogled tabele v prilogi 7.5).

3.2.6 Sklepne ugotovitve glede vseh spletnih strani

Ker sem si izbral pet (5) spletnih strani, je bilo pri vsakem kriteriju možnih pet (5) odgovorov z DA ali NE. Več ko je bilo odgovorov z 'ne', večja je bila možnost pojava kibernetske mimikrije in več ko je bilo odgovorov 'da', manjša je bila možnost kibernetske mimikrije. Najbolj problematično je bilo ugotoviti kibernetsko mimikrijo spletnih strani pri odgovornosti za spletno stran in kdaj je bila spletna stran nazadnje osvežena. Največ kibernetske mimikrije se kaže pri statističnih podatkih, ki lahko najbolj zavedejo uporabnika. Problem je tudi pri pristranskosti same spletne strani. Pri večini spletnih strani ni problematično povezovanje do drugih spletnih strani in prikazovanje virov, temveč ali so viri relevantni kot predstava informacij. Spletne strani so po navadi tudi celotno objavljene.

V analizi teh petih spletnih strani opažam, da so v povprečju manj kibernetsko mimikretične kot se zdi na prvi pogled. Vendar se vseeno gibljejo okoli povprečja, saj

sta dve (2) spletni strani kibernetsko mimikretični (to sta strani *Martin Luther King Jr*. in *The White House.net*) in dve (2) nista kibernetsko mimikretični (to sta *The White House.gov* in *American Cancer Society*), ena (1) pa ima znake kibernetske mimikrije (stran *Halloween, its origins and customs*).
Najbolj sta problematična kriterija kibernetske mimikrije glede veljavnosti same spletne strani in nepristranskosti, najmanj pa obseg delovanja in sam namen spletne strani.
Najbolj kibernetsko mimikretični sta bili spletni strani *The Martin Luther King Jr.* in *The White House.net*, saj je iz analize očitno, da sta strani tvegani za uporabo in sem ju tudi kritično ocenil. Ti dve spletni strani vsebujeta vse kriterije kibernetske mimikrije.
Najmanj ali skoraj nič sta bili kibernetsko mimikretični spletni strani *The White House.gov* in *American Cancer Society*, ki sta po oceni sheme najbolj varni za uporabnike, saj so informacije pristne in relevantne. Informacijam na teh dveh straneh lahko uporabnik najlažje zaupa in je najtežje prevaran s strani ponudnika te strani. Čeprav je kibernetsko mimikrijo težko ocenjevati na spletni strani, je bilo z uporabo sheme to lažje izvesti, ker je shema objektivno naravnana, saj deluje tako, da samo potrdimo, ali je na spletni strani določena lastnost prisotna ali ne. Najpomembnejša ugotovitev iz analize spletnih strani po shemi je, da se kibernetska mimikrija na spletnih straneh pojavlja predvsem v sami vsebini spletne strani.

Iz sheme je razvidno, da več ko je negativnih odgovorov, več je na spletni strani kibernetske mimikrije. Shema omogoča, da s pomočjo posameznih kriterijev ugotovimo koliko je spletna stran zavajajoča za uporabnika. Shema je pokazala, da se največ kibernetske mimikrije pojavlja na področju natančnosti ali skrbnosti za spletno stran. To pomeni, da je zelo pomembno, da je na spletni strani prisotna formalna oseba, ki skrbi za spletno stran. To je največkrat administrator. Pomembno je tudi, da je administrator dostopen prek elektronskega sporočila ali telefona. Shema je pokazala, da je kibernetska mimikrija prisotna, če ni znan avtor, skupina, organizacija, institucija ali vladno telo. Shema je tudi pokazala, da je spletna stran manj zavajajoča, če obstajajo povezave na druge spletne strani in če lahko stran preverjamo z biografskimi ali drugimi viri. Pomembna je tudi predstavitev spletne strani v pomenu, da več ko je ponudb in reklam na spletni strani bolj je prisotna kibernetska mimikrija. Za kibernetsko mimikretične spletne strani je značilno, da preusmerjajo pozornost od pomembnih stvari za uporabnika na nepomembne privlačne vsebine (podrobnejši predogled sheme v prilogi 7.6).

Povprečje petih (5) spletnih strani, pomeni, da se na dveh spletnih straneh kažejo znaki kibernestske mimikrije. Na svetovnem spletu se pojavlja množično mimikretično posnemanje spletnih strani. To lahko potrdim iz svoje empirije, saj je na spletni strani *The White House.net* nekaj hekerjev resnično uporabilo prevaro, da bi pridobilo določeno prednost, ki je v njihovem primeru bila sporočilo. Tudi s Charlesom Babbegom (v Mali 2002) se lahko strinjam, da so tudi zavestne prevare del kibernetske mimikrije, saj gre za premišljeno ponarejanje znanstvenih poskusov z namenom ogoljufati ali napačno informirati znanstveno javnost. Prav tako pritrjujem Paulu Piperju (v Mali 2002), da so ponarejene spletne strani v preobleki predstavljale legitimne strani z namenom razširjanja dezinformacij.

Tudi to je razvidno iz evalvacije spletne strani *The White House.net*: na tej strani iščemo informacije, za katere mislimo, da so legitimne, ter nato ugotovimo, da se stran samo skriva pod navidezno legitimnostjo, vendar je v resnici popolnoma dezinformacijska, kar potrjuje, da gre za kibernetsko mimikrijo.

Spletno stran *Martin Luther King Jr.* lahko označimo kot spletno stran, ki se predstavlja kot povsem izmišljena stran. Izmišljene ali fiktivne strani močno zavajajo posameznika in tudi organizacije. Take strani so popolnoma izmišljene samo zaradi koristi tistih posameznikov, ki si resnično želijo manipulirati z drugimi.

Lahko se tudi strinjam z Mario Bakardjievo (2002), da običajni uporabnik interneta nima pomembnega vpliva na dogodke, ki se mu lahko dogodijo ob uporabi spletnih strani. Problem v kibernetskem mimikretičnem prostoru je tudi v tem, da ne moremo nadzirati samih dogodkov, saj se hitro spreminjajo z razvojem informacijskih komunikacijskih tehnologij.

Ponarejene strani so tiste spletne strani, ki so lažne in sporočajo lažne informacije. V našem primeru vsebujeta obe spletni strani ponarejene kibernetske elemente, to sta stran *Martina Luther King Jr.* kot stran *The White House.net.* Namere ponarejenih spletnih strani lahko razdelimo za politične namene in za zabavništvo. Tako lahko stran '*Martin Luther King Jr.*' označimo za politični namen ponarejene strani, medtem ko je namen strani *The White House.net* predvsem za zabava. Dejavnike, ki sem jih omenjal v teoriji kibernetske mimikrije, sem zaznal tudi v empiričnem delu.

4 ZAŠČITA UPORABNIKA PRED KIBERNETSKO MIMIKRIJO

Uporabnik se pred mnogimi mimikretičnimi prevarami zavaruje tako, da postane bolj pozoren na zavajajoče spletne strani, ki jih uporablja (Nasvet 2009). Pri tem si lahko pomagamo z omenjeno evalvacijsko shemo, saj z njo kritično ovrednotimo spletno stran, še preden pričnemo brati razne informacije in/ali pošiljati svoje osebne podatke. Če uporabimo shemo, pri ocenjevanju hitro zaznamo znake prevare. Iz sheme lahko razberemo, ali gre za izmišljeno stran ali za ponarejeno. Težje pa ugotovimo, ali so informacije na strani relevantne in resnične.

Kibernetska mimikrija spletnih strani ni le izraz za prevare, temveč usmerja pozornost na to, kako odkriti mimikrijo na določeni spletni strani. To ugotovimo tako, da najprej pregledamo, kdo je avtor spletne strani, če tega ni, pogledamo osebne podatke na strani, ki so ponavadi dostopni pri kontaktih. Če upoštevamo, da se posameznik bolj varno počuti pri uporabi interneta, je to koristna zaščita.

Sam namen spletne strani je lahko družbeno mimikretičen: ta lastnost se lahko spremeni v kibernetsko mimikrijo. Če znamo oceniti kibernetsko mimikrijo, nam ni treba poznati bolj specifičnih podrobnosti o spletni straneh. Za oceno kibernetske mimikrije lahko uporabimo samo dele ali določene kriterije sheme, ki sem jo uporabil v evalvaciji. Zaščita uporabnika in ocena spletne strani sta medsebojno odvisni in ne moreta obstajati druga brez druge.

Lahko omenim tudi Antona Veddra (2001), ki je omenjal moralo uporabnika spletnih strani, da mora tudi sam uporabnik razviti odnos do tega, kaj je relevantna informacija, ki jo nam jo ponuja spletna stran. Bistveno je, da uporabnik loči med pozitivnim in negativnim namenom spletne strani, ki je seveda subjektivno orientiran. Uporabnik je ključni element za mimika, da ga le-ta lahko prevara, zato je pomembno, da se uporabnik usposobi, da ga mimik ne more prevarati. Uporabnik mora postati bolj premišljen in previden od mimika, ki ustvari spletno stran z določenim namenom okoriščanja.

5 ZAKLJUČEK

Kot sem ugotovil v empiričnem delu, se kibernetska mimikrija lahko pojavlja na določenih spletnih straneh, vendar je to težko zaznati. Najbolj pogost znak kibernetsko mimikretične strani je ponarejanje ali hlinjenje drugih spletnih strani, ki so širše prepoznavne po svoji obliki in vsebini kot kredibilne spletne strani.

Pri pisanju diplomske naloge sem ugotovil, da je kibernetska mimikrija spletnih strani resen problem na internetu. Zelo močan del kibernetske mimikrije je širjenje napačnih informacij uporabnikom z namenom prevarati jih na katerikoli način. To sem ugotovil iz svojih dveh analiz spletnih strani, npr. spletna stran *The White House.net* je ponaredek originalne spletne strani *The White House.gov'*, ponarejena stran je narejena samo za prenašanje napačnih informacij za uporabnikom.

Kibernetska mimikrija je fenomen tudi na informacijsko-komunikacijskem področju, saj omogoča tehnološki potencial za posameznike, ki so družbeno mimikretični. Najbolj so nevarne tiste spletne strani, ki dajejo uporabniku neko upanje, da bodo nekaj pridobil, npr. denar, izdelek ali nagrado, vendar se to po navadi obrne v napačno smer. Najbolj so kibernetske tiste spletne strani, ki proizvajajo lažne informacije za uporabnike. K temu veliko pripomore tudi sama potrošniška družba, ki nekako sili posameznika, da se spušča v prostore kibernetike, kjer so prevare prisotne na vsakem koraku. Tukaj gre predvsem za odločitve posameznikov in ne toliko za tehnologijo, ki omogoča kibernetsko mimikrijo. Na učinek kibernetske mimikrije vpliva tudi predznanje uporabnika o spletnih straneh.

Ugotovitve iz empiričnega dela so potrdile, da so kriteriji, po katerih sem zaznal uporabnost sheme, koristni za uporabnike, da ocenijo spletno stran, še preden jo pričnejo uporabljati. Kriteriji so se izkazali za veljavne indikatorje za zaznavanje mimikretičnih spletnih strani.
Glavni namen kibernetsko mimikretičnih spletnih strani je dobiti korist od uporabnika spletne strani, tako da je oškodovan na področju, kjer tega ne pričakuje. Najbolj pomembno je, da uporabnik spletne strani uporablja tako, da jih tudi sproti ocenjuje, da poskuša preprečiti prevaro, ki se mu lahko zgodi, če je ne opazi oziroma ni pozoren.

Kibernetski prostor je prostor, poln svobode, in s tem tudi prevar in poneverb spletnih strani. Mimikrija se tukaj kot oznaka pojavlja v tem smislu, da se spletna stran pretvarja za nekaj, kar v resnici ni. Lahko tudi pričakujemo, da bolj ko bo tehnologija spleta zapletena, več bo tudi kibernetske mimikrije. To je mogoče primerjati s samo družbo, saj je razvidno, da bolj ko se družbe razvijajo iz tradicionalnih v moderne ter iz materialno vrednostno usmerjenih v postmaterialne, več mimikrije je zaznati pri dejanjih posameznikov, korporacij, družb itd.
Menim, da se v tem primeru kibernetska mimikrija pojavlja ne glede na kulturo, prostor, čas, jezik in programski jezik, ki je zlorabljen v ta namen.

Lahko dodam, da je kibernetska mimikrija še relativno neraziskano področje družbene mimikrije, tako v svetu kot tudi pri nas. Tudi literature ni veliko o sami kibernetski mimikriji. Zato bi bilo tudi dobro, da bi se pričelo raziskovati kibernetsko mimikrijo kot pojav, ki prinaša škodo za uporabnikom in družbi. Kibernetska mimikrija dobi moč, ko ji uporabnik interneta verjame, ko napačna informacija postane prava informacija.

Dobro bi bilo izoblikovati univerzalno shemo za preverjanje ne/mimikretičnosti spletnih strani, hkrati pa se zavedam, da bi bila to težka in/ali tvegana naloga, saj se mimikrija spletnih strani pojavlja v različnih oblikah ter se spreminja s časom in novimi tehnologijami.
Menim, da bi bilo dobro, če bi bili uporabniki bolj ozaveščeni o tovrstnih prevarah. Tako bi bilo dobro na tem področju opraviti podrobnejše raziskave, da bi se bolj zavedali mnogoterih razsežnosti kibernetske mimikrije in bi s tem pripomogli k večji strokovnosti na tem področju tudi v Sloveniji.

6 LITERATURA

ARNES, Akademska in raziskovalna mreža Slovenije. 2004. *SI-CERT 2004-06/«Phishing«-nova oblika spletne prevare (kraja)*. Dostopno prek: http://www.arnes.si/si-cert/obvestila/2004-06.html (17. avgust 2009).

Bakardjieva, Maria. 2005. *Internet society: the internet in everyday life*. London: Thousand oaks, New Delhi: Sage.

Dokl, Jure. 2006. *Internet in koncept človekove varnosti.* Diplomsko delo. Ljubljana: FDV.

E-uspeh.com. 2009. *Kaj je URL*? Dostopno prek: http://www.e-uspeh.com/pomoc/kaj-je-url.htm (17. avgust 2009).

Ferligoj, Anuška, Karmen Leskošek in Tina Kogovšek. 1995. *Zanesljivost in veljavnost merjenja.* Ljubljana: FDV.

Gambetta, David. 2005. *Deceptive Mimicry in Humans*. Cambridge in London: The M.I.T Press. Dostopno prek: http://www.nuffield.ox.ac.uk/users/gambetta/Deceptive %20Mimicry.pdf (17. avgust 2009).

Greenwood, Aleteia in Douw Steyn. 2009. *Criteria for Evaluating Internet Resources*. Science and Engineering: UBC Library University of British Columbia. Dostopno prek: http://www.library.ubc.ca/home/evaluating/ (17. avgust 2009).

Gruban, Andreja. 2003. *Družbeni in znanstveni vidiki (kraje) intelektualne lastnine*. Diplomsko delo. Ljubljana: FDV.

Hafner, Špela. 2006. *Internetne prevare na spletnih dražbah*. Diplomsko delo. Ljubljana: EF.

Lachmann, Michael in Bergstrom, T. Carl. 2004. The disadvantage of combinatorial communication. *Proceedings of the Royal Society of London ß.* 271: 2337-2343.

Dostopno prek: http://octavia.zoology.washington.edu/publications/publications.html (17. avgust 2009).

Lesley University webpage. 2008. *Evaluating web sites*. Cambridge: Lesley University. Dostopno prek: http://web.lesley.edu/default.asp (17. avgust 2009).

Mcmillin, Paul. 1998. *Five criteria for evaluating Web pages*. Cornell University Library: Ithaca NY. Dostopno prek: http://www.library.cornell.edu/olinuris /ref/webcri t.ht ml (17. avgust 2009).

Microsoft. *Zaščitite se. Varnost na spletu se začne pri vas*. Dostopno prek: http://download.microsoft.com/download/0/9/.../zascitite%20se-03.pdf (17. avgust 2009).

Mintz, Anna P. 2002. *Web of deception: Misinformation on the internet*. New York: CyberAge Book.

Nasvet. 2009. *Internetne prevare in potegavščine*. Dostopno prek: http://www.nasvet.com/ internet-prevare/ (17. avgust 2009).

RTVSLO. 2006. *Klik NLB opozarja pred ponaredki*. Dostopno prek: http://www.rtvslo.si/slovenija/klik-nlb-opozarja-pred-ponaredki/62646 (17. avgust 2009).

SK EUR-Lex. 2008. *Evropski parlament*. Dostopno prek: http://eur-lex.europa.eu/Notice.do?mode=dbl⟨=sl&ihmlang=sl&lng1=sl,sk&lng2=bg,cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,mt,nl,pl,pt,ro,sk,sl,sv,&val=485805:cs&page= (17. avgust 2009).

Smrke, Marjan. 2007. *Družbena mimikrija*. Ljubljana: FDV.

Vedder, Antonio. 2001. *Misinformation through the internet: epistemology and ethics*. Antwerpen, Groningen, Oxford: Intersentia.

7 PRILOGE

PRILOGA A: Shema: Kriteriji za evalvacijo internetnih virov (Aletei Greenwood in Douw Steyn)

Author or source	• Is there an author of the work? If so, is the author clearly identified? • Are the author's credentials for writing on this topic stated? • Is the author affiliated with an organization? • Does the site or page represent a group, organization, institution, corporation or government body? • Is there a link back to the organization's page or a way to contact the organization or the author to verify the credibility of the site (address, phone number, email address)? • Is it clear who is responsible for the creation and/or maintenance of the site or page? **Why Question the Author or Source of a Web Page?** It is important to ask these questions because often we are taught to believe that what we read in a magazine or book, or on the Web, is true. But this is not necessarily the case. If you cannot find an author or an organization connected to a website be very, very suspicious. If no one wants to stand behind the creation of the page why should you believe what is written there? Even if you can find an organization or author you still need to be cautious and make sure that the organization and/or author are who they say they are. This may include further research on a particular author or organization.
Accuracy	• Is this page part of an edited or peer-reviewed publication? • Can factual information be verified through footnotes or bibliographies to other credible sources? • Based on what you already know about the subject, or have checked from other sources, does this information seem credible? • Is it clear who has the responsibility for the accuracy of the information presented? • If statistical data is presented in graphs or charts is it labeled clearly? • Look at the Aspartame website and ask yourself if the information seems credible and accurate. **Why Question the Accuracy of a Web Page?** In terms of quality control, the world of traditional print publishing and the Internet bear little resemblance to each other. In the scholarly publication process there are a number of steps an article goes through before editors and referees decide whether or not to publish it. When an author submits an article an editor can assign it to two, sometimes as many as four, independent referees. This is called the peer-review process. The referees review the article and write reports that recommend acceptance, acceptance with minor changes, acceptance with major changes, or rejection. Final acceptance rates are about 30%, and the entire process can take up to a year. It used to be possible to say that in *general* on the Web there are no editors (unlike most print publications). But now it is possible to find many edited documents and peer-reviewed ejournals available on the Web. It could be said though, that there are few editors *of* the Internet. There is no system in place, for the entire Internet, for people to proofread and "send back" or "reject" a document until it meets the standards of a publishing house's reputation. This lack of review and revision process means that not all Web pages are reliable or valuable. Documents can easily be copied and falsified, or copied with omissions and errors - intentional or accidental. Articles from journals, magazines and periodicals are becoming increasingly available through the Internet. The table below shows some of the characteristics of scholarly and popular journals. Not all the criteria will be met for every journal, and there will be exceptions, but being aware of the differences will assist you to select sources appropriate to your research needs. **Scholarly Journals** **Popular Magazines**

Examples	Journal of the American Medical Association (JAMA) Water, Science and Technology Foreign Affairs Science Nature	Time Newsweek Psychology Today
Authors	Researchers Professors Scholars Professionals who are usually experts in narrow fields	Journalists Lay people Anonymous
References	Includes references, bibliographies or footnotes	Rarely includes references, bibliographies or footnotes
Edited by?	Submitted articles are subjected to a rigorous peer-review process by researchers, professionals and/or students of the field	Submitted articles may be reviewed by journalists and lay people
Language	Specialized language of the discipline is used Often includes tabulated data, graphs and diagrams	Language is non-technical
Contents	Always includes an abstract Lengthy articles of original research In-depth analysis of topic Substantial book reviews	Shorter articles of general interest Coverage of current events/news Some brief book reviews
Presentation and Graphics	Less flashy, more "serious" in appearance Advertisements are rare (an exception is medical journals) Articles are often divided into explicitly named (and sometimes numbered) sections	More eye-catching appearance Many pictures Many advertisements
Where Indexed?	Found in specialized indexes such as Anthropological Index Georef Medline	Found in general periodical indexes such as Academic Search Elite Canadian Periodical Index Reader's Guide Abstracts (But keep in mind that general periodical indexes also include scholarly materials)

	Sloppy or poorly put together graphs or charts should be regarded with suspicion. Not only is such information difficult to use, it is also inconsistent with quality research from a credible source and should lead you to suspect the accuracy of the information on the page. Regarding the Aspartame website: Some of the clues that tell you to be cautious about the information on this page are: visually it is all over the place, the bold letters, the bright colours, the liberal use of exclamation marks. But there are testimonials and doctors opinions and those can be convincing to some people.
Currency	• Is there a date stating when the document was originally created? • Is it clear when the site or page was last updated, revised or edited? • Are there any indications that the material is updated frequently or consistently to ensure currency of the content? • If there are links to other Web pages are they current? **Why Question the Currency of a Web Page?** Currency of information is particularly important in the Sciences as findings can change drastically in short periods of time. How current the Web page or site you are looking at is relevent because if you are going to use information from a site you want to know that the information is updated or revised if necessary, or at the very least that the page is looked at and maintained by the webmaster with some consistency. The date showing the currency of a site is usually near the bottom of the page. If links to other Web pages are not current this is a fairly good sign that the site is not well-maintained.
Objectivity	• Is the page free of advertising? If the page does contain advertising, are the ads clearly separated from the content? • Does the page display a particular bias or perspective? Or is the information presented factually, without bias? • Is it clear and forthcoming about its view of the subject? • Does it use inflammatory or provocative language? **Why Question the Objectivity of a Web Page?** If advertisements are present look for a relationship between the content of the page and the advertising. Are the advertising and content connected? Ask yourself if the sponsors of the advertisements could have sponsored the research reported on a Web site. For example: You find a Web page about a vitamin supplement and the page has advertisements flashing over it, selling the same health supplement. Be cautious and sceptical that the content of the page is without bias. Make sure that the information is factual, not just testimonials of satisfied 'customers'. Check other sources to verify the information. Look closely at how information is presented. Are opinions clearly stated, or is the information vague? It is acceptable for a page to present a biased opinion, but you as the consumer of the information should know what that opinion is, it should be clear, not hidden.
Coverage	• Is there any indication that the page is complete and is not still under construction? • If there is a print equivalent to the Web page, is there clear indication of whether the entire work or only a portion is available on the Web? **Why Question the Coverage of a Web Page?** If there is any indication that the page is still under construction it may be better not to use it, as aspects of the page, as well as the information on it, may change by the time it is finished. If you find an excellent page and feel you simply must use it, but it is still under construction, it may be a good idea to include that fact in your bibliography. Your professor may see a different page than the one you referenced by the time you hand in your finished paper. If you are looking at a Web page for which there is a print equivalent check to see if the entire work is on the Web page. If it is a portion of the work make sure that quotes have not been taken out of context or information has not been misrepresented.
Purpose	• What is the primary purpose of the page? To sell a product? To make a political point? To have fun? To parody a person, organization or idea? For examples of web site parodies

	see: Dihydrogen Monoxide Feline Reactions to Bearded Men • Is the page or site a comprehensive resource or does it focus on a narrow range of information? • What is the emphasis of the presentation? Technical, scholarly, clinical, popular, elementary, etc. **Why Question the Purpose of a Web Page?** If the primary purpose of the Web site is to sell a product make sure the information is not biased if you are thinking of using it for a research paper. If the primary point is to have fun, or parody a person or organization you may not want to use it as a reference for a research paper, unless your paper has to do with Web site hoaxes. If a site or page is not comprehensive, and focuses on a narrow range of information it might be still be useful, just remember to look at the page critically. If a page has a narrow focus try to make sure that relevant information has not been left out.

Vir: Greenwood in Steyn (2009).

PRILOGA B: Tabele evalvacij spletnih strani

Tabela 7.1: Evalvacija spletne strani American Cancer Society

Kriteriji	Vprašanja	Pozitivni ali negativen odgovor (pozitiven odgovor 1 točko in negativen 0 točk)
Avtor ali vir	Je omenjen avtor dela ali bolj jasno identificiran?	Da
	Ali obstaja priporočilo za pisanje na to temo?	Da
	Ali je avtor včlanjen v kako organizacijo?	Da
	Ali stran predstavlja skupino, organizacijo, institucijo, združenje ali vladno telo?	Da
	Je povezava vrnjena nazaj na organizacijsko stran ali je povezana z avtorjevo stranjo (naslov, Telefonska številka, email naslov)?	Da
	Je jasno kdo je odgovoren za ustvarjeno ali vzdrževano stran?	Da
Natančnost/skrbnost	Je stran celotno objavljena?	Da
	Ali lahko informacije preverjamo preko bibliografskih ali drugih virov?	Da
	Je natančno določeno kdo je odgovoren za skrbnost predstavitve strani?	Da
	Ali so na strani predstavljeni statistični podatki, kot so grafi ali stolpci, ki bi bili nerelevantni?	Ne
Veljavnost	Ali obstaja stanje podatka, ko je bil dokument izvorno ustvarjen?	Da
	Je jasno razvidno kje je bila stran nazadnje osvežena, objavljena ali prenovljena?	Da
	Ali obstajajo povezave na druge spletne strani?	Da

Nepristranskost	Ali stran ne vsebuje propagandnih sporočil?	Da
	Ali spletna stran ne prikazuje pristranskosti?	Da
	Ali stran ne vsebuje rabo vnetih ali provokativnih jezikovnih izrazov?	Da
Obseg delovanja	Ali je stran dokončno narejena in zaključena?	Da
Namen	Ali je namen strani pozitiven?	Da
	Je stran obsežna z viri?	Da
	Ali ima stran omenjen dostop do informacij?	Da
	Ali je poudarek na predstavitvi aktualen?	Da
Vsota pozitivnih oziroma negativnih odgovorov		20 pozitivnih odgovorov in 1 negativen odgovor

Tabela 7.2: Evalvacija spletne strani Martin Luther King, Jr

Kriteriji	**Vprašanja**	**Pozitivni ali negativen odgovor (pozitiven odgovor 1 točko in negativen 0 točk)**
Avtor ali vir	Je omenjen avtor dela ali bolj jasno identificiran?	Ne
	Ali obstaja priporočilo za pisanje na to temo?	Ne
	Ali je avtor včlanjen v kako organizacijo?	Ne
	Ali stran predstavlja skupino, organizacijo, institucijo, združenje ali vladno telo?	Ne
	Je povezava vrnjena nazaj na organizacijsko stran ali je povezana z avtorjevo stranjo (naslov, Telefonska številka, email naslov)?	Ne
	Je jasno kdo je odgovoren za ustvarjeno ali vzdrževano stran?	Ne
Natančnost/skrbnost	Je stran celotno objavljena?	Da
	Ali lahko informacije preverjamo preko bibliografskih ali drugih virov?	Da
	Je natančno določeno kdo je odgovoren za skrbnost predstavitve strani?	Ne
	Ali so na strani predstavljeni statistični podatki, kot so grafi ali stolpci, ki bi bili nerelevantni?	Ne
Veljavnost	Ali obstaja stanje podatka, ko je bil dokument izvorno ustvarjen?	Ne
	Je jasno razvidno kje je bila stran nazadnje osvežena, objavljena ali prenovljena?	Ne
	Ali obstajajo povezave na druge spletne strani?	Da
Nepristranskost	Ali stran ne vsebuje propegandnih sporočil?	Ne
	Ali spletna stran ne prikazuje pristranskosti?	Ne

	Ali stran ne vsebuje rabo vnetih ali provokativnih jezikovnih izrazov?	Ne
Obseg delovanja	Ali je stran dokončno narejena in zaključena?	Da
Namen	Ali je namen strani pozitiven?	Ne
	Je stran obsežna z viri?	Da
	Ali ima stran omenjen dostop do informacij?	Da
	Ali je poudarek na predstavitvi aktualen?	Ne
Vsota pozitivnih oziroma negativnih odgovorov		6 pozitivnih odgovorov in 15 negativen odgovor

Tabela 7.3: Evalvacija spletne strani The White House.net

Kriteriji	**Vprašanja**	**Pozitivni ali negativen odgovor (pozitiven odgovor 1 točko in negativen 0 točk)**
Avtor ali vir	Je omenjen avtor dela ali bolj jasno identificiran?	Ne
	Ali obstaja priporočilo za pisanje na to temo?	Ne
	Ali je avtor včlanjen v kako organizacijo?	Ne
	Ali stran predstavlja skupino, organizacijo, institucijo, združenje ali vladno telo?	Ne
	Je povezava vrnjena nazaj na organizacijsko stran ali je povezana z avtorjevo stranjo (naslov, Telefonska številka, email naslov)?	Ne
	Je jasno kdo je odgovoren za ustvarjeno ali vzdrževano stran?	Ne
Natančnost/skrbnost	Je stran celotno objavljena?	Da
	Ali lahko informacije preverjamo preko bibliografskih ali drugih virov?	Da
	Je natančno določeno kdo je odgovoren za skrbnost predstavitve strani?	Ne
	Ali so na strani predstavljeni statistični podatki, kot so grafi ali stolpci, ki bi bili nerelevantni?	Ne
Veljavnost	Ali obstaja stanje podatka, ko je bil dokument izvorno ustvarjen?	Ne
	Je jasno razvidno kje je bila stran nazadnje osvežena, objavljena ali prenovljena?	Ne
	Ali obstajajo povezave na druge spletne strani?	Da
Nepristranskost	Ali stran ne vsebuje propagandnih sporočil?	Ne
	Ali spletna stran ne prikazuje pristranskosti?	Ne
	Ali stran ne vsebuje rabo vnetih ali provokativnih jezikovnih izrazov?	Ne
Obseg delovanja	Ali je stran dokončno narejena in	Ne

	zaključena?	
Namen	Ali je namen strani pozitiven?	Ne
	Je stran obsežna z viri?	Ne
	Ali ima stran omenjen dostop do informacij?	Da
	Ali je poudarek na predstavitvi aktualen?	Ne
Vsota pozitivnih oziroma negativnih odgovorov		3 pozitivnih odgovorov in 18 negativen odgovor

Tabela 7.4: Evalvacija spletne strani Halloween, its origins and customs

Kriteriji	**Vprašanja**	**Pozitivni ali negativen odgovor (pozitiven odgovor 1 točko in negativen 0 točk)**
Avtor ali vir	Je omenjen avtor dela ali bolj jasno identificiran?	Da
	Ali obstaja priporočilo za pisanje na to temo?	Da
	Ali je avtor včlanjen v kako organizacijo?	Da
	Ali stran predstavlja skupino, organizacijo, institucijo, združenje ali vladno telo?	Da
	Je povezava vrnjena nazaj na organizacijsko stran ali je povezana z avtorjevo stranjo (naslov, Telefonska številka, email naslov)?	Da
	Je jasno kdo je odgovoren za ustvarjeno ali vzdrževano stran?	Ne
Natančnost/skrbnost	Je stran celotno objavljena?	Da
	Ali lahko informacije preverjamo preko bibliografskih ali drugih virov?	Da
	Je natančno določeno kdo je odgovoren za skrbnost predstavitve strani?	Ne
	Ali so na strani predstavljeni statistični podatki, kot so grafi ali stolpci, ki bi bili nerelevantni?	Ne
Veljavnost	Ali obstaja stanje podatka, ko je bil dokument izvorno ustvarjen?	Da
	Je jasno razvidno kje je bila stran nazadnje osvežena, objavljena ali prenovljena?	Ne
	Ali obstajajo povezave na druge spletne strani?	Da
Nepristranskost	Ali stran ne vsebuje propagandnih sporočil?	Da
	Ali spletna stran ne prikazuje pristranskosti?	Da
	Ali stran ne vsebuje rabo vnetih ali provokativnih jezikovnih izrazov?	Da
Obseg delovanja	Ali je stran dokončno narejena in zaključena?	Da
Namen	Ali je namen strani pozitiven?	Da
	Je stran obsežna z viri?	Da

	Ali ima stran omenjen dostop do informacij?	Da
	Ali je poudarek na predstavitvi aktualen?	Da
Vsota pozitivnih oziroma negativnih odgovorov		17 pozitivnih odgovorov in 4 negativen odgovor

Tabela 7.5: Evalvacija spletne strani The White House.gov

Kriteriji	**Vprašanja**	**Pozitivni ali negativen odgovor (pozitiven odgovor 1 točko in negativen 0 točk)**
Avtor ali vir	Je omenjen avtor dela ali bolj jasno identificiran?	Da
	Ali obstaja priporočilo za pisanje na to temo?	Da
	Ali je avtor včlanjen v kako organizacijo?	Da
	Ali stran predstavlja skupino, organizacijo, institucijo, združenje ali vladno telo?	Da
	Je povezava vrnjena nazaj na organizacijsko stran ali je povezana z avtorjevo stranjo (naslov, Telefonska številka, email naslov)?	Da
	Je jasno kdo je odgovoren za ustvarjeno ali vzdrževano stran?	Da
Natančnost/skrbnost	Je stran celotno objavljena?	Da
	Ali lahko informacije preverjamo preko bibliografskih ali drugih virov?	Da
	Je natančno določeno kdo je odgovoren za skrbnost predstavitve strani?	Da
	Ali so na strani predstavljeni statistični podatki, kot so grafi ali stolpci, ki bi bili nerelevantni?	Da
Veljavnost	Ali obstaja stanje podatka, ko je bil dokument izvorno ustvarjen?	Da
	Je jasno razvidno kje je bila stran nazadnje osvežena, objavljena ali prenovljena?	Da
	Ali obstajajo povezave na druge spletne strani?	Da
Nepristranskost	Ali stran ne vsebuje propagandnih sporočil?	Da
	Ali spletna stran ne prikazuje pristranskosti?	Da
	Ali stran ne vsebuje rabo vnetih ali provokativnih jezikovnih izrazov?	Da
Obseg delovanja	Ali je stran dokončno narejena in zaključena?	Da
Namen	Ali je namen strani pozitiven?	Da
	Je stran obsežna z viri?	Da
	Ali ima stran omenjen dostop do informacij?	Da
	Ali je poudarek na predstavitvi aktualen?	Da

Vsota pozitivnih oziroma negativnih odgovorov		21 pozitivnih odgovorov in 0 negativnih odgovorov

Tabela 7.6: Povprečne evalvacije posameznih kriterijev in spletnih strani

Kriteriji	**Vprašanja**	**Število pozitvnih odgovorov (od 0 do 5)**
Avtor ali vir	Je omenjen avtor dela ali bolj jasno identificiran?	3
	Ali obstaja priporočilo za pisanje na to temo?	3
	Ali je avtor včlanjen v kako organizacijo?	3
	Ali stran predstavlja skupino, organizacijo, institucijo, združenje ali vladno telo?	3
	Je povezava vrnjena nazaj na organizacijsko stran ali je povezana z avtorjevo stranjo (naslov, Telefonska številka, email naslov)?	3
	Je jasno kdo je odgovoren za ustvarjeno ali vzdrževano stran?	2
Natančnost/skrbnost	Je stran celotno objavljena?	5
	Ali lahko informacije preverjamo preko bibliografskih ali drugih virov?	5
	Je natančno določeno kdo je odgovoren za skrbnost predstavitve strani?	2
	Ali so na strani predstavljeni statistični podatki, kot so grafi ali stolpci, ki bi bili nerelevantni?	1
Veljavnost	Ali obstaja stanje podatka, ko je bil dokument izvorno ustvarjen?	3
	Je jasno razvidno kje je bila stran nazadnje osvežena, objavljena ali prenovljena?	2
	Ali obstajajo povezave na druge spletne strani?	5
Nepristranskost	Ali stran ne vsebuje propagandnih sporočil?	3
	Ali spletna stran ne prikazuje pristranskosti?	2
	Ali stran ne vsebuje rabo vnetih ali provokativnih jezikovnih izrazov?	3
Obseg delovanja	Ali je stran dokončno narejena in zaključena?	4
Namen	Ali je namen strani pozitiven?	3
	Je stran obsežna z viri?	4
	Ali ima stran omenjen dostop do informacij?	5
	Ali je poudarek na predstavitvi aktualen?	3
Povprečna vrednost pozitivnih oziroma negativnih odgovorov		3,2

Tabela 7.7: Tabela vseh obravnavanih spletnih strani

Kriteriji	Vprašanja	**American Cancer Society**	**Martin Luther King, Jr**	**The White House.net**	**Halloween, its origins and customer**	**The White House.gov**
Avtor ali vir	Je omenjen avtor dela ali bolj jasno identificiran?	1	0	0	1	1
	Ali obstaja priporočilo za pisanje na to temo?	1	0	0	1	1
	Ali je avtor včlanjen v kako organizacijo?	1	0	0	1	1
	Ali stran predstavlja skupino, organizacijo, institucijo, združenje ali vladno telo?	1	0	0	1	1
	Je povezava vrnjena nazaj na organizacijsko stran ali je povezana z avtorjevo stranjo (naslov, Telefonska številka, email naslov)?	1	0	0	1	1
	Je jasno kdo je odgovoren za ustvarjeno ali vzdrževano stran?	1	0	0	0	1
Natančnost /skrbnost	Je stran celotno objavljena?	1	1	1	1	1
	Ali lahko informacije preverjamo preko bibliografskih ali drugih virov?	1	1	1	1	1
	Je natančno določeno kdo je odgovoren za skrbnost predstavitve strani?	1	0	0	0	1
	Ali so na strani predstavljeni statistični podatki, kot so grafi ali stolpci, ki bi bili nerelevantni?	0	0	0	0	1
Veljavnost	Ali obstaja stanje podatka, ko je bil dokument izvorno ustvarjen?	1	0	0	1	1
	Je jasno razvidno kje je bila stran nazadnje osvežena, objavljena ali prenovljena?	1	0	0	0	1
	Ali obstajajo povezave na druge spletne strani?	1	1	1	1	1
Ne/pristranskost	Ali stran ne vsebuje propagandnih sporočil?	1	0	0	1	1
	Ali spletna stran ne prikazuje pristranskosti?	1	0	0	1	1
	Ali stran ne vsebuje rabo vnetih ali provokativnih jezikovnih izrazov?	1	0	0	1	1
Obseg delovanja	Ali je stran dokončno narejena in zaključena?	1	1	0	1	1
Namen	Ali je namen strani pozitiven?	1	0	0	1	1
	Je stran obsežna z viri?	1	1	0	1	1
	Ali ima stran omenjen dostop do informacij?	1	1	1	1	1
	Ali je poudarek na predstavitvi aktualen?	1	0	0	1	1
Vsota pozitivnih oziroma negativnih odgovorov		20 pozitivnih odgovorov in 1 negativen odgovor	6 pozitivnih odgovorov in 15 negativen odgovor	3 pozitivnih odgovorov in 18 negativen odgovor	17 pozitivnih odgovorov in 4 negativen odgovor	21 pozitivnih odgovorov in 0 negativnih odgovorov