UNIVERZITET U SARAJEVU

FAKULTET POLITIČKIH NAUKA

ODSJEK POLITOLOGIJA

ELEMENTI POLITIČKOG UPRAVLJANJA U CYBER PROSTORU

-magistarski rad-

Kandidatkinja : Alma Draganović

Broj indeksa: 138/II-UPD/19

Mentor: Doc.prof. Sarina Bakić

Sarajevo,februar 2022.

ODSJEK POLITOLOGIJA

ELEMENTI POLITIČKOG UPRAVLJANJA U CYBER PROSTORU

-magistarski rad-

Kandidatkinja : Alma Draganović

Broj indeksa: 138/II-UPD/19

Mentor: Doc.prof. Sarina Bakić

Sarajevo, februar 2022.

ZAHVALNICA

Upućujem najiskrenije zahvale svojoj mentorici doc. dr. Sarina Bakić na strpljenju, pomoći i trudu pri izradi ovog završnog master rada.

Također, izražavam veliku zahvalnost svima koji su bili dostupni i spremni da pomognu u prikupljanju materijala potrebnog za razradu i pisanje istog. Velika hvala svim kolegama i prijateljima na riječima podrške u danima kad inspiracija utihne, također, hvala im na pruženim rukama prijateljstva; bez njih studij ne bi prošao tako zabavno.

Najveća zahvala ide mojim roditeljima i porodici na nesebičnoj podršci, razumijevanju i ljubavi koju su mi pružali tokom studija, te koji nikada nisu izgubili povjerenje u mene i moje sposobnosti.

SAŽETAK

Politike i norme informacione sigurnosti prisutne su već godinama u državnim sektorima zemalja i međunarodnim organizacijama, ali protekle godine i ekspanzija tehnologije i uopćeno Interneta, sa sobom su donijele napredak, ali i nesigurnost upravljanja i korištenja raznih informacija. Istraživanje se bavi uticajem novih tehnologija na politički sektor, njihovim razumijevanjima i adekvatnim sistemima zaštite.

Sve političke stranke danas koriste internet za prenošenje informacija o izbornom procesu, kandidatima i radnjama koje namjeravaju preduzet u slučaju pobjede na izborima. S druge strane, sva nezadovoljstva sa vlasti i vladajućim političarima, prvo se dešavaju online, a potom prelaze u prosteste i okupljanja građana na određenim mjestima i lokacijama. Način na koji političari i političke stranke upravljaju svojim aktivnostima, sprovode pravila i norme, te se štite od svih izazova koje online aktivnosti donose, bit će detaljno izložene u ovom radu.

KLJUČNE RIJEČI: Internet, politika, cyber prostor, novi mediji, demokratija, cyber kriminal i cyber sigurnost.

SADRŽAJ

1. UVOD

Riječ politika nastala je od grčke riječi polis, što znači grad ili država, a od nje je izvedena riječ politeia ili latinski politia što znači: unutrašnje uređenje i način života jedne ljudske zajednice ili opća stvar svih građana polisa. Ako želimo pobliže da shvatimo samo značenje riječi politika, reći ćemo da ona predstavlja sposobnost upravljanja nekom državom i u novom demokratskom[1] društvu se shvata i doživljava kao vještina vođenja, odnosno održavanja političke vlasti. Politika zasigurno nije mnogima od nas najbitnija stvar u životu ali definitivno jeste bitna karika u lancu održivosti, jer upravo od nje zavisi način i stil života modernog demokratskog društva.

Pojavom novih medija, politička komunikacija je poprimila sasvim novu dimenziju. Odnos između političkih stranaka i potencijalnih birača je dostigao najviši nivo dvosmjerne komunikacije, gdje su sada birači u prilici da lično postavljaju pitanja i istog trena dobiju odgvovore od simpatizera stranke koju podržavaju. U razvijenim zemljama svijeta Internet predstavlja sve češći kanal u političkoj komunikaciji. Gotovo da nema stranke ili kandidata koji ne koristi Internet u svojoj kampanji. Internet je povećao mogućnost prenošenja informacija većoj ciljanoj skupini za puno kraće vrijeme nego što se to radilo putem štampe, televizije, radija… Sve političke stranke danas koriste internet za prenošenje informacija o izbornom procesu, kandidatima i radnjama koje namjeravaju preduzet u slučaju pobjede na izborima. S druge strane, sva nezadovoljstva sa vlasti i vladajućim političarima, prvo se dešavaju online, a potom prelaze u prosteste i okupljanja građana na određenim mjestima i lokacijama.

[1] Pojam demokratija označava oblik vlasti u kojem sve odluke neke države donosi većina njenih građana, direktno ili indirektno kroz stranačke, odnosno državne izbore. Kad su ti uslovi ispunjeni, izabrana vlast se može smatrati demokratskom izabranom vlašću.

2. METODOLOŠKI DIO ISTRAŽIVANJA

2.1. Problem istraživanja

Svjedoci smo jednog novog vremena tehnoloških promjena koje podrazumijeva korištenje moderne tehnologije gdje direktni susret sa pojedincem ili grupom kao biračima, danas više nije ključna za obavljanje političkih aktivnosti. Uloga masovnih medija jača kroz godine, te dobijaju ulogu javnog foruma na kojem se političke stranke i kandidati utrkuju za pažnju i poverenje potencijalnih birača. Možemo reći da su mediji postali jedan vid platforme za prezentaciju političkih stranaka uopće. Modernizacija medijskog sistema, prije svega prostora u kom djeluju, utiče na strukturu, sudionike i procese političke komunikacije. Mediji dominiraju sistemom posredovanja i sve više postaju preduslov komunikacije, kako u društvu i organizacijama, tako i u raznim političkim strankama.

Trenutna situacija u svijetu sa pandemijom je prisilila mnoge političke stranke da razviju novi način komuniciranja međusobno, ali i sa javnosti u cyber prostoru. Taj način komunikacije, koji ima svoje dobre strane kao što su brža prezentacija postignutih i željenih ciljeva, dostupnost i praćenje podataka, ima i loše strane. Danas je mnogo teže političarima pratiti i uticati na samu političku stranku i aktivnosti kojima se bavi, upravo zbog virtuelnog svijeta u kojem smo se svi našli, gdje imam malo ili nikako direktnih kontakata. To područje unutrašnjeg vođenja stranke i donošenje političkih odluka u vremenu krize smatram još uvijek nedovoljno istraženim područjem, pa upravo sam odabir teme i pisanje o istoj će me približiti novim izazovima i načinima odlučivanja i rukovođenja.

2.2. Predmet istraživanja

Razvoj tehnologije i njena implementacija u naš svakodnevni život se dešava prevelikom brzinom, mijenjajući pritom naše rutine. Cyber prostor je virtuelna stvarnost, to je prostor uspostavljen uz pomoć i posredovanje kompjuterske tehnologije. Raspolaganje potrebnom i kvalitetnom količinom informacija predstavlja jedan od temeljnih elemenata uspješne političke strategije. Umrežene sjednice, stranački sastanci, cjelokupne predizborne kampanje, izborni procesi i slično, još su uvijek relativno neistražena polja djelovanja današnje političke scene, te ih je primamljivo detaljnije analizirati i istražiti.

2.3. Teorijska osnova istraživanja

Cyber prostor je bitan faktor svakodnevnih aktivnosti i ostvarenih rezultata sa političkog aspekta u savremenom društvu. On uključuje prije svega, sam Internet, gdje spadaju web stranice, slobodne enciklopedije, VoIP, internet telefonija, te svi ostali oblici komunikacije potrebni za nesmetano obavljanje svakodnevnih aktivnosti.

Računarstvo u oblacima (engl. cloud computing) danas je gotovo nezaobilazno sredstvo pohranjivanja podataka, te samom primjenom svih drugih digitalnih tehnologija, koristimo također i računarstvo u oblacima.

Mobilne tehnologije (engl. mobile technologies) omogućile su da osoba koja se nalazi bilo gdje, ima računar u ruci, te može pratiti i obavljati potrebne aktivnosti. Jedna od tih aktivnosti jeste i pristup e-mailovima, koji ujedno predstavlja začetke cyber prostora. Mađutim, upravo ta fleksibilnost i dostupnost dovode do određenih organizacijskih i emocionalnih napora. Elektronskim komuniciranjem teže je razviti i očuvati zdravu kulturu unutar neke

organizacije, u ovom slučaju, konkretno neke političke stranke, dobre odnose njenih članova, te atmosferu povjerenja i zalaganja za političke ciljeve.

2.4. Ciljevi istraživanja

2.4.1. Naučni cilj istraživanja

Naučni cilj ovog istraživanja jeste opisati cyber prostor kao relativno novi fenomen, te cyber kulturu kao bitan faktor tog prostora. Predstaviti elemente političkih upravljanja u takvom prostoru, te vođenje izborne kampanje u uslovima pandemije. Pokušat ćemo opisati način na koji cyber prostor utiče na političke promjene kao i radnu atmosferu unutar političke stranke.

2.4.2. Društveni cilj istraživanja

Društveni cilj istraživanja bi bio upoznavanje relativno novog načina poslovanja koje se temelji na on line ili virtuelnom prostoru, gdje su direktni kontakti rijetki ili ih nikako nema, vođenje organizacije u jednom takvom „neopipljivom“ domenu, gdje su lične kontakte zamijenile razne on line platforme kao što je Skype, Teams, Voip telefonija i slično. Kako smatramo da će ovakav trend poslovanja i nakon pandemije ostati većim dijelom zastupljen širom svijeta, izazov je i prilika približiti se ovoj vrsti literature, te steći nova znanja.

2.5. Metode istraživanja

Za potrebe ovoga istraživanja koristit ćemo opće naučne metode. Teorijski dio je prikupljen iz sekundarnih izvora kao što su razni naučni članci i knjige. Kao metodu ispitivanja

koristit ćemo anketu, koja ujedno predstavlja i najčešće korišteni postupaka za ispitivanje ciljane grupe. Anketom nazivamo skup postupaka pomoću kojih se prikupljaju izjave ispitanika s ciljem da se dođe do određenih podataka o njihovom ponašanju ili o njihovim stavovima, mišljenjima, interesima i slično, a radi statistike, ispitivanja tržišta ili kao temeljno polazište za potrebe nekog drugog istraživanja.

Istraživanje je provedeno online putem Google obrasca (ankete) koju su ispunjavali kontakti putem društvene mreže Facebook i Instagram. Anketna pitanja sastojala od osam kratkih pitanja sa ponuđenim odgovorima. Istraživanje je provedeno na uzorku od 100 ispitanika.

Anketa je bila kratka i ispitanici su je popunili unutar jedne minute. Na taj se način, vjerujemo, zadržala izvrsna motivacija i iskrenost kod ispitanika.

2.6. Hipoteze

Generalna hipoteza: Cyber prostor pruža veliki broj prednosti upravljanja političkim pitanjima, adekvatne kulture unutar političke stranke, ali donosi i određeni broj nedostataka i prijetnji. Internet predstavlja moderni kanal komunikacije kojim je moguće unaprijediti već postignute rezultate, ali ujedno i pruža mogućnost manjim strankama da steknu ista ili približna promotivna dejstva. Putem interneta veliki auditorij je u prilici da vidi promotivne poruke političkih stranaka, neovisno o broju njenih kandidata, kao i finansijskoj potpori koja stoji iza iste.

Pomoćna hipoteza I: Upravljanje u cyber prostoru zahtijeva nove kompetencije i dodatne vještine.

Pomoćna hipoteza II: Cyber prostor doprinosi učinkovitijem oglašavanju i efikasnijim rezultatatima, kako na političkoj sceni generalno, tako i na izborima, samo ako politički predstavnici i kandidati iskoriste njegov prostor kao mjesto za dvosmjernu komunikaciju.

2.7. Struktura rada

Rad se sastoji od devet poglavlja. U prvom se govori o uvodnim razmatranjima, a od drugog do devetog poglavlja izlaže se teoretski dio usko vezan za temu rada. U zadnjem desetom poglavlju je analizirana istraživačka komponenta rada, te date preporuke na problem istraživanja, i na kraju zaključna razmatranja i osvrt na problematiku istog.

3. NOVI MEDIJI I POLITIČKO KOMUNICIRANJE

3.1. Internet

Internet je globalna paketna podatkovna mreža koja zajedno povezuje računare i računarske mreže korištenjem istoimenog protokola (internet protokol=IP). Godine 1969. Internet kao takvu mrežu pokreče Agencija za napredna istraživanja Ministarstva odbrane SAD-a (Department of Defense's Advanced Research Projects Agency), ARPANET, na kalifornijskom sveučilištu u Los Angelesu. Njegov prvobitni cilj je bio omogućiti naučnicima sa različitih univerziteta da razmjenjuju mišljenja, rezultate istraživanja i slično, a koji su se nalazili na različitim lokacijama.

Internet je omogućio potpuno nove oblike društvene aktivnosti i interakcije, zahvaljujući svojim osnovnim karakteristikama kao što je pristupačnost, rasprostranjena primjena i transparentnost. Razne društvene mreže poput Facebooka, Twittea, Instagrama i druge, su stvorile novi oblik socijalizacije. Velika količina nformacija koja se na njima nalazi omogućava svim korisnicima da iste dijele, promovišu, te putem istih spoznaju i razmjenjuju zajedničke interese sa drugim ljudima. Također, Internet i društvene mreže omogućavaju korisnicima da se povežu i tako održavaju kontakte koji prije pojave Interneta nisu bili mogući osim ukoliko nemamodirektni kontakt sa osobom ili osobama. Generacije rođene u 21. vijeku su uveliko

postale ovisne o dostupnosti Interneta, te svim mogućnostima koje on pruža. Možemo reći da danas nema osobe koja nema profil na nekoj društvenoj mreži.

Slika 1. *Novi mediji*

Izvor: *https://olc.sfu.ca/*

Internet pored svojih socijalnih karakteristika, znatno olakšava i unapređuje poslovanje. Nekadašnje interakcije „licem u lice“ zamijenjene su interakcijom preko Interneta, te na taj način štede na vremenu i novcu. Međutim, bez obzira na prednosti koji donosi, neki smatraju Internet nužnim zlom, te ne dijele mišljenje da on olakšava život. Razlog tome može biti upravo ta moderna socijalizacija, gdje su svi uvezani, ali bez direktnih kontakata. Nekadašnja druženja u kafićima, koncertima, u prirodi i slično, zamijenila su virtuelna druženja, što većina starijih generacija ne smatra ispravnim.

Već je ranih 1990-ih bilo jasno da budućnost leži u Internetu, ali teško da je ko znao koliko će brzo Internet postati naša svakodnevnica bez koje više ne možemo zamisliti život. Digitalna revolucija i Internet su doveli do integracije različitih medijskih oblika i ubrzanog razvoja globalnog tržišta, a mediji kakve smo nekada znali morali su se brzo prilagoditi kako bi zadovoljili zahtjeve tržišta i ostali relevantni svojim korisnicima. Pored toga što su velikim dijelom zamijenili tradicionalni način ljudskog komuniciranja, novi mediji su također promijenili način na koji vidimo javnost, ali i političku scenu i komunikaciju koja se na njoj odvija. Labaš (2009: 14-18) kao karakteristike novih medija navodi sljedeće:

(a) DIGITALNOST: Podaci su obrađeni digitalnom, odnosno brojčanom obliku. Informacija se pretvara u binarni kod, što znači brže i lakše širenje informacija. Digitalna konvergencija ključi je proces koji je omogućio razvoj novih medija.

(b) INTERAKTIVNOST: jeste mjera moguće sposobnosti nekoga medija da korisniku dopusti uticaj na sadržaj i/ili formu prenesene komunikacije. Postoje tri nivoa interaktivnosti:

1. ostvarivanje mogućosti selekcije (jednosmjerna interaktivnost, npr.: teletekst),
2. medij predviđa povratni kanal kako bi primio informacije od korisnika (npr.: funkcioniranje World Wide Weba) i
3. sam korisnik proizvodi informacije koje sistem stavlja u opticaj, uz preradu sadržaja koju stvaraju drugi sudionici. Na ovom nivou se izražava ideja društvene interakcije.

(c) MULTIMEDIJALNOST: Sadržaj je izražen različitim kanalima, kao što su tekst, zvuk, slika, grafika sa snažnom integracijom različitih kodova. Fidler (2004: 44–45) multimedijalnost objašnjava kao sistem pomiješanih medija koji prenose informacije kroz različite mješavine pokretnih videa, animacija i zvuka, ali i nepokretnih slika i pisanih riječi.

(d) KIBERNETIČKI PROSTOR (CYBERSPACE): Telematske mreže razvile su se u komunikacijskom i društvenom smislu. Postale su strukture, sredstva komunikacije između korisnika, a funkcije koje ostvaruju pripisuju se masovnim medijima.

(e) HIPERTEKSTUALNOST (HIPERMEDIJALOST): Skup informacija povezan je nelinearno, a omogućuje personalizirano korištenje (ibid). Tekstu je na taj način dodana dimenzija dubine, a sve je češće i korištenje hipermedija.

Tehnološki napredak i razvoj medija doveo je do toga da smo svakodnevno okruženi s nekoliko ekrana, odnosno medijskih platforminpreko kojih koristimo medijske sadržaje, informišemo se i komuniciramo. Televizija više nije jedini ili najzastupljeniji elektronski medij, već se masovno koriste i druge medijske platforme poput računara, tableta, pametnih telefona. Kad govorimo o podjeli medija govorimo o tri osnovne podjele:

- štampani mediji,
- elektronski mediji,
- novi mediji.

U štampane medije ubrajamo: knjige, novine, magazine i časopise. U elektronske medije radio i televiziju, a noviji medij je Internet o kojem smo upravo govorili. Medije razlikujemo prema vrsti ili sektoru (knjiga, štampa, novine, časopisi), prema geografskom nivou i pripadnosti (lokalni, nacionalni, međunarodni), prema obliku vlasništva ili upravljačke kontrole (privatni, javni, državni) i prema bliskosti javnog i političkog mišljenja (matični i alternativni mediji). Za potrebe istraživanja, medije možemo podijeliti u dvije velike skupine:

1. Tradicionalni mediji
2. Digitalni mediji

U tradicionalne medije ubrajamo novine, časopise, radio i televiziju, dok su digitalni mediji svi mediji koji svoj medijski sadržaj objavljuju ili nude putem Interneta ili putem digitalnih mreža i uređaja. Sadrže slike, tekstove, zvučne i video zapise, grafiku i animaciju i druge digitalne oblike. Može im se pristupiti putem računara, mobilnih telefona, tableta, televizora, igraćih konzola, digitalnih kućnih aparata i slično.

Mediji poput televizije, radija i dnevne štampe su danas postali nezamislivi bez svoje digitalne verzije i prisutnosti u obliku Web stranica, mobilnih aplikacija, foto galerija, zvučnih zapisa, filmova i video klipova, emitiranja programa u realnom vremenu (live) ili stranica na društvenim mrežama. Mediji i medijska kultura utiču na svakodnevni život oblikujući pojedinca,

njegov karakter, norme ponašanja i stil života. Na taj način mediji određuju definiciju ljepote, uspješnosti i moći.

3.2. Politika

Riječ politika dolazi od grčke riječi „polis“ što znači grad ili država. Danas politika predstavlja skup znanja i vještina koja se primjenjuju u različitim situacijama među ljudima radi ostvarivanja interesa. Politiku možemo definisati kao sposobnost upravljanja političkom zajednicom i državom općenito, te se odnosi na upravljanja državnim institucijama pomoću kojih ljudi ostvaruju svoje interese. Svaki pojedinac politiku doživljava individualno i prema njoj se odnose na različite načine. Politika se može posmatrati kao politički proces, odnosno nadmetanje, kao što su izbori. Također, može se posmatrati kao institucija gdje se odvijaju politički procesi i donose odluke koje imaju uticaj na sve sfere ljudskog života. Političke stranke imaju karakter organizacija koje ispunjavaju bitne funkcije u demokratskom procesu upravljanja. Miroslavljević (2010:66) kao osnovne funkcije političke stranke navodi:

1. Učešće na izborima gdje je osnovni cilj i pobjeda na istim;
2. Zastupanje društvenih interesa;
3. Pružanje programskih alternativa;
4. Izbor i obuku političkih vođa koji će upravljati državom.

Od političkih stranaka države zahtijevaju da ispune zakonske obaveze kao što su registracija i pravne obaveze, a to podrazumijeva potreban broj registrovanih članova, predsjednika stranke i pisani statut. Nije rijetkost da se u nekim slučajevima političke stranke udruže radi zajedničkih ciljeva, i takve stranke se nazivaju konzorcij.

3.3. Komunikacija

Komunikacija se dugi niz godina odvijala putem televizije, radija, štampe, časopisa, plakata, letaka, ličnih kontakata i slično. Sredstvo komunikacije novog doba jeste svakako Internet, koji je svakako postao i sredstvo političke komunikacije. Tokom razvoja Interneta i rasta broja korisnika, oglašavanja i promocije se u najvećoj mjeri dešavaju upravo putem ovog medija. Danas gotovo da i ne postoji politička stranka ili kandidat koji ne koristi Internet i društvene mreže u svojoj kampanji. Pet načina prezentovanja i oglašavanja se danas koristi u političkoj komunikaciji, a to su:

1. elektronski mediji (radio i televizija),
2. štampani mediji (novine i časopisi),
3. izložbeni mediji (billboardi i plakati),
4. lični kontakti, i
5. Internet i društvene mreže.

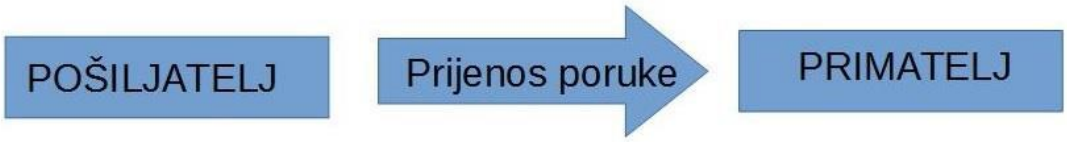
Ovi komunikacijski kanali se dijele u tri skupine s obzirom pružaoca i primatelja informacija. To su:

1. pasivni,
2. dinamički i
3. interakcijski

Pasivni komunikacijski kanali su izložbeni mediji, odnosno plakati, billboardi, itd. *Dinamički* kanali su televizija, radio, štampa i web portali. *Interakcijski* komunikacijski kanali predstavljaju ličnu komunikaciju, dogovorena masovna okupljanja i nove medijske tehnologije gdje su okupljanja online, bez ličnog kontakta, te u takve medije možemo uvrstiti razne forume, kao i društvene mreže.

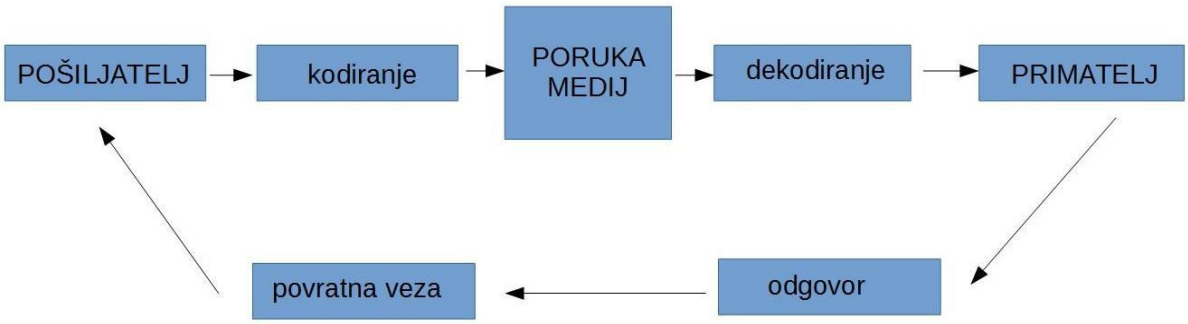
Demokratija je definisana određenim principima gdje primarni princip polazi od toga da su svi ljudi jednaki i da imaju određena prava kao pojedinac i kao dio društva. Demokratija je nastala onog momenta kada je svim građanima omogućeno da aktivno učestvuju u životu zajednice, da imaju osnovna ljudska prava kao što su sloboda govora i izražavanja, kao i glasanje

na političkim izborima. Drugi princip demokratije jeste da je vlada sastavljena od ljudi i da postoji da bi služila narodu. Vlada je odgovorna za zaštitu prava građana, a zauzvrat oni daju vladi privremeno ovlašćenje da donosi odluke u njihovo ime. Demokratskoj vladi dato je ovlašćenje da donosi odluke za vrijeme izbornog perioda ili mandata, a koju je izabralo građanstvo. Vlast demokratske vlade je ograničena zakonima koji štite društvene i političke slobode, koje su definisane Ustavom.



Slika 2. *Jednostavan komunikacijski process*

Izvor: *C. L. Bovee, J. V. Thill (2012): Savremena poslovna komunikacija.*



Slika 3: *Model komuniciranja*

Izvor: *Cutlip, S. M.,Center, A. H. & Broom, G. M. (2010): Učinkoviti odnosi s javnošću*

Prema Kotleru (2001), ove elemente možemo definisati na sljedeći način:

- Pošiljalac: strana koja šalje poruku;

- Kodiranje: postupak prenošenja zamišljenog u simbole;
- Poruka: niz simbola koje emituje pošiljalac;
- Medij: kanali prenošenja poruka od pošiljaoca do primaoca;
- Dekodiranje: postupak kojim primalac objašnjava značenje simbola koje je emitovao pošiljalac;
- Primalac: strana koja prima poruku;
- Odgovor: reakcija primaoca nakon primanja poruke;
- Povratna veza (feedback) dio odgovora primaoca koji isti povratno saopštava pošiljaocu;
- Smetnja: neplanirani zastoj ili pogrešno penesena poruka tokom procesa komuniciranja.

3.4. Politička komunikacija

Tokom ovog istraživanja i traženja članaka putem Interneta, te sprovođenjem ankete koja je bila sastavni dio ovog rada, ustanovili smo određena podudaranja kada su u pitanju stavovi o tome da se Internet u razvijenim zemljama sve češće koristi u političkoj komunikaciji. Gotovo da nema stranke ili kandidata koji ne koristi internet u svojoj kampanji.

Proces razmjene političkih sadržaja u vrijeme izbora, koji se odvija putem komunikacijskih kanala (medija), a u svrhu postizanja određenih efekata, predstavlja političko komuniciranje. Prema Blumer i Kavanagh (1999:209-213) poznata su tri perioda u političkoj komunikaciji. Prvi period jeste period prije početka televizije, kada su kanali komunikacije bili direktni i primarni. U drugom periodu fokus se preusmjerio na prenošenje poruka putem masovnih medija i povećao je potražnju za profesionalcima u komunikaciji, koji su bili vješti u iskorištavanju ovih kanala. U trećem periodu politička komunikacija postaje još izraženija, a samim tim i profesionalnija. Političke stranke i kandidati pokušavaju slati poruke kroz veliki broj kanala i na veće ciljane grupe.

3.4.1. Interna komunikacija

Bez obzira na veličinu političke stranke i broju njenih članova, interna komunikacija je od velikog značaja. Za ovu vrstu komunikacije potrebno je osigurati okruženje u kojem se može slobodno izražavati i stvarati ideje. Snažne i uspješne političke stranke i njihovi lideri su svjesni važnosti ovog vida komunikacije, jer je odnos s ljudima postao sastavni dio cjelokupnog razvoja i prosperiteta. Samim time predstavlja važnu ulogu u procesu upravljanja strankom i njenim članovima, tokom kampanje, u vrijeme izbora, i na kraju, ukoliko su svi parametri uspješno realizovani, tokom izbornog perioda, odnosno vlasti. Interna komunikacija jeste komunikacija koja svakako postoji u političkom tijelu, ali je nedostupna za javnost.

Glavni problemi interne komunicije se odnose na nedovoljan, odnosno veliki broj podataka u političkoj stranci. Nedostatkom potrebnih informacija koje su bitne za uspješno obavljanje zadataka, te uspješno vođenje kampanje, doći će do negativne atmosfere u cijeloj stranci, kao i ličnim nezadovoljstvom samih kandidata. U situacijama kada je dostupno previše podataka može doći do zbunjenosti i pada motivacije, te se tako cijela kampanja dovodi u nezavidan položaj. Treba postići optimalan broj potrebnih informacija jer obje ekstremne situacije rezultiraju smanjenom produktivnosti u političkoj stranci. Da bi jedna politička stranka bila uspješna, njeni članovi moraju:

- jasno definisane odgovornosti unutar stranke;
- razumjeti ciljeve stranke;
- uspostaviti dobre kanale komunikacije unutar stranke.

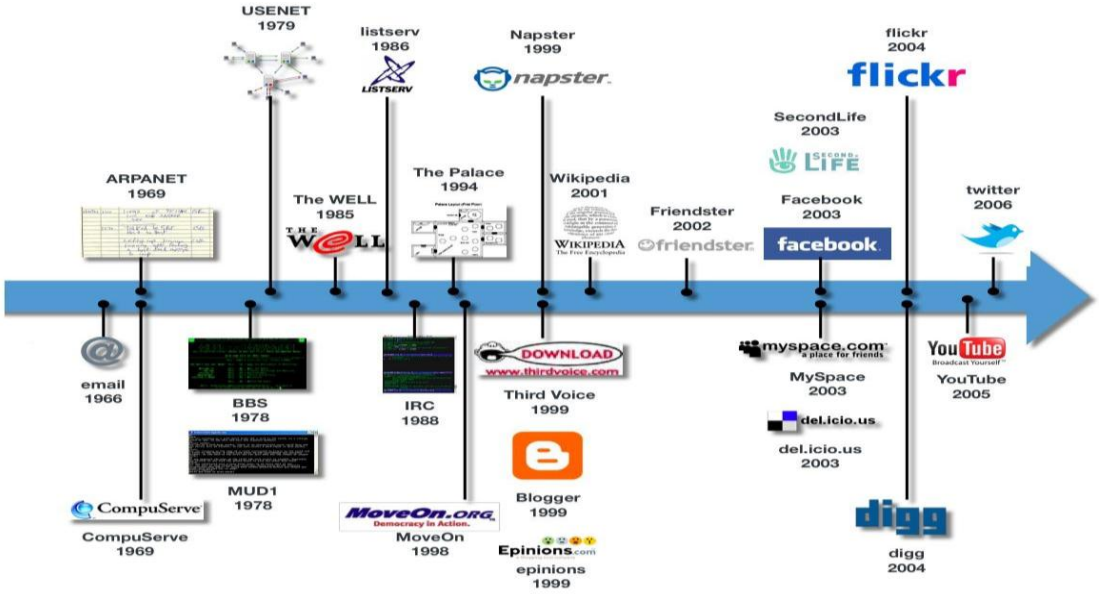
3.4.2. Spoljna komunikacija

Svaka politička stranka koja teži ka što većem broju glasova na izborima i ponovo ukazanom povjerenju od strane građana, mora imati dobre kanale komunikacije, kako od

lokalnog nivoa ka državnom nivou, tako i u obrnutom smjeru. Pouzdane i redovne informacije su ključ uspjeha na političkoj sceni.

Oglašavanje usmjereno na društvene mreže i oglasne mogućnosti koje one pružaju, predstavlja zasebnu tehniku internetskog oglašavanja. Razvojem društvenim mreža te rastom broja korisnika, jačao je i interes poslovnih subjekata za primjenu društvenih mreža u marketinškim aktivnostima. U početku su bili usmjereni na veće i poznatije društvene mreže kao primjerice Facebook ili Linkedin. No kako se svakim danom razvijaju nove društvene mreže, političari i stranke imaju na izbor mnogobrojne društvene mreže koje nude veliki broj novih mogućnosti oglašavanja, promocije željenoj ciljanoj skupini. Danas je normalno da svi subjekti političke scene koriste društvene mreže te na taj način privlače nove članove i birače.

Ekspanzija društvenih mreža počinje već 1995. godine sa čuvenim sajtom Classmates.com, da bi se kasnije pojavio My space koji je dugo vremena bio najpopularniji sajt tog tipa u svijetu. Pojavom My space 2003. godine društvene mreže dobijaju svoj standardizovani oblik. Taj pojam se nekako zaokružio i počeli su širom sveta da niču slični sajtovi, da bismo 2006. godine dobili i Facebook. Facebook je prvobitno bio namijenjen studentima kako bi mogli međusobno komunicirati i razmjenjivati informacije. Kasnije su se mnogi drugi univerziteti i škole, kao i velike kompanije širom svijeta, priključile ovoj društvenoj mreži. Godine 2008. postaje najpopularnija web stranica za društveno umrežavanje. Facebook svojim korisnicima omogućava da postavljaju slike, videozapise, komentare na svojim i tuđim profilima, razmjenjuju poruke, lajkove itd. Administratori ove društvene mreže konstantno dodaju nove funkcionalnosti na postojeću platformu. Kada je riječ o Facebooku kao oglašivačkoj platformi, odmah se ističe kako je izuzetno razvijena te kako prednjači u odnosu na ostale. Ono što se prvenstveno izdvaja kao prednost ove društvene mreže jeste što je moguće oglašavati se sa jako malo novca. Upravo tu karakteristiku iskorištavaju i političke stranke prilikom kreiranja stranica stranaka i kandidata, gdje su mogu usmjeriti na određenu ciljanu skupinu.



Slika 4. *Razvoj društvenih mreža*

Izvor: *https://www.pinterest.com/pin/535506830419407 26/*

Oglašavanjem putem društvenih mreža nastoji se stvarati kreativan sadržaj kako bi se njime privlačilo pažnju čitatelja odnosno korisnika tih mreža, te ih motiviralo da sadržaj dijele dalje. Time se sadržaj širi putem društvenih mreža do mnogobrojnih korisnika.

3.5. Politički marketing

Sintagma „politički marketing“ prvi put se spominje 1956. godine u knjizi Professional Public Relations and Political Power, američkog autora Sean Q Kellya. Prema široj definiciji, politički marketing je pronalaženje, održavanje i produbljenje dobrih dugoročnih odnosa s biračima radi postizanja dobrobiti i za društvo i za političku stranku, tako da se ciljevi pojedinog političkog kandidata i stranaka uključenih u proces podudaraju. To se postiže obostranom

razmjenom i ispunjenjem datih obećanja. [2] Politički marketing jeste sveobuhvatno područje koje u sebi sadrži znanja iz ekonomije, socijalne psihologije, komunikologije i politologije. U razvijenim zemljama svijeta, politički marketing je poznata i uveliko primjenjiva disciplina, dok u zemljama u tranziciji nema dovoljno razvijene političke prakse, a s tim niti razvijenog političkog marketinga.

Politički marketing predstavlja mnogo kompleksniji pojam u praksi. Bitnu kariku u političkom uspjehu predstavlja izbor adekvatnih tehnika i aktivnosti kojim se nastoji pridobiti što veći broj birača i kandidata. Šta god bila pozadina političkog marketinga i političke motivacije za određenim akcijama, iza kojih su se često nazirali ekonomski i drugi interesi, javnosti je to trebalo objasniti, uvjeriti je i pridobiti na njima razumljiv i prihvatljiv način.

Kada govorimo o stranačkoj promociji, važno je napomenuti da se promocija sastoji od promotivnog miksa, odnosno od više različitih aktivnosti kojima je cilj prenijeti informacije sadašnjim i budućim biračima. Pod elementima marketinškog miksa podrazumijevamo svaki oblik komuniciranja stranke sa biračima i javnošću. Osnovna namjena promocije je informisati, uvjeriti i uticati na odluke javnosti po pitanju odabira stranke ili samo jednog od kandidata unutar te stranke. Kandidat koji želi da bude izabran i preuzme političku funkciju mora da posjeduje vrline i kvalitete koje ga čine sposobnim za ovaj zadatak. Cilj političkog marketinga jeste da istakne sposobnosti i stručnost određenog kandidata i da ih prezentuje građanima. Dobro isplanirane političke aktivnosti, uspješna i adekvatna organizacija mogu znatno da olakšaju izbornu pobjedu čak i onim strankama koje ne raspolažu sa velikim finansijskim sredstvima.

Politički marketing obuhvata veći broj oblasti kao što je ekonomija, psihologija i sociologija, pa i same političke nauke. Razvijene zemlje već uveliko koriste i primjenjuju politički marketing. Upravo online glasanje prilikom izbora, predstavlja snažan alat političkog marketinga. Izbor odgovarajućih tehnika i aktivnosti kojim se nastoji pridobiti što veći broj birača predstavlja bitan faktor političkog uspjeha. Svako obraćanje javnosti mora biti osigurano

[2] Baines, P.R., Egan, J.(2001): Marketing and political campaigning: mutually exclusive or exclusively mutual?, Qualitative Market Research: An International Journal, Vol. 4, No. 1, str. 25-33

predstavljanjem što jasnije određenih akcija, treba biti uvjerljivo i na kraju rezultirati pridobivanjem novih članova i glasača.

Stranačka promocija se sastoji od od više različitih aktivnosti koje imaju za cilj prenijeti informacije javnosti. Osnovna namjena promocije je informisati, uvjeriti i uticati na odluke javnosti po pitanju odabira stranke ili samo jednog od kandidata unutar te stranke. Kandidat koji želi da bude izabran i preuzme određenu političku funkciju mora da posjeduje kvalitete koje ga čine adekvatnim za taj zadatak.

Dobro isplanirane političke aktivnosti, uspješna i adekvatna organizacija, mogu da olakšaju izbornu pobjedu, čak i onim strankama koje nemaju veliku finansijsku moć. U Bosni i Hercegovini se politička scena zasniva uglavnom na ekonomskom marketingu, gdje stranke i kandidati gledaju prvenstveno svoje interese. U političkim kampanjama nema izlaganja i prezentacije ciljeva i djelovanja stranke i onoga što je u interesu građana, već stranke obećavaju prosperitet na generalnom državnom nivou, koji se možemo reći, ponavlja od izbora do izbora.

Podjela države po entitetskoj osnovi i medijska podijeljenost su bitno odredili, a i danas određuju način organizacije i provedbu izbornih kampanja ali i samog političkog marketinga u Bosni i Hercegovini. Istaknuto je da je period nastanka političkog marketinga u Bosne i Hercegovine istovremeno bio i period različitih vrsta sukoba gdje su posljedice bile katastrofalne, a naročito su se odnosile na odsustvo slobode, tolerancije i ljudskih prava. Taj period je vezan za nastanak političkog marketinga ali i za nastanak manipulacije građanima. Cilj političkog marketinga je nastojati obe strane uključiti u određenu političku opciju, ideju ili aktivnost. Prvo se analiziraju potrebe birača, pa se tek tada na osnovu dibivenih rezultata kreira zadatak i cilj djelovanja. Postoji jedanaest instrumenata političkog komuniciranja u demokratskom društvu (Grbeša, Lalić, 2003, str. 37-38). To su:

1. Agenda setting
2. Istraživanje javnog mišljenja
3. Uokviravanje (Framing)

4. Konstruiranje spektakla
5. Pakiranje politike
6. Kreiranje i upotreba imidža
7. Spin-doktori
8. Odnosi s javnošću
9. Stvaranje pseudodogađaja
10. Državna kontrola nad medijima
11. Politička retorika

Podjela koju su napravili Grbeša i Lalić jeste najsličnija instrumentima koji se mogu koristiti u političkom uređenju kakav je u Bosni i Hercegovini.

Agenda setting pretpostavlja da mediji, javnost, politički akteri i institucije pokušavaju uticati na ključne teme političkog i društvenog života. Njih mogu nametnuti političari ili javnost putem dominantnog medija. Pretpostavlja se da prednost i primarnost kojim se pojedinim temama pristupa u masovnim medijima utiču na njihovo značenje u javnosti. Medijima se u tom smislu ne pripisuje sposobnost da utiču na to šta će ljudi misliti, ali u velikoj mjeri određuju o čemu će ljudi misliti.

Istraživanje javnog mišljenja danas ima važnu ulogu i uticaj u demokratski oblikovanim društvima. Za političke kandidate istraživanje javnog mišljenja je važno u pogledu smjernica kako najbolje voditi kampanju.

Uokviravanje/Framing u ovom smislu može značiti isticanje jedne i prikrivanje druge strane stvarnosti. Framing se ne odnosi samo na odabir vijesti, jer i slušalac tih vijesti koristi svoje postojeće okvire. Važno je ukazati na razliku između kriterija odabira vijesti i stvaranja okvira kojima se teme i događaji modificiraju i predstavljaju.

Konstruisanje spektakla navodi javnost da podržavaju dobre ideje i političke stranke koji su predstavljeni kao takvi, a da se suprotstavljaju neistomišljenicima.

Pakiranje politike je način da se politički događaji banaliziraju, a lična predstavljanja uveličavaju.

Imidž u političkoj komunikaciji je bitan i za kandidata i za stranku. Zadatak političkog marketinga je oblikovati i promovisati pozitivne programe ibaktivnosti. Dobro izgrađen imidž predstavlja snažno oružje političke komunikacije.

Spin-doktori su osobe zadužene za oblikovanje javnog mišljenja o različitim temama, osobama ili događajima vještim manipuliranjem masovnim medijima.

Odnosi s javnošću su postali nezamjenjiv instrument političkog komuniciranja, a kolika je njihova važnost govori činjenica da danas gotovo sve vlade i državne ustanove imaju informacijski menadžment. Odnosi s javnošću su planirana i svjesna aktivnost kojom se uspostavlja i održava međusobno razumijevanje između političke scene i njene javnosti.

Pseudodogađaji predstavljaju kreiranje događaja samo zato da bi dospjeli do masovnih medija i nisu spontani već se dešavaju planirano. Pseudodogađaji se najčešće kreiraju u vrijeme predizbornih kampanja, i na taj način se političke stranke i kandidati nastoje što češće pojavljivati u javnosti.

Državna kontrola nad medijima se najčešće manifestuje u manje razvijenim zemljama, pomoću tehničke nerazvijenosti i nametanjem regulacija vlade. Oblici državne kontrole nad medijima su najčešće cenzura, tajnost i regulacija.

Politička retorika je temeljni instrument političkog komuniciranja jer upravo o jeziku koji se koristi u politici ovisi pakiranje politike, postavljanje agende, kreiranje imidža ali i drugih instrumenata savremenog političkog komuniciranja.

U novije vrijeme oni se nadopunjuju sa dva instrumenta, a to su: političko oglašavanje i političke kampanje. Političko oglašavanje se odnosi na zakup i korištenje oglasnog prostora, plaćeno po komercijalnim cijenama, kako bi se političke poruke prenijele javnosti. Najčešće korišteni mediji za ovu svrhu su televizija, dnevna štampa, društveni i mediji. Političke kampanje su organizovane i unaprijed isplanirane akcije s ciljem postizanja određenih političkih ciljeva.

3.5.1. Odnosi s javnošću

Unutar političkog marketinga pojavljuje se posebna funkcija, a to je odnosi s javnošću. Njena zadaća jeste održavanje dvosmjerne komunikacije, razumijevanje, saradnja sa javnosti i redovno izvještavanje o aktuelnostima stranke. Sredstva odnosa s javnošću su:

- odnosi s medijima,
- publicitet,
- korporativno komuniciranje i
- lobiranje.

Odnosi s medijima predstavljaju praćenje objava u medijima te njihova analiza kojom se želi vidjeti utjecaj tih objava na javnost. Publicitet predstavlja slanje poruke u medije tako da se informacije dobijaju iz vanjskog izvora. Korporativnim komuniciranjem se želi povećati reputacija stranke ili kandidata, te se isto takvo komuniciranje može primijeniti i u slučaju izborne kampanje. Lobiranje služi kako bi se utjecalo na odluku o glasanju, što u korist stranke ili kandidata, tako i u korist javnosti. U političkim odnosima s javnošću je vrlo teško stvoriti naklonost javnosti zato što su građani često nepovjerljivi. Upravljanjem medijima se želi stvoriti stalna pozitivna prisutnost političkog kandidata u različitim medijima. U ovom slučaju se koriste već spomenuti spin doktori koji zapravo upravljaju vijestima i načinom kako se kandidat prikazuje u medijima na način da se ciljanoj javnosti nameće željena percepcija. Ugled, odnosno imidž političkog kandidata predstavlja i cjelokupan ugled političke stranka, osim ukoliko je kandidat neovisan. Posljednja aktivnost koja se provodi kod odnosa s javnošću jest interna komunikacija. Internom komunikacijom u političkoj stranci, kao i internom komunikacijom u samom timu koji radi na političkoj kampanji kandidata se povećava pozitivna slika kandidata jer su i sami članovi neke stranke te zaposlenici kampanje ciljana javnost. Odnosi s javnošću prilikom izbornih kampanja se sastoje od nekoliko koraka pomoću kojih se provode aktivnosti, a to su:

- Prvi korak jeste izrada strategije za izbornu kampanju, a osoba koja kreira istu mora biti stručnjak za odnose s javnošću.

- Kreiranje komunikacijskog PR tima gdje se skupljaju stručnjaci koji će raditi na određenim segmentima strategije komuniciranja. Vrlo je važno da se kod izborne kampanje pokrije svaki dio strategije.
- Izrada plana medijskih aktivnosti kojima se utvrđuje kada, kako i gdje će izborni kandidat, ali i ostali članovi stranke, pojavljivati.
- Sređivanje promotivnih i web sadržaja. Izrada plana oglašavanja u medijima kroz vanjsku promociju, TV promociju, radio, štampu, Internet, i drugo. Prilikom oglašavanja bitno je voditi računa o budžetu koji je predviđen za isto.

Razvojem tehnologije pojavili su se novi oblici političkih odnosa s javnošću, a prvenstveno odnosa putem Interneta. Možemo s pravom reći da su društvene mreže postale strateško mjesto za provođenje odnosa s javnošću u izbornim kampanjama.

4. CYBER PROSTOR

Za pojam cyber još ne postoji precizna i sveobuhvatna definicije. Anić (2004) navodi kako je cyber prvi element u riječima koji označava nešto vezano uz svijet prividne stvarnosti koji nastaje pomoću informacione tehnologije.

Cyber prostor ili virtuelni prostor je termin koji je prvi put upotrijebio William Gibson u naučnofantastičnom romanu Le Neuromacien, 1984. godine, kako bi opisao čitav skup informacionih resursa koji su raspoloživi preko računarskih mreža. On predstavlja nerealan prostor putem kojeg se prenose elektronski podaci između računara širom svijeta. To nije prostor koji se može vidjeti i dotaknuti, već digitalna konstrukcija razvijena pomoću računara.

Internet ne poznaje prostorne udaljenosti i vremenske zone. Prostorne udaljenosti, vrijeme i brzina više ne predstavljaju konkurentske prednosti. Prednost danas proizilazi isključivo iz znanja, kreativnosti i volje da se nešto učini. Unutar cyber prostora nailazim na

informacije koje možemo vidjeti, čuti i dotaknuti. Virtualni svijet može biti informativan, koristan i zabavan, ali također i dosadan i neudoban.

Cyber prostor je nastao kao rezultat društvenih potreba i tehnoloških inovacija. On nam pruža raznovrsne mogućnosti i u svijetu umreženog društva i predstavlja dominantni kanal komunikacije. Različiti sadržaji na koje u njemu nailazimo su postale svakodnevnica svakog čovjeka, organizacije i države. Cyber prostor možemo istraživati na dva načina:

1. kao korak prema usavršavanju svijeta u kojem živimo, ili
2. kao korak prema stvaranju svijeta o kojem maštamo.

Činjenica jeste da cyber prostor neće zamijeniti interakciju licem-u-lice, ali može uticati na društvene probleme koji su nastali kao posljedica nedostatka komunikacije. Virtualna zajednica je realna, jer se obraća ljudima koji nemaju pravo glasa, a žele biti dio zajednice. To su mjesta okupljanja na kojima se zajednica gradi i traje. Pošto je korijenje virtualne zajednice plitko, ukoliko dođe do trauma i problema, lakše se odvojiti od takve zajednice, nego u slučaju napuštanja
fizičke zajednice (Leburić, Sladić, 2004:51)

4.1. Komunikacija sa javnošću unutar cyber prostora

Informacione tehnologije rapidno rastu i razvijaju se. Njihov uticaj na stanje i razvoj političke vlasti u demokratskom uređenju još uvijek nisu konačno istražene. Cyber prostor je dostupan u svakom trenutku svakome, i u njemu se donosi mišljenje, a zatim i krajnje odluke po pitanju političkih stranki i kandidata. Mnoge političke platforme su danas dostupne široj javnosti, te se putem njih moe doći do onih informacija koje prije nisu bile dostupne. Internet pruža globalni prostor za komunikaciju, gdje se svaka osoba može informisati o političkoj, socijalnoj, ekonomskoj, i drugoj situaciji koja se tiče direktno svakog pojedinca.

S druge strane, te komunikacione tehnologije su dovele do relativno novog oblika demokratije, elektronske ili e-demokratije gdje je uloga Interneta veoma bitna. Ciljevi e-demokratije su transparentnost, razumijevanje, odgovornost, angažovanost, donošenje odluka, uključenost, dostupnost, sudjelovanje, povjerenje u demokratiju, demokratske institucije i demokratske procese. Kako navodi Damnjanović (2009) u stručnom radu, tri su koncepta elektronske demokratije:

1. Teledemokratija,
2. Cyberdemokratija i
3. Elektronska demokratizacija

Teledemokratija: Ovaj pristup se oslanja na kritiku predstavničke demokratije u Sjedinjenim Američkim Država i kritiku izveštavanja klasičnih medija. Teledemokrate polaze od činjenice da se ni politika ni novinarstvo ne mogu na primjeren način suočiti sa sve većim zahtjevima socijalno raslojenog američkog društva. Uspostavljena je prosta demokratija gledalaca, usmjerena samo na velike političke spektakle kao što su preizborne debate i izbori. Ona doprinosi tome da se politička elita udaljava od života svojih birača. Već je pojavom digitalne televizije pokrenut čitav niz novih projekata. Novi mediji mogu da dopune predstavničke sisteme neposredno demokratskim postupcima, a da birači nemaju niakav direktni kontakt ni sa aktivnostima stranke, kao ni sa aktivnostima određenog kandidata. To se može ostvariti na dva načina, tele-glasanjem i pomoću online sastanaka državne, odnosno lokalne vlasti. Na taj način građani imaju osjećaj da su nosioci suvereniteta.

Cyberdemokratija: Pristalice ovog koncepta vide u potencijalima računarskih mreža razlog da zahtijevaju da demokratija bude neposrednija, da vladu više usmjeravaju građani, što oni u postojećem sistemu upravo vide kao manu i zastoj cijelog državnog sistema. Društvu koje danas poznajemo kao „virtuelna zajednica“, komunkacija je dostupna svakog momenta, bez obzira na geografsku rasprostranjenost, te s tim u vezi, ona bi trebala da unaprijedi angažovanost i informisanost kada je političko obrazovanje građana u pitanju. Cyberdemokrate se protive svakoj vrsti državnog centralizma. Usmjereni su u samoorganizovane, nevladine institucije. U skladu s

tim, Internet ne bi trebao da bude samo sredstvo komunikacije već „mreže zajednica“ koje teže ka tome da uspostave i održavaju politički život.

Elektronska demokratizacija: Ovaj koncept se temelji na komunikaciji podržanoj računarima, te da uspostavlja alternativne kanale komuniciranja između onih koji vladaju i onih kojima se vlada. Za razliku od koncepata teledemokratije ili cyberdemokratije, ovdje se prednost ne daje procesima neposredne, već procesima predstavničke demokratije. Novi mediji doprinose tome da državna vlast treba da teži ka tome da bude više dostupna i otvorena za javnost. Na taj način Internet kao sredstvo informisanja, komunikacije i distribucije, treba da podstakne politički angažman građana povećavanjem njihovog stepena informisanosti i uključenosti u sam rad vlade.

4.2. Upravljanje unutar cyber prostora

Napredak tehnologije zadnje dvije decenije omogućio je da nam ulazak u cyber prostor uvijek bude omogućen pomoću pametnih telefona i bežičnog interneta. Shodno tome, pravovremene, tačne i aktuelne informacije određene stranke na njenoj stranici su preduslov za daljnje aktivnosti i promociju. Internet se pokazao kao idealno sredstvo dvosmjerne komunikacije, i upravo takva dvosmjerna komunikacija predstavlja uspješno kreiranje politike zajedno sa građanima. Mediji poput televizije ili radija pružaju oglasne prostore, ali kroz njih se ne može dvosmjerno komunicirati, odnosno učestvovati u raznim diskusijama. Društvene mreže pružaju nepregledan prostor za razmjenu ideja, stavova akcija, gdje svaka stranka i kandidat mogu kreirati stranicu i putem nje se oglašavati i komunicirati sa građanima i biračima.

Cyber prostor je svakodnevno izložen brojnim napadima koji pokušavaju narušiti njegovu cjelovitost, pouzdanost, dostupnost i sigurnost. Cyber napadači mogu biti pojedinci, grupe, kao i države. Cilj cyber napadača može biti nanošenje štete pojedincu, organizaciji, državi i cjelokupnom državnom sistemu. Budući da je cyber prostor postao ključna digitalna informacijsko-komunikacijska infrastruktura na kojoj se temelji uspješnost djelovanja brojnih

drugih nacionalnih i međunarodnih tijela, ni njegova odbrana ne može se rješavati jedino i isključivo unutar nacionalnog odbrambenog sistema. Prema tome, potpuna, efiksna i stručna nacionalna i međunarodna saradnja temeljni su uslovi na kojima treba počivati upravljanje unutar cyber prostora.

Budući da cyber prostor nema granica, načini upravljanja njime još uvijek nisu definisani. To dovodi do problema u kojima je onima koji su spremni počiniti zločine lakše preći granice putem interneta, jer nije jasno gdje je nadležnost. Da se ikad uspostavi upravljački režim, on bi se najvjerojatnije sastojao od više sudionika i aktera, uključujući nacionalne, međunarodne i privatne aktere, poput predstavnika kompanija, društvenih mreža, vladinih i nevladinih organizacija, kao i pojedinaca.

4.3. Prednosti i nedostaci upravljanja u cyber prostoru

Demokratija kakvu danas poznajemo daje pravo građanima da izražavaju svoje stavove za vrijeme izbornih procesa. Za vrijeme predizborne šutnje jako je slaba komunikacija između političara i birača. Zbog toga novi mediji, a posebno društvene mreže, omogućavaju da se i u ovom periodu odvija kmunikacija između političara i građana, među kojima su uglavnom i potencijalni budući birači. Na taj način političke stranke imaju priliku da saznaju i mišljenja javnosti, a sve u cilju adekvatnijeg djelovanja. Ukoliko stranke i kandidati ne koriste Internet kao sredstvo komunikacije, ne mogu ni imati u vidu da li i u kojoj mjeri njihove poduzete akcije ostavljaju pozitivan dojam na javnost. Internet prvenstveno treba smatrati sredstvom dijaloga, a ne sredstvom promocije i oglašavanja.

Političari u Bosni i Hercegovini političari još uvijek nemaju običaje da se na ovakav način povežu sa biračima, pa samim tim nemaju mogućnosti za dvosmjerno komuniciranje koje pruža Internet i razne društvene mreže.

Još jedna od prednosti upravljanja u cyber prostoru jeste ta što i male stranke u komunikaciji sa potencijalnim biračima, imaju šansu za ravnopravan položaj sa velikim strankama iza kojih stoji mnogo novca. Manje političke stranke pokazuju veću efikasnost i produktivnost upravo zbog mogućnosti ravnopravnog promovisanja, a s ciljem da imaju što veći broj glasova i rangiranja u državnoj vlasti. Društvene mreže i blogovi predstavljaju sredstvo kojim stranke mogu pridobiti članove i birače kako bi sudjelovali i aktivno provodili izborne kampanje u stvarnom svijetu. S druge strane, kriminal o kojem ćemo kasnije više govoriti, predstavlja veliki nedostatak virtuelnog djelovanja kao što je to slučaj u cyber prostoru.

5. ETIKA U CYBER PROSTORU

Etika se bavi vrijednostima i pravilima koje pojedinac ili društvo smatra poželjnima ili nepoželjnima. Kako navode Silajdžić i Mahmutćehajić (2019:176-185), pri procjeni posljedica postoje tri različita pristupa u odlučivanju o moralnom ponašanju. To su etički egoizam, utilitarizam i altruizam. Prema etičkom egoizmu, postoji samo jedno načelo ponašanja: načelo vlastitog interesa koje upotpunjuje sve dužnosti pojedinca. Ono što djelovanje čini ispravnim jest činjenica da je u vlastitu korist. Utilitarizam je također konzekvencijalistička teorija koja ispravnost određenog postupka određuje s obzirom na posljedice koje će taj postupak imati na sve jedinke njime zahvaćene. Prema tome, moralno ispravan je onaj postupak koji za posljedicu ima najveću ukupnu količinu korisnosti (utility). Utilitarizam se stoga čestoodređuje i kao teorija koja za ispravno djelovanje uzima ono koje donosi najveću moguću korist dobrih nad lošim posljedicama (ili najmanju moguću korist loših nad dobrim posljedicama). Načelo na kojem se temelji ova etička teorija utilitaristi nazivaju „načelo najveće sreće“ (Greatest Happiness Principle). Moralnost je karakteristika koja određuje ovo načelo. Koncept altruizma definiše određeno moralno načelo koje prisiljava ljude da nesebično pomažu drugima, često žrtvujući vlastite interese, želje i potrebe. Dakle, altruizam jeste ponašanje kojem je cilj pomoganje drugima, a da se ne očekuje neka vrsta nagrade od njih. Altruistični postupci su svjesni i sadrže namjeru da se nekome pomogne i zahtijevaju određeno žrtvovanje ili odricanje.

Kao što je već spomenuto, vodstvo je proces u kojem vođa utiče na druge kako bi ostvarili zajednički cilj. Budući da vođe imaju više moći i nadzora nego sljedbenici, imaju i veću odgovornost. Etika je važna za vodstvo, prije svega zbog potrebe za uključivanjem sljedbenika pri ostvarenju zajedničkih ciljeva, a zatim i zbog uticaja koji vođe imaju na organizacijsko funkcionisanje. Politika predstavlja područje gdje je etika odnosno etički ispravno ponašanje jedno od važnijih karakteristika svih njenih učesnika. Upravo to etički ispravno ponašanje i djelovanje, obezbjeđuje glasove na izborima. Način tog ponašanja i djelovanja kojim se odvija izborna kampanja i lobiranje novih birača, govori mnogo o stranci i kandidatima koje predlaže.

Čovjekovo moralno i etičko djelovanje se upravo može uočiti na političkoj sceni. Potreba za kodeksima ponašanja je uvijek prisutna, bez obzira da li nastupa kandidat kao pojedinac, ili cijela stranka kao organizacija. Kada je političko djelovanje u pitanju, mora postojati javna svijest koja će zahtijevati poštovanje etičkih i moralnih principa. Za izgradnju javne svijesti važni su pravedni krivični zakoni i njihova dosljedna primjena. Potrebna je etika sa pogledom unaprijed, etičko rasuđivanje koje će se dogoditi prije učinjene radnje. Osnovna načela i vrijednosti određuju način razmišljanja i postupanja, postaju izvor za konkretna nadahnuća i djelovanja, pomažu rješavanje konkretnih pitanja:

1. Dostojanstvo čovjeka,
2. Odnos osoba – društvo,
3. Ljudska prava,
4. Opšte ili zajedničko dobro,
5. Solidarnost,
6. Participacija,
7. Preferencija opcije za siromašne, osnovne vrijednosti: istina, sloboda, pravda, solidarnost, mir i djelotvorna ljubav.

Vođenje etičke politike u savremenim uslovima demokratije iziskuje izuzetne napore, a iznad svega visok nivo svijesti o značaju etičkog djelanja zasnovanog na plemenitim vrijednostima.

5.1. Deontološki pristup

Deontologija jeste etička pozicija koja polazi od dužnosti kao osnove moralnosti. Najznačajniji zastupnik deontološkohg pristupa jeste Immanuel Kant. Prema Kantu, dužnost je nešto uzvišeno, veliko i veličanstveno. Poštovanje i obavljanje ljudskih dužnosti jeste moralni imperativ, koji doživljavamo kao zapovijest našeg uma koje zahtjeva da naše postupanje bude takvo da ispunjava ljudsko načelo.

Etici dužnosti se može pristupiti na više načina, ali im je zajedničko da ispravno ili pogrešno djelovanje nije određeno samo posljedicama, nego i namjeri samog djelovanja. Primjer deontološkog pristupa etici jeste dobro poznata svima, a to je Deset božjih zapovijedi. To je skup pravila, koji identificira određene oblike djelovanja kao one kojih se trebamo pridržavati, odnosno od kojih se trebamo suzdržavati, bez obzira na njihove posljedice. Pođe li se od dužnosti kao kategorije koja je svojstvena i za svaku etiku i za svako pravo, onda je u etici prava moguće govoriti o deontološkom pristupu. Prema ovom pristupu, čovjek ima unaprijed, u skladu sa svojom prirodom, dužnost da djeluje pravedno, pri čemu tu dužnost ne može osporiti nikakvo nepredviđeno događanje i posljedice. Shodno tome, nameće se pitanje: Da li je čovjek sposoban svoje etičke norme mijenjati i prilagođavati sa onim izazovima koje nameću promijenjene okolnosti života, pa tako i one u cyber prostoru?

Deontologijom se zove cijelo područje u kojem su dužnosti polazna osnova pravnog pristupa, procedura i rješenja. Pravna pravila određuju i nameću prava i dužnosti i propisuju postupke za postizanje različitih ciljeva u teoriji i praksi. U različitim deontološkim priručnicima, pravnici, prije svega žele da podstaknu na etičke i moralne dužnosti.

5.2. Konzekvencijalistički pristup

Prema konzekvencijalističkom pristupu potrebno je donijeti odluku koja će najvećem broju ljudi donijeti najveću sreću, odnosno prema principu koji je poznat kao princip najveće sreće. Osnivač konzekvencijalističkog pristupa, Jeremy Bentham, bio je uvjeren da je moguće izmjeriti i izračunati količinu sreće i tako donijeti odluku koja je etički ispravna prema principu najveće sreće. Prema Benthanu, pri izračunavanju sreće u obzir potrebno je uzeti sljedeće:[3]

- intenzitet – to je jakost ili snaga sreće; ako postupak dovodi do trostruko jačeg osjećaja sreće tada je taj postupak trostruko bolji postupak;
- trajanje – postupak je bolji što sreća traje duže (npr. postupak koji proizvede dva sata sreće dvaput bolji od postupka koji proizvede jedan sat sreće);
- izvjesnost ili neizvjesnost – bolji je onaj postupak čija je vjerojatnost za sreću veća (npr. postupak koji s vjerojatnošću od 50 posto dovodi do neke količine sreće dvostruko je bolji od postupka koji dovodi do iste količine sreće s vjerojatnošću od 25%);
- bliskost ili udaljenost – postupak je bolji što brže dovodi do sreće (npr. ako će postupak dovesti do sreće za dva sata onda je on bolji od postupka koji će do sreće dovesti za tri sata);
- čistoća - omjer sreće i boli do koje dovodi neki postupak (ako dva postupka dovode do jednake količine sreće, bolji je onaj postupak koji do te sreće dovodi uz manje boli);
- obim - broj ljudi na koje se odražava neki postupak, postupak je bolji što usrećuje veći broj ljudi (npr. postupak koji usreći sto ljudi sto je puta bolji od postupka koji usreći jednog čovjeka).

Konzekvencijalistički pristup uzima u obzir posljedice djela, za razliku od deontološkog koji se osniva na temelju unaprijed određene dužnosti. Stroga primjena dužnosti kao kategoričkog imperativa znači da pravnog sudionika ne obavezuje pretpostavljena posljedica. On svoju odluku donosi na osnovi tog što je normirano kao njegova dužnost, pa je kao takvo u skladu sa njegovom prirodom u kojoj je razumsko prosuđivanje osnova djelovanja. To znači da

[3] Berčić, B. (2012): Filozofija. Ibis: Zagreb, str. 134

primjena dužnosti može imati za posljedicu ugrožavanje temeljnog prava. Ako konzekvencijalistički pristup nije potpuna zamjena za deontološki, onda on može biti njegova važna nadopuna. Kada sudionik pravnog odlučivanja može s dovoljnom pouzdanošću pretpostaviti posljedicu nekog djelovanja kojom je ugroženo nečije pravo, što bi moglo biti izbjegnuto ili umanjeno uz žrtvovanje deontološki određene norme, opredijelit će se za onu odluku koja će omogućiti najbolji ili najmanje štetan ishod.

Deontološki i konzekvencijalistički pristup su nadopuna ili alternativa jedan drugome. Ako se odlučuje primijeniti konzekvencijalistički pristup, to znači da presuđuje procjena posljedice. Procjenu je moguće napraviti s većom ili manjom vjerovatnošću, pa će o tome ovisiti i pravna odluka: ako se sa sigurnošću može procijeniti posljedica koja je bolji ishod postupka, uz uvjet da se odustane od deontoloških dužnosti, razložno je donijeti upravo takvu odluku. Najproširenija teleološka teorija je utilitarijanizam. U njoj je korisnost posljedice presudni faktor za donošenje odluka, pa je ona konzekvencijalistička. U skladu s tom teorijom, ispravno djelovanje unapređuje opće dobro. To opće dobro može biti opisano u pojmovima „korisnosti“. Princip korisnosti je temelj moralnosti i krajnji kriterij ispravnosti i neispravnosti. Korisnost se odnosi na krajnju dobit koju daje neko djelovanje. S etičkog stanovišta, princip korisnosti nije bezuvjetno mjerilo. Nije prihvatljivo predviđanje najveće moguće koristi za pojedinca, pri čemu se zanemaruje ili isključuje činjenica da pojedinac ima položaj i veze u društvu te da njegova korist ne može proizvoditi štetu za druge. Praktično, utilitarijanizam nameće donošenje moralnih odluka pomoću racionalne procjene objektivnih troškova i dobiti. U većini moralnih dilema na raspolaganju su različite mogućnosti djelovanja. Čim su te različite mogućnosti određene i razvrstane, svaka od njih je ocjenjivana u pojmovima njenih direktnih ili indirektnih troškova i dobiti. Na osnovi uvida u te različite mogućnosti, odlučuje se za onu s najvećim ukupnim dobitima ili najmanjim ukupnim troškovima za najširu zajednicu na koju utiče ta odabrana mogućnost.

5.3. Etika vrline

Posljednja od glavnih etičkih teorija koju ćemo objasniti jeste etika vrlina koja potječe još od Aristotela. Za razliku od prethodne dvije teorije gdje prioritet u vrednovanju imaju njihovi postupci, etika vrlina je teorija u savremenoj etici prema kojoj prioritet u vrednovanju imaju karakterne osobine i vrline. Pojam vrline u antičkoj Grčkoj se koristio i u izvanmoralnom smislu: ono što je dobro kvalitetno obavlja svoju funkciju i time ispunjava svoju svrhu. Kada govorimo o moralnim vrlinama, bitno je reći kako je Aristotel smatrao da ih ljudi ne posjeduju po svojoj naravi. Ono što posjedujemo su određeni kapaciteti za njihovo ostvarenje i bitna stvar jeste da kroz adekvatan odgoj izgradimo dobar karakter. Ovdje se zapravo postavlja pitanje što čini dobru osobu. Često se kaže da nam deontološki i konzekvencijalistički pristup govore „Što trebamo činiti?“, dok nam etika vrlina govori „Kakvi trebamo biti?“. Prema tome, etika vrlina u fokus stavlja to kakvi jesmo, a ne šta činimo.

Mogućnosti izbora deontološkog ili konzekvencijalističkog pristupa u svim njihovim oblicima, kao i njihovih kombinacija, stavlja čovjeka koji rješava konkretan slučaj pred odluku o izboru. Ako deontološki i konzekvencijalistički pristup imaju oslonac u objektivnom znanju koje je moguće formulisati u smjernice, uputstvo i priručnik, drugi pristup, bilo da je on njihova nadopuna, oslonac traži u osobi kao subjektu odlučivanja. Osoba, u našem slučaju političar djeluje s jasnom ulogom ili ciljem gdje su bitna tri faktora:

1. djelovanje,
2. funkcija koja se obavlja i
3. cilj s kojim je ta funkcija povezana.

Dobrog političkog kandidata karakteriše njegovo djelovanje i djelovanje stranke u skladu sa Zakonom. Etika vrline mora postati svojstvo karaktera u kojem se proizvode stavovi i vrline određenog kandidata ili stranke. Mora se znati zašto se čini to što se čini. Prisustvo morala zahtjeva da se preuzme lična odgovornost za odluke i akcije. To znači da se od svake stranke i kandidata očekuje da iznese i objasni razloge svoga djelovanja, odluka i poduzetih akcija.

6. KRIMINAL U CYBER PROSTORU

Računarski kriminal obuhvata kriminal vezan za kompjuterske mreže koje se koriste:

- Kao cilj napada (napadaju se serveri, funkcije i razni sadržaji koji se nalaze na mreži);
- Kao sredstvo ili alat (prodaja putem Interneta kao što su seksualne usluge, ljudski organi, ljudi općenito (trgovina ljudima), dječija pornografija, vjerske sekte i drugi nedozvoljeni sadržaj;
- Kao okruženje u kojem se napadi realizuju (korištenje cyber prostora za prikrivanje kriminalnih radnji).

Pored toga, računarski kriminal podrazumijeva kriminal vezan za računarske sisteme (hardver i softver) koji se koriste kao sredstvo izvršenja krivičnog djela. Pojam cyber kriminal se veže za oblik kriminalnog ponašanja koji podrazumijeva korištenje računarske opreme. Ovaj oblik kriminala šteti bezbjednosti računarskih sistema, s ciljem da se nekome ili nečemu nanese šteta. Osobe koje vrše takve kriminalne radnje se nazivaju cyber kriminalci. Najčešći oblici načina izvršenja krivičnog djela iz oblasti cyber kriminala su (Duggan, 2015, str., 141.):

- neovlašteno dolaženje do pasvorda i korištenje istih bez dozvole stvarnih vlasnika a u cilju pribavljanja protivpravne materijalne koristi ili drugih benefita (zloupotreba informacija u cilju diskreditacije vlasnika ili sakrivanja stvarnog autora informacija preko drugih IP adresa...)
- neovlašteno sprečavanje ili ometanje pristupa javnoj mreži,
- izrada i unošenje računarskih virusa u namjeri njegovog unošenja u tuđi računar ili računarsku mrežu ili telekomunikacionu mrežu,
- unos netačnih ili propuštanje unosa tačnih podataka ili na drugi način uticanje na rezultat elektronske obrade i prenosa podataka u namjeri pribavljanja protivpravne imovinske koristi,
- zloupotreba audio-vizuelnih sadržaja.

U zavisnosti od tipa počinjenog djela, cyber kriminal može biti:

- politički, koji čine cyber špijunaža, hakiranje, cyber sabotaža, cyber ratovanje i cyber terorizam;
- ekonomski cyber kriminal čine cyber prevare, hakiranje, krađa internet usluga, piratstvo softvera, piratstvo mikročipova i baza podataka, prevare internet aukcije, cyber industrijska špijunaža;
- proizvodnja i distribucija nedozvoljenih i štetnih sadržaja čine, pedofilija, dječija pornografija vjerske sekte, širenje rasističkih i nacističkih kao i sličnih ideja i stavova, zloupotreba žena i djece, manipulacija zabranjenim proizvodima, supstancama i robom (droga, ljudski organi, oružje);
- povrede cyber privatnosti čine nadgledanje e-pošte, spam, phiching, prisluškivanje, praćenje e-konferencija, itd.

Sama namjena i prostor u kojem djeluje čine da se cyber kriminal ne može kontrolisati unutar granica neke države. Kako predstavlja prijetnju za pojedinca, tako i za državnu sigurnost. Za ovakvu vrstu kriminala posebno su pogodne društvene mreže čijom pojavom je cyber kriminal napredovao. One predstavljaju sredstvo preko kojeg cyber kriminalci na lak način dolaze do svojih ciljeva. Društvena mreža koja je posebno poznata po konstantnoj prisutnosti cyber kriminala je Facebook. Neki od oblika ovog vida kriminala su krađa identiteta, rad na crno i dječja pornografija. Najviše zastupljeni su krađa identiteta i dječja pornografija. Iako nije tačno poznato koliko cyber kriminal utječe na ekonomiju zemalja pretpostavlja se da se gubici mjere u bilionima eura godišnje.

Postoje određene mjere i metode predostrožnosti koje se mogu napraviti u cilju zaštite od cyber kriminala. Neke od njih se realizuju na sljedeći način:

1. Korištenje anivirusnog paketa koji obuhvata kompletnu uslugu internet sigurnosti. Malware je zajednički naziv za štetne programe kojim se najčešće služe cyber kriminalci kako bi pristupili tuđim kompjuterima. Takvi programi su obično skriveni u prilozima e-

mailova ili kao besplatan sadržaj na Internetu. Antivirusni program je potrebno redovno ažurirati, te pratiti upozorenja koja nam javlja.

2. Koristiti šifre sa znakovima, simbolima i slovima koje nije lako pogoditi, te ih mijenjati s vremena na vrijeme. Kada se bira šifra ne treba koristiti neku riječ ili datum koji imaju veze sa nama lično, već generisane šifre, a u tome nam može pomoći pasvord generator.
3. Kako se ne bi desilo da zaboravimo svoju šifru, lastpass vrlo lako može spasiti i sačuvati šifru za bilo koju stranicu. To će smanjiti šansu da neko pogodi našu šifru te ukrade naš identitet, zloupotrijebi informacije i slično.
4. Zaštititi svoje lične podatke na društvenim mrežama pomoću postavki za privatnost. Lični podaci koji su lako dostupni cyber kriminalcima mogu biti iskorišteni protiv nas, tako da, što manje informacija dijelimo javno, to je bolje sa aspekta sigurnosti. Treba voditi računa o sadržaju koji se objavljuje, jer sve što se jednom objavi, zauvijek ostaje na Internetu.
5. Važno je voditi računa o tome koje stranice posjećujemo i na kojim sajtovima pravimo svoje korisničke račune. Ukoliko posjećujemo online kockarnice, trebalo bi pratiti savjete stručnjaka koji stranice detaljno pregledaju i ocijene da li su sigurne i pouzdane za korištenje.
6. Zaštita kućne mreže (home network) sa jakom šifrom, kao i VPN. VPN (virtual private network) će šifrirati sav promet ostavljajući naše uređaje dok ne stigne na odredište. Čak i ako haker uspije doći u našu komunikacijsku liniju, oni neće opstruirati ništa osim šifriranog prometa.
7. Oprezno surfati internetom i paziti kakav sadržaj se preuzima. Pripaziti se lažne e-poruke (phishing) finansijskih institucija u kojima se od nas traži da potvrdimo podatke o računu. Takve e-poruke trebamo prijaviti institucijama od kojih navodno dolaze, kako bismo pomogli u razotkrivanju prevaranta. Finansijske institucije nikada od svojih korisnika ne traže bilo kakve potvrde putem e-poruka.
8. Razgovarati sa svojom djecom o prihvatljivom načinu upotrebe interneta i pratiti njihovu online aktivnost. Usmjeriti ih ka prikladnim internetskim stranicama. Osigurajti im da

znaju da nam se mogu obratiti ukoliko dožive bilo kakvo neugodno iskustvo online, poput uznemiravanja ili uhođenja.

9. Ukoliko počnemo sumnjati da smo žrtva cyber krimnala, moramo upozoriti lokalnu policiju o onome šta nam se dešava. Ako se i čini da zločin možda i nije toliko ozbiljan, ipak ga trebamo prijaviti jer time možemo pomoći u spriječavanju iskorištavanja ljudi u budućnosti.

Države članice Vijeća Europe i ostale države potpisnice, dana 23.01.2001. godine su u Budimpešti usvojile Europsku konvenciju o računarskom kriminalu, a Bosna i Hercegovina je dana 25.03.2006. godine donijela Odluku o ratifikaciji ove Konvencije. Cilj Konvencije je da realizira vijeće jedinstvo između svojih članova i intenziviranje saradnje sa drugim državama članicama Konvencije u borbi protiv cyber kriminala i potrebu za zaštitom legitimnih interesa povezanih sa razvojem računarskih tehnologija, sprečavanje zloupotrebe računarskih sistema, mreža i podataka, te brža i efikasnija borba protiv krivičnih djela počinjenih u cyber prostoru, olakšavajući njihovo otkrivanje, istragu i gonjenje kako na unutrašnjem, tako i međunarodnom nivou. Konvencija razlikuje četiri vrste krivičnih djela počinjenih u cyber prostoru, i to (Karahmetović et al., 2019):

- djela protiv povjerljivosti, integriteta i dostupnosti računarskih podataka i sistema, u koja se ubrajaju: nedozvoljeni pristup računarskim sistemima, povreda integriteta podataka, povreda integriteta sistema i zloupotreba;
- računarska djela, u koja se ubrajaju računarsko falsificiranje i računarska prevara;
- djela vezana za sadržaj, u koja se ubrajaju djela koja se odnose na dječiju pornografiju;
- djela u vezi sa napadom na intelektualno vlasništvo i odnosna prava.

Cilj Konvencije jeste da države potpisnice uvrste prethodno navedena krivična djela (ukoliko već nisu) u nacionalna krivična zakononska uređenja. Konvencija je naročito važna zbog brzine djelovanja strana u postupku. Države potpisnice, pa tako i Bosna i Hercegovina su odredile kontakt osobu u ovakvim vidovima međunarodne pomoći i sradnje, koja će biti dostupna za saradnju 24 sata na dan i 7 dana u sedmici, a u cilju osiguranja trenutne pomoći u

istragama koje se tiču krivičnih djela povezanih sa računarskim sistemima. Kontakt osoba u Bosni i Hercegovini je ovlaštena službena osoba iz Federalne uprave policije Federacije Bosne i Hercegovine i ovlaštena službena osoba iz Ministarstva unutrašnjih poslova Republike Srpske. Međutim, ono što je bitno ovdje naglasiti jeste to da Bosna i Hercegovina još uvijek nije napravila strategiju o zaštiti osjetljivih računarskih podataka. Iako se neke strategije djelimično bave pitanjem cyber sigurnosti, Bosna i Hercegovina ostaje jedina država u jugoistočnoj Europi bez sveobuhvatne strategije cyber sigurnosti na državnom nivou. Najpoznatiji cyber napadi u svijetu su:

1. WannaCry Ransomware napad - WannaCry ransomware jeste cyber napad koji uključuje infekciju Microsoft Windowsa pomoću računarskog crva. Preko 230 000 računara su napadnuta u 150 zemalja širom svijeta. Wannacry ransomware uključuje šifriranje datoteka iz ranjivih računara i zahtijeva plaćanje otkupnine u iznosu od oko 600 dolara koje se plaćaju u kriptovaluti. Uzrok infekcije iza napada smatra se EternalBlue koji je razvila američka Nacionalna sigurnosna agencija, ali je procurio u Shadow Brokers, skupinu hakera. Međutim, otkriće prekidača ubijanja minimiziralo je širenje ransomwarea.
2. Shamoon Računarski virusni napad - Shamoon je vrsta računarskog virusa koji se pripisuje infekciji računarskih sistema i cyber špijunaže na računarima u energetskom sektoru. Također poznat kao Disttrack, Shamoon je koristila grupa hakera pozna pod nazivom „Rezanje mačeva pravde“.
3. Operacija Olimpijske igre - Operacija Olimpijske igre je šifrirani naziv za sabotaže i poremećaje nuklearnih postrojenja u Iranu putem internetskih napada. Tvrdi se da je izvor napada vlada Sjedinjenih Američkih Država i Izraela, ali dvije zemlje nikada službeno nisu priznale odgovornost. Kampanja sabotiranja iranskih nuklearnih reaktora započela je tokom uprave predsjednika Busha i nastavljena je tokom administracije predsjednika Obame. Dvije zemlje su koristile računarski virus poznat kao Stuxnet da bi se infiltrirao u iranske računarske sisteme koji su mogli zaustaviti rad u 1 000 centrifuga u nuklearnoj elektrani Natanz. Međutim, infekcija računara nije bila ograničena samo na nuklearni objekt, već se virus proširio na nekoliko ličnih računara u regiji.

4. Operacija Shady Rat - Operacija Shady Rat je šifrirani naziv za neprekidni cyber napad usmjeren na vladine institucije i organizacije u 14 zemalja širom svijeta, pa čak i na međunarodne organizacije kao što su Ujedinjeni narodi. Operacija Shady RAT uključivala je infiltraciju računarskih sistema i krađu vrijednih i osjetljivih dokumenata s računara. Dmitri Alperovitch koji je nazvao cyber napad vodio je istrage kako bi utvrdio izvor napada. Zbog povećanja napada u danima prije Ljetnih olimpijskih igara 2008. godine u Kini, analitičari vjeruju da su napade sponzorisan od strane kineske vlade.
5. Titan Rain - Titan Rain je kodni naziv za niz cyber napada na američke računarske sisteme koji su se dogodili početkom 2000-ih godina. Napadi su bili usmjereni na glavne izvođače Ministarstva odbrane, uključujući Redstone Arsenal, NASA i Lockheed Martin. Cyber napadi su bili u obliku cyber špijunaže gdje su napadači uspjeli dobiti osjetljive informacije iz računarskih sistema. Istrage o utvrđivanju uzroka napada pokazale su da su kineske vojske imale ruku u njihovom pogubljenju, što je kineska vlada poricala. Ostali sporadični napadi usmjereni su na britansko ministarstvo obrane, što je događaj koji je ozbiljno zategnuo odnose između Velike Britanije i Kine.
6. Cyber napadi u Estoniji 2007. godine - 27. aprila 2007. godine Estonija je bila podložna nizu cyber napada na neviđenom nivou. Napadi su paralizirali računarske mreže u parlamentu Estonije, ministarstvima, bankama i medijima. Napadi su bili odgovor na odluku o premještaju brončanog vojnika iz Talina, kao i ratnih grobnica u glavnom gradu. Neposredna reakcija estonske vlade bila je baciti krivnju na ruski Kremlj, optužbe koje se kasnije povukla zbog neosnovanosti. Vlada je također povećala ulaganja u cyber sigurnost, kao i izradu Priručnika o međunarodnom pravu u Talinu koji se primjenjuje na cyber ratovanje i koji opisuje međunarodne zakone o cyber ratovanju. Julski 2009. cyber napadi - U julskim cyber napadima bilo je nekoliko cyber napada koji su se širili protiv Južne Koreje i Sjedinjenih Američkih Država. Cyber napadi koji su se dogodili u tri vala uticali su na više od 100 000 računara u dvjema zemljama i upućeni su na internetske stranice državnih institucija, uključujući Bijelu kuću, Južnokorejsku nacionalnu skupštinu, Pentagon i medijske kuće. Iako tačan izvor napada nije poznat, mnogi analitičari ukazuju na telekomunikacijsko ministarstvo Sjeverne Koreje.

7. OpIsrael - Izrael je bio skraćenica za niz cyber napada koji su se širili protiv izraelskih internetskih stranica. Cyber napadi započeli su za vrijeme Dana sjećanja na holokaust, 7. aprila 2013. godine i uključivali su curenje baza podataka, otmice baza podataka i defacemente. Web stranice su bile usmjerene na one koji pripadaju školama, izraelskim novinama, malim preduzećima, neprofitnim organizacijama i bankama.
8. Cyber napadi na Mijanmar - Godina 2010. bila je godina kada je Mijanmar proveo svoje prve izbore za 20 godina. Međutim, u nekoliko mjeseci koji su prethodili izborima, zemlju je pogodio niz cyber napada koji su uticali na mnoge korisnike interneta širom zemlje. Cyber napadi na Mijanmar 2010. godine bili su DDoS prirode (distribuirano uskraćivanje usluge) i počeli su 25. oktobra 2010. godine. Napadi su preplavili Ministarstvo pošte i telekomunikacija, vodećeg internetskog pružatelja usluge u zemlji, preplavivši podatkovni ulaz s više podataka od propusnosti. Vladajuća stranka u zemlji spekulirala je da je uključena u cyber napade kao način ušutkavanja neslaganja.
9. Singapurski cyber napadi - Cyber napadi u Singapuru u 2013. bili su niz cyber napada koje je provodila skupina hakera Anonymous protiv vlade Singapura. Prema riječima hakera, napadi su bili odgovor na donesene propise o web cenzuri od strane vlade. Sajber napadi su trajali nekoliko dana i bili su usredotočeni na vladine web stranice, kao i na račune društvenih medija utjecajnih ljudi.

Među političkim cyber kriminalima posebno se izdvajaju: izdaja, špijunaža i neka vojna krivična djela. Izdaja se sastoji u pružanju pomoći neprijateljskoj zemlji u borbi protiv svoje zemlje na taj način što se učestvuje u ratu na strani neprijatelja, daju obavještenja o tajnama svoje zemlje i slično. Špijunaža se sastoji u prikupljanju u namjeri predaje, saopštavanju ili predaji tajnih (povjerljivih) podataka stranoj državi. Tajni podaci su od posebnog državnog, vojnog i nacionalnog interesa i oni se mogu predati i saopštiti stranoj državi ili putem izveštaja pojedinaca ili kroz rad posebnih obavještajnih službi. Da bi onemogućila rad stranih obavještajnih službi, države izgrađuju sisteme kontraobavještajnih službi sa svojim specijalizovanim agencijama. Vojna krivična djela koja pripadaju političkom kriminalitetu obuhvataju sve aktivnosti kojima se ugrožava vojna bezbjednost i spremnost jedne države.

6.1. Cyber špijunaža

Osnovna karakteristika cyber špijunaže jeste odavanje podataka, prije svega tajnih informacija, a osnovni oblik jeste odavanje i predavanje povjerljivih podataka. Pri tome špijunaža može biti motivisana političkim, vojnim ili ekonomskim razlozima, zbog čega se mnoge zemlje preko svojih tajnih službi angažuju u otkrivanju službenih tajni drugih zemalja.

Cyber špijunaža nužno podrazumijeva otkrivanje i dobijanje tajne, pri čemu vlasnik iste nije dao odobrenje za to, bez obzira radi li se o jednom vlasniku ili više njih. Cyber špijunaža za svoje kriminalne radnje koristi isključivo Internet. Prilikom izvođenja cyber špijunaže uglavnom se koriste špijunski programi (Keyloger, RAT,...), trojanski konji (specijlni trojanci napravljeni da špijuniraju korisnika), virusi i slično. Osnovna karakteristika cyber špijunaže je odavanje tajne, a osnovni oblik je saopštavanje, predaja ili ustupanje povjerljivih podataka za koje nije dato odobrenje. Pri tome špijunaža može biti motivisana vojnim, političkim ili ekonomskim razlozima.

Teško je reći koliko se u današnjem vremenu slučajeva špijunaže događa svakodnevno. Mediji iz svih zemalja svijeta izvještavaju o velikim špijunskim aferama, ali razlog što znamo za njih jeste taj da je neko prilikom ovih kriminalnih radnji razotkriven i najvjerovatnije uhvaćen. Također, jako je teško procijeniti koliko se špijunaže događa u svijetu, prvenstveno zbog toga što u mnogim slučajevima razne vladine institucije, agencije i organizacije ne iznose u javnost uspjele ili neuspjele pokušaje prisluškivanja i špijunaže zbog negativnog publiciteta. Poznati su određeni faktori koji mogu pomoći u shvaćanju obima cyber špijunaže. To su:

- Povoljna cijena kao dostupnost računara koja su sve jednostavnija za korištenje;
- Računari se koriste za čuvanje povjerljivih podataka;
- Podaci se u elektronskoj formi lako prebacuju i prenose;

- Današnji operativni sistemi i aplikacije sadrže mnoge elemente sigurnosnih slabosti i propusta;
- Rasprostranjenost, pristupačnost i upotrebljivost Interneta su dovele do ubrzanog i učestalog razvoja cyber špijunaže.

Cyber špijunaža se najčešće koristi u industriji kako bi se stekla prednost nad konkurencijom tako da se istraži proizvod koji će se plasirati na tržište, te pokuša napraviti jednak ili bolji proizvod prije nego ga konkurencija stigne plasirati. Također, još jedna od najčešćih primjena cyber špijunaže jeste u vojne svrhe. Razlog za to je što svaka zemlja želi biti najjača i želi znati čime raspolažu druge zemlje jer vojna nadmoć, nažalost, znači i nadmoć u svemu ostalom. Cyber špijunaža se izvodi pomoću špijunskih programa, računarskih virusa, trojanskih konja i raznim drugim načinima. Kako i u kojoj mjeri se cyber špijunaža može uzeti u obzir ako govorimo u kontekstu cyber politike? Političke stranke i njihovi kandidati prilikom svojih kampanja prezentuju ideje i stavove za koje se salažu, gdje se te ideje prije samo predstavljanja javnosti, dijele između članova stranke, putem e-maila, foruma, chata, privatnih poruka i slično. Protivničke stranke ukoliko žele doći do plana djelovanja druge stranke ili kandidata, to mogu učiniti na lak način, samo ukoliko u svojim redovima imaju nekog ko uspješno vlada informacijonom tehnologijom i savremenim vidovima komunikacije.

6.2. Hakiranje

Hakiranje (engl. hacking) je neovlašteni pristup podacima i programima, a njegovu pojavu uslovio je brzi napredak informacione tehnologije, koji je donio činjenicu da se danas najrazličitije arhive i ustanove za čuvanje podatka, počevši od privatnih, preko poslovnih, pa do državnih, temelje na automatskoj obradi podataka podržavanoj računarima i raznim softverima namjenjenim za analizu i obradu podataka. Prema Eric S. Raymondu, američkom računarskom programeru, koji je ujedno i zagovornik i autor pokreta otvorenog koda, haker (engl. hacker)

izvorno označava osobu koja izrađuje namještaj sjekirom. Eric daje osam mogućih razumijevanja pojma haker. Definiše hakera kao osobu koja uživa istražujući detalje programskog sistema i kako proširiti njegove sposobnosti. Onaj koji entuzijastično, čak i opsesivno programira. Osoba koja cijeni hakerske vrijednosti, brza je u programiranju. Haker može biti ekspert za bilo koji program ili bilo ko ga često koristi. Haker također može označavati bilo kakvog entuzijastu koji ne mora biti vezan uz računar. Na primjer, haker može biti astronom koji je entuzijastičan oko onoga što radi. Hakeri se mogu definirati i kao osobe koje vole intelektualne izazove i kreativno prelaženje granica. Zadnje definiranje pojma haker je da je on zlonamjerna osoba koja pokušava otkriti osjetljive informacije.Osnovne karakteristike hakinga su:

- Neovlašten i detaljno planiran pristup;
- Nasilan pristup prilikom razbijanja i ulaska u zaštite sistema;
- Pristup se realizuje kroz upad u sistem, pri čemu se termin „upad“ koristi za označavanje raznih metoda i tehnika provaljivanja u sistem;
- Upadi u sistem baziraju se na visokom profesionalnom znanju;
- Mjesto upada je po pravilu udaljeno od mjesta gdje se organizovao napad i nalazi napadač;
- Napadač istovremeno čini i druga djela: špijunažu, sabotažu, prevaru, pronevjeru, krađu usluga, distribuciju virusa i razne druge manipulacije;
- Haking mogu da organizuju i izvode pojedinci ili grupe.

Napadi na mrežnu infrastrukturu mogu biti bez poteškoća planirani i izvedeni jer mnogim mrežama se može pristupiti s bilo kojeg mjesta u svijetu putem Interneta. Metode sigurnosti koje koriste sistemi zaštite računarske infrastrukture moraju biti aktivne i dovoljno efikasne kako bi otkrile i spriječile lažno predstavljanje. Kod lažnog predstavljanja, moramo razlikovati fizičku i elektronsku formu lažnog predstavljanja. O fizičkom predstavljanju govorimo kada počinitelj koristi relevantan korisnički identitet kako bi pristupio povjerljivim računarskim podacima. Za lažno predstavljanje kažemo da je elektronsko kada počinitelj koristi legalni korisnički identifikacijski broj ili pasvord kako bi se prijavio u računaraski sistem i na taj način nelegalno

došao u posjed podataka i informacija. Pokušaj da se efikasno preduhitre i spriječe sve veći upadi hakera u važne kompjuterske sisteme, administrativne, korporacijske i vojne baze podataka, strategija Sjedinjenih Američkih Država, koja između ostalog, hakerski napad na informacione sisteme smatra činom rata, naglašava sankcije i određene kazne za ovakva djela, zbog čega će Pentagon biti spreman da, po potrebi, uzvrati i tradicionalnom vojnom silom.

Najveća hakerska konvencija osnovana je 1992. godine pod imenom DEFCON u Las Vegasu u obliku zabave na kojoj se pojavilo stotinjak ljudi. Na dvadesetoj DEFCON konferenciji je prisustvovao direktor NSA-e (engl. National Security Agency), general Alexander. Pojavilo se je preko 10 000 ljudi iz različitih zemalja. Društvo na konvenciju DEFCON promatra kao anonimni nelegalni skup na kojem se uče nelegalne djelatnosti. Suprotno navedenome, sami polaznici DEFCON-a ga definišu kao javno finansiran privatni party na koji dolaze hakeri kako bi se družili, razmijenili znanja i postignuća.

6.3. Cyber sabotaža

Sabotaža predstavlja isplaniranu i namjernu akciju usmjerenu na slabljenje politike, državnog sistema ili organizacije, s ciljem njenog rušenja, poremećaja ili totalnog uništenja. Osoba koja se bavi sabotažom naziva se saboter. Najčešći oblici cyber sabotaže su oni koji djeluju destruktivno na operativno-informativne mehanizme i korisničke programe, prije svega, one koji imaju funkciju čuvanja podataka (Dragičević, 2004, str. 114). To se najčešće realizuje korištenjem standardnih uslužnih programa, sopstvenih programa ili korišćenjem tehnika kao što su logička bomba, trojanci, sporedna vrata ili virusi.

Sabotažom se postižu određeni ciljevi, najčešće političke prirode. Na taj način se namjerno ometaju procesi institucionalnog rada ili vojnog djelovanja i omogućava smjenjivanje ili preuzimanje kontrole nad njima. Najčešći primjeri sabotiranja su sprovedeni korištenjem botnet-ova za ostvarivanje DoS napada. Botnet mreža ili „zombi mreža“ je mreža koju čine zaraženi računari, a koji se još nazivaju botovi ili zombiji. Njima upravlja haker ili grupa hakera, a najčešće se koriste za DoS napade, krađu osobnih podataka i za slanje velike količine spam

poruka. Botom se naziva zaražen računar kao i virus koji je uzrok zaraze. Ovakve mreže nastaju da bi donijele korist i prednost hakerima koji stoje iza njih. One pružaju širok spektar opcija koje stoje hakerima na raspolaganju. Jako su popularne u hakerskim krugovima, te mnoge velike IT kompanije kao što je Microsoft, imaju posebne odjele koji se bave suzbijanjem razvoja ovih mreža. Botnet mreže nastaju tako što hakeri izrade virus odnosno bota kojim će zaraziti ostale računare kako bi ih povezali u jednu botnet mrežu. Odjel za sigurnost kompanije Microsoft je u saradnji sa partnerima kao što su Symantec, ESET i još nekoliko telekomunikacijskih kompanija, dana 12.10.2020. godine s Interneta isključio veliku ransomware botnet mrežu Trickbot. Ucjenjivački softver (engl. ransomware) je vrsta štetnog softvera koja korisniku uskraćuje pristup računarskim resursima i traži plaćanje otkupnine za uklanjanje postavljenih ograničenja. Neki oblici ransomwarea kriptiraju datoteke, a neki jednostavno zaključavaju sistem i prikazuju poruku koja korisnika nagovara na plaćanje otkupnine. Do sada je ova mreža bila jedna od najvećih malware operacija na svijetu koja je od kraja 2016. godine ransomwareom napala preko milijun računara.

Kada je prvi put zabilježena aktivnost Trickbota, njegovi su kreatori radili na unaprjeđenju načina distribucije zloćudnih programa, te ga pretvorili u modularno rješenje koje je nudilo i „usluge“ napada ransomwareom. Sigurnosne kompanije koje su radile na rušenju ove mreže pratile su i analizirale njezinu aktivnost i analizirale više od 125 tisuća primjeraka njezinih zloćudnih programa kako bi otkrile izvor cijele operacije. Nakon toga su dobili sudski nalog te u suradnji s telekomima iz više zemalja s Interneta isključili osnovnu infrastrukturu koja je služila za distribuciju. Proces širenja virusa se najčešće odvija na društvenim mrežama, raznim forumima, stranicama za preuzimanje raznih aplikacija gdje hakeri virus ubacuju u slike, druge programe i slično. Saboteri mogu imati različite motive, koji mogu biti političkog, ekonomskog, vojnog, službenog ili privatnog karaktera.

6.4. Cyber terorizam

Nakon dobro poznatog napada na Sjedinjene Američke Države, 11. Septembra 2011. godine, terorizam poprima sasvim drugo shvatanje, značenje i tretman za države i cjelokupnu svjetsku populaciju. Za američki FBI (The Federal Bureau of Investigation) terorizam je protuzakonita provedba sile protiv osoba ili imovine s ciljem zastrašivanja ili prisiljavanja vlade, civilnog stanovništva ili bilo koga unutar društva kako bi se unaprijedili vlastiti politički ili socijalni ciljevi. Iako danas u svijetu postoji nekoliko desetaka raznih definicija terorizma, najveći doprinos u pokušaju da pruži jedinstvenu definiciju dala je Europska Unija. U okvirnoj odluci Vijeća o borbi protiv terorizma iz 2002. godine, po prvi put se za sve države članice uvodi jedinstvena definicija pojma terorizam. Terorističkim činom smatra se svako namjerno djelo koje po svojoj prirodi ili kontekstu može ozbiljno naškoditi nekoj državi ili međunarodnoj organizaciji, a inkriminirano je u međunarodnom pravu i počinjeno s ciljem ozbiljnog zastrašivanja građanstva, prisiljavanja neke vlade ili međunarodne organizacije da nešto učini ili ne učini, ozbiljnog ugrožavanja ili uništavanja političkih, ustavnih, privrednih ili društvenih struktura neke države ili međunarodne organizacije, navodi se u Okvirnoj odluci Vijeća o borbi protiv terorizma, od 13. juna 2002. godine.

Sam pojam terorizma i njegova definicija donekle se mijenjala kroz historiju, ali najbliže tumačenje današnjeg poimanja terorizma jest ono po kojemu je terorizam ciljano organiziran kako bi se usmjerio na izazivanje straha s namjerom ostvarenja određenog političkog ili društvenog cilja. Temeljna sredstva terorizma u postizanju njegovih ciljeva su teži oblici nasilja, ubistva i teški zločini s tendencijom velikih razaranja i masovnog uništenja.

Historija terorizma polazi od drevnih vremena, kada su već tada suparnici nastojali na različite modalitete, od plašenja do fizičkog nasilja, deklasirati suparnike. Mogu se istaknuti primjeri terorizma i terorističkih djelovanja, terorističkih skupina tokom historije, a to su (Marić, 2012, str. 91):

1. Među prvim terorističkim skupinama, za koje se ističu klasificirani podaci djelovala je na Bliskom istoku čak daleko u prvom vijeku. Članovi i pripadnici te terorističke skupine nazivali su se Zeloti. Oni su bili židovski nacionalisti koji su se oduvijek borili protiv Rimske uprave postavljenom nad Judejom. Spomenuta skupina pojavila se čak unutar

šeste godine istog vijeka, te su vrlo ubrzo započeli provoditi terorističke aktivnost. Unutar Judeje imali su zacrtane ciljeve ubijanja i mučenja Rimljana i Židova koji su prihvaćali rimsku nadvlast. Kasnije su pored terorističkih aktivnosti vodili gerilske borbe i ratove u pustinjskim i brdskim područjima. Taj rat smatra terorističko-gerilski Zelota potrajao je sve do stvorene židovske pobune.

2. Tokom historije teroristi su težili provoditi aktivnosti prema politici, te su počinjenim zločinima htjeli prije svega srušiti vlast. U XI. vijeku na lokalitetu i području države Irana stvara se i okupira organizirana grupa Hashashini. Osim što su stvarali i koristili hašiš, bili su profesionalne i plaćene ubice. Djelovali su više od 200 godina i vodili se vjerskim učenjem. Težili su provoditi i raditi ubistva - atentate, učestalo uz samožrtvovanje. Za njih je karakteristično da su uveli mučeništvo. Indijske thuge bili su najduža teroristička skupina tokom historije, koja je djelovala čak šest ili sedam vijekova. Kao skupina mučili su i davili svoje žrtve, a sve žrtvovanjem Kaliju, koji je smatran indijskim bogom terora i uništenja, a Britanci su stali na kraj ovoj skupini te su ih uništili sredinom devetnaestog vijeka.

Terorizam je višeslojna pojava koja, ako se želi sagledati u cjelini, podrazumijeva interdisciplinarni pristup i usporedno istraživanje iz više područja. Uzroci otežanosti bavljenja tom društvenom pojavom su u tome što postoji niz raznih subjektivnih i objektivnih faktora koji usporavaju rješavanje složene problematike terorizma. Najčešće objektivni faktori su društveni odnosi i sukobi interesa te nepotpuno pravno regulisanje ove pojave, dok subjektivni faktori proizlaze iz politički uzrokovanog ponašanja zemalja na međunarodnoj osnovi koje nerijetko radi određenih interesa, eliminišu i provode kršenje međunarodne obaveze čije izvršavanje treba ispomoći u eliminisanju i suzbijanju terorizma.

Od pojave terorizma do danas, on je toliko osmišljen i teorijski oblikovan da je formulisana odgovarajuća doktrina s mnogim pravilima, postupcima i rutinama, tako da se može govoriti o terorizmu kao doktrini nasilnog djelovanja i o terorizmu kao praksi sistemskog nasilja u borbi za postizanje određenog (političkog) cilja (Talović, 2010, str. 71).

Savremeni terorizam javlja se kao blaža forma terorizma iz 90-ih godina. Postoji i javlja se u manjoj mjeri nego ranije, usmjeren je na dvije regije, a prema kategoriji, zadacima i primijenjenom oružju u napadima ne razlikuje se u velikoj mjeri od onoga koji se javljao u godinama ranije. Savremeni terorizam se odnosi na ogroman uzrok nesigurnosti modernog vremena. Svakako je terorizam postao svjetski fenomen. Naziva se savremeni iz razloga što danas postoji:

- veća pristupačnost informacija,
- bolja uvezanost ljudi kroz priopćavanje uz različite medije,
- nagli tehnološki progres,
- rast i jačanje industrije naoružanja.

Cyber terorizam podrazumijeva napade na kompjuterske sisteme ili mreže iza kojih stoje neki politički ciljevi. Često su namjenjeni za prepad vlade ili građana neke države ili izazivanje ekonomskih gubitaka. Pod cyber terorizmom podrazumijevaju se i fizički napadi i uništavanje važnih kompjuterskih sistema i infrastruktura. Postoje tri osnovna načina na koja teroristi mogu da koriste računare za koordinisanje, planiranje i izvršavanje svojih aktivnosti u ostvarivanju svojih ciljeva:

1. Korišćenje računara kao alata. Terorističke grupe koriste internet za propagiranje svojih ideja preko web sajtova i prikupljanje finansijskih sredstava, obično u vidu dobrotvornih priloga, kao i prikupljanje i razmjenu obaveštajnih podataka;
2. Teroristi mogu da koriste računare u planiranju i organizovanju svojih programa rada. Oni u računarima drže svoje finansijske knjige, terorističke planove, potencijalne ciljeve, dnevnike prismotre, planove napada i slično.
3. Cyber teroristi mogu da koriste računare za neovlašten pristup državnim i vladinim informacionim sistemima gdje te radnje najčešće rezultiraju velikim katastrofalnim posljedicama. Kako se računarska tehnologija razvijala, terorističke organizacije su također dobile priliku da putem Interneta izražavaju, razmjenjuju, i šire svoje ideje za ostvarivanje zajedničkih ciljeva. Putem Interneta i raznih sajtova regrutuju nove članove,

organizuju obuke i prikupljaju finansijska sredstva za ostvarivanje budućih terorističkih poduhvata.

Moderni terorizam se oslanja na psihološki rat kao sredstvo postizanja ciljeva, stvarajući paniku i strah među građanima. Teroristički napadi su često slučajni te nisu usmjereni na pojedinca, već na grupu koja dijeli zajedničke karakteristike i predstavljaju cilj neke organizacije ili državnog sistema. Pored klasičnog oružja postoje i ona savremenija koja podrazumijevaju primjenu razne hemijske, biološke, nuklearne i radiološke supstance koje klasificiraju i određuju mete i napade u skladu sa njihovim ciljevima. Nove terorističke organizacije, kao i njihova djelovanja, baš kao i političke stranke i njihove kampanje, temelje se na Internetu i globalnom umrežavanju. Napadi koji se organizuju i pokreću putem Interneta, čine osnovne dijelovi cyber kriminala. Učesnici u ovakvim radnjama su često mladi hakeri koji su željni eksperimentisanja sa sigurnosnim pitanjima i koji su zainteresovani za nove tehnologije. Teroristi prvenstveno imaju za cilj stvaranje panike i straha, stvaranje državne zabrinutosti, ekonomske nestabilnosti ili diskriminacije političkih protivnika. Kada su karakteristike terorista u pitanju, u literaturi postoji saglasnost da je u pitanju heterogena grupa, najčešće osobe muškog pola, različite vjerske i nacionalne pripadnosti, stepena obrazovanja i profesije. Procjenjuje se da je preko 95% terorističkih napada u svijetu planirano, organizovano i izvedeno od strane osoba muškog pola, dok su žene uglavnom zadužene za regrutovanje novih članova, održavanje kuća u kojima se skrivaju teroristi neposredno prije i nakon napada, poslove medicinskih sestara i slično.

Posljednjih godina vidljiv je sve veći broj cyber napada na političke mete, državnu infrastrukturu i web stranice komercijalnih korporacija. Te napade su počinile države, grupe hakera i kriminalne organizacije. Cyber teroristi su prvenstveno zainteresovani postizanje globalne medijske pažnje kojom će osigurati željeni uticaj na državne sisteme, destabilizaciju javnog života i stvaranje panike i straha kod građana.

Danas korištenje globalnih mreža omogućava jednostavnu i jeftinu komunikaciju između kompanija, vlada, država, pojedinaca i svih drugih zainteresovanih strana, te su vrlo dobro uspostavljene. Međutim, globalne mreže su omogućile zločine i terorističkа djelovanja.
Cyber terorizam kao koncept ima različite definicije, uglavnom zbog toga što stručnjaci sigurnosti ima svoju vlastitu definiciju. Taj se pojam može definirati kao korištenje informacijske tehnologije od strane terorističkih skupina ili pojedinaca kako bi ostvarili svoje ciljeve. To može uključivati korištenje informacijske tehnologije te poduzimanje napada protiv mreža, računarskih sistema i telekomunikacijskih infrastruktura, te obavljanje elektronske prijetnje. Kao i mnoge druge političke organizacije, terorističke grupe koriste Internet za sakupljanje novčanih fondova. Najčešće korištene metode finansiranja sastoje se od kanalisanja fondova koji proizlaze iz legalnih (donacije i privredne aktivnosti) ili nelegalnih aktivnosti (prevare pomoću kreditnih kartica, trgovine drogom i dijamantima), najčešće uz posredovanje legitimnih humanitarnih organizacija.

6.5. Cyber ratovanje

Društveni konflikti su jedna od najupečatljivijih karakteristika historije ljudskog roda. Oni su historijska ali i aktuelna konstanta ljudskih zajednica, te su kao takav fenomen od davnina privlačili pažnju teoretičara iz oblasti filozofije, historije, prava, psihologije, sociologije, vojnih i drugih nauka. Ratni sukob je svakako jedan od najekstremnijih oblika društvenih konflikata. Rat je kompleksan i intenzivan sukob koji može biti prouzrokovan klasnim, ekonomskim, političkim, rasnim i vjerskim neslaganjima. Rat predstavlja društvenu pojavu koja se može posmatrati sa različitih aspekata: historijskog, vojnog, etičkog, ekonomskog, političkog, itd. Međutim, potpuno razumijevanje ove pojave postaje ostvarivo jedino metodom multidisciplinarnog pristupa. Potreba za jačanjem vojne moći i sistema bezbjednosti primorava države da investiraju u naoružanje i vojnu opremu i da ulažu u druge oblike vojne potrošnje. Danas, kada se govori o poboljšanoj bezbjednosti u najvećem dijelu sveta i smanjenoj mogućnosti izbijanja rata velikih razmjera, vojni izdaci i dalje rastu. Za to postoje brojni razlozi a jedan od najznačajnijih je taj što u razvijenim državama vojna potrošnja ima značajan uticaj na razvoj.

Cyber ratovanje je podvrsta informacionog ratovanja koja se odvija unutar cyber prostora. Na cyber prostor može uticati bilo koja grupa ili organizacija koja posjeduje računare koji se mogu povezati u postojeće računarske mreže. Internet napadi neke grupe mogu biti usmjereni na namjerno ubacivanje dezinformacija na neke internet forume, enciklopedije, blogove i web stranice sličnog karaktera ili mogu biti strogo usmjereni prema mrežnoj sabotaži tj. Internet terorizmu.

Priroda cybe ratovanja je još uvijek nedovoljno ispitana i specifična. U cyber prostoru je gotovo nemoguće upratiti i otkriti identitet učesnika sukoba i njihove motive za takvim djelima. Samo u slučaju da je napad isprovocirao i započeo neki subjekat međunarodnog prava sa namjerom da pokrene agresiju nad drugim subjektom međunarodnog prava. Takva preduzeta akcija se može smatrati ratovanjem. U praksi, broj slučajeva cyber ratovanja je znatno manji od ukupnog broja cybet napada. Najveći broj takvih napada odnosi se na cyber kriminal i situacije u kojima je prekršen neki krivični zakon jedne države ili međunarodni zakon krivičnog prava.

Cyber ratovanje je vrsta neprijateljske aktivnosti preduzeta protiv računarskih mreža, računarskih sistema i baza podataka sa ciljem degradiranja ili uništavanja ciljanih sistema. Na taj način ciljani sistemi mogu biti neupotrebljivi, degradiranih performansi što može uticati na komandanta da donese lošu odluku usljed nedostatka informacija.

Cyber ratovanje se definiše i kao neovlašćeno upadanje vlade jedne države u računare ili mreže druge nacije, kao i preduzimanje drugih operacija i radnji koje utiču na računarski sistem, a sve u cilju dodavanja, izmjene i falsifikovanja podataka, kao i prouzrokovanje oštećenja računara, mrežnih uređaja ili objekata kontrole rada računarskih sistema.

Objekat cyber napada su informacioni resursi, odnosno njihov potencijalni cilj može da bude sve što povezuje, pokreće i održava informacioni sistem, vojni sistem, sistem državne

uprave, sistem za kontrolu kopnenog, plovnog, vazdušnog i željezničkog saobraćaja, sistem za snabdijevanje električnom energijom, plinom, vodom i slično. Nekada je cyber ratovanje podrazumijevalo samo međusobno prozivanje i provokacije sukobljenih država. Sa većom integracijom ključnih sistema za upravljanje (ekonomskih, političkih, vojnih,..) stvorili su se uslovi kakve danas imamo i za pravi cyber rat.

Metode cyber ratovanja su taktike, tehnike i koraci koje primjenjuju zaraćene strane, a oružja su ona sredstva ratovanja koja su napravljena, koriste se ili namjeravaju da se koriste u sukobu i koja su u mogućnosti da povrijede ili usmrte lica, kao i uništenje raznih javnih i privatnih objekata.

Cyber napadi se mogu razlikovati po cilju, intenzitetu, obimu, trajanju i efektima. Rizik od kolateralne štete raste sa ambicijom, vrstom i tehnikom napada. Iako se broj napada u cyber prostoru neprestano povećava, u većini slučajeva je gotovo nemoguće tehnički utvrditi njihovu pravu prirodu. Prilikom cyber kriminala, špijunaže i ratovanja, koriste se iste metode, tehnike i sredstva, a razlikuje ih jedino činjenica ko su napadači i da li postoji odgovornost države i vlade za napad. U praksi se također razlikuju i posljedice napada. Osim toga, svi slučajevi sukoba između subjekata međunarodnog prava ne predstavljaju stanje rata. S druge strane, rat može biti formalno proglašen od zvaničnih predstavnika država, ali to nije neophodan uslov da bi on postojao. Svakom ratu predhode razni oblici sukoba koji uglavnom nemaju status ratnih aktivnosti, ali imaju potencijal da eksliraju u ratne sukobe ukoliko se ne pronađe dogovor i rješenje. U slučaju kada se dogodi ratni sukob između zaraćenih strana, malo je vjerovatno da će se on voditi isključivo u formi cyber ratovanja.

Aktere cyber ratovanja možemo podijeliti u dvije različite kategorije. Kriterijum podjele jeste postojanje odnosno nepostojanje namjere kod počinioca računarskog upada. U tomjsmislu možemo praviti razliku između umišljajnog cyber napada, i napada bez umišljaja.

Umišljajni cyber napad koji se koristi u cyber ratovanju je svaki napad izvršen pomoću cyber sredstava sa ciljem da namjerno utiče na nacionalnu bezbjednost ili da stvori uslove za dalje operacije protiv nacionalne bezbjednosti. Umišljajni napadi se mogu izjednačiti sa ratovanjem - to je nacionalna politika na nivou ratovanja. Oni uključuju bilo koju radnju koja je izvršena protiv protivnikovog računara i informaciono-komunikacionih sistema.
Neumišljajni cyber napad izvode akteri, najčešće pojedinci, koji nenamjerno ugrožavaju nacionalnu bezbjednost i uglavnom nisu svjesni potencijalnih posljedica svojih napada na međunarodnom nivou. U ove aktere spadaju svi oni koji počine cyber infiltraciju, zaobilazeći odbrambene mehanizme sistema, te manipulišu, iskorištavaju ili uništavaju informacije sadržane u sistemu odnosno sam sistem. Ovi akteri imaju različite motive i namjere ali, u osnovi, ne namjeravaju da nanesu štetu nacionalnoj bezbjednosti ili daljim operacijama protiv nacionalne bezbjednosti. Važno je napomenuti da postoje slučajevi da ovom kategorijom aktera manipulišu oni akteri koji napade sprovode sa umišljajem, iskorišćavajući njihovo znanje i sposobnosti u cyber operacijama.

Svi pomenuti akteri koriste iste osnovne alate za izvršenje napada, kao što su računar, modem, telefon, i softver. Budući da su osnovni alati za izvršenje napada zajednički u cijelom spektru aktera cyber ratovanja, u praksi je teško identifikovati napadača. Broj Internet korisnika u budućnosti mogao bi biti mnogo veći od predviđenog. On bi mogao da premaši prikazane procjene usljed globalnog trenda u bežičnom pristupanju Internetu kao i pojeftinjenja računara i računarske
opreme na tržištu. To bi, svakako, povećalo rizik od cyber ratovanja.

Države imaju dužnost da spriječe cyber napade sa svoje teritorije protiv drugih država. Ova dužnost zapravo obuhvata nekoliko aktivnosti: donošenje strogih krivičnih zakona, sprovođenje energičnih istraga od strane kriminalističkih agencija, krivično gonjenje napadača i, tokom istražnog i krivičnog postupka, saradnja sa državom-žrtvom cyber napada. Ovo su dužnosti svih država i obavezujuće su u sklopu međunarodnog prava.

7. SIGURNOST U CYBER PROSTORU

Problemi koji nastaju iz kompjuterizacije društva počeli su još sedamdesetih godina prošlog vijeka da izazivaju zabrinutost vlada i odgovarajućih institucija, ali i nadnacionalnih subjekata međunarodnih odnosa. Prva među njima bila je vlada Švedske, koja je izradila studiju o opasnostima što ugrožavaju društvo zbog koncentracije i širenja kompjuterizovanih podataka i zbog prekograničnog toka takvih podataka. Studija pod naslovom „Ranjivost kompjuterizovanog društva“ završena je 1979. godine pod pokroviteljstvom Komiteta za osjetljivost računarskih sistema (Committee on the Vulnerability of Computer Systems) i izražavala je ozbiljnu zabrinutost u vezi sa razvojem kompjuterizovanih sistema i veličine njihovog uticaja na društvo. Zatim je u Španiji 1981. godine održano međunarodno savjetovanje u organizaciji španske vlade i Organizacije za ekonomsku saradnju i razvoj (OECD), a već 1982. godine u rješavanje ovog problema uključila se i Europska ekonomska zajednica (EEC). Komisija EEC je iste godine formirala grupu europskih naučnika sa zadatkom da izradi studiju o osetljivosti (ranjivosti) europskih društava.

U okviru Savjeta Europe (CoE) formiran je 1985. godine komitet koji se bavio pitanjima ugroženosti društva zbog automatizacije informacionih sistema. Jedan broj refleksija na kriminalitet u oblasti računarskih tehnologija takođe je bio razmatran i na sedmom Kongresu UN, održanom 1985. godine u Milanu. Tokom 1985. godine i u Norveškoj je izrađen izveštaj nazvan „Ranjivost društva zavisnog od računara“ (The Vulnerability of a Computer Dependent Society), u kojem je zaključeno da je „situacija vrlo ozbiljna“ sa stanovišta društvene i nacionalne bezbjednosti.

Cyber sigurnost je proces zaštite računara, servera, mobilnih uređaja, elektronskih sistema, mreža i podataka od zlonamjernih napada. Definiše se i kao sigurnost informacionih tehnologija ili elektronska sigurnost informacija. Generalna skupština Ujedinjenih Naroda je u

New Yorku, u 30. Januara (2004:58th sess.), zahtijeva da svi sudionici adresiraju sljedećih devet komplementarnih elementa:

1. Svijest. Sudionici bi trebali biti svjesni potrebe za sigurnošću informacijskih sistema i mreža i šta oni mogu učiniti kako bi se poboljšala sigurnost;
2. Odgovornost. Sudionici su odgovorni za sigurnost informacijskih sistema i mreža na način koji odgovara njihovim individualnim ulogama. Oni bi trebali redovito razmatrati svoje politike, prakse, mjere i postupke, te procijeniti jesu li oni prikladni za njihova okruženja;
3. Odgovor. Sudionici bi trebali djelovati pravovremeno i na kooperativan način kako bi spriječili, otkrili i reagirali na sigurnosne incidente. Oni bi trebali, po potrebi, dijeliti informacije o prijetnjama i ranjivostima, te implementirati procedure za brzu i učinkovitu suradnju kako bi se spriječilo, prepoznalo i reagiralo na sigurnosne incidente. To može podrazumijevati prekograničnu razmjenu informacija i suradnju;
4. Etika. S obzirom na sveprisutnost informacijskih sistema i mreža u modernim društvima, sudionici moraju poštivati legitimne interese drugih ljudi, prepoznajući da njihovo djelovanje ili nedjelovanje može naškoditi drugima;
5. Demokracija. Sigurnost treba provoditi u skladu s vrijednostima priznatim u demokratskim društvima, uključujući slobodu razmjene misli i ideja, slobodan protok informacija, povjerljivost informacija i komunikacija, odgovarajuću zaštitu osobnih podataka, otvorenost i transparentnost;
6. Procjena rizika. Svi sudionici trebaju provoditi periodične procjene rizika kojima se identificiraju prijetnje i ranjivosti. Procjene rizika trebaju biti dovoljno široko usmjerene kako bi obuhvatile ključne unutarnje i vanjske faktore, kao što su tehnologije, fizički i ljudski faktori, politike i treća strana pružanja usluga. Procjene rizika trebaju omogućiti određivanje prihvatljivog nivoa rizika, te pomoći u odabiru odgovarajućih kontrola za upravljanje rizikom od potencijalne štete informacijskim sistemima i mrežama u svjetlu prirode i važnosti informacija koje trebaju biti zaštićene;

7. Sigurnosni dizajn i provedba. Sudionici trebaju inkorporirati sigurnost kao neophodan element prilikom planiranja i dizajniranja, upravljanja i korištenja informacijskih sistema i mreža;
8. Upravljanje sigurnošću. Sudionici trebaju usvojiti sveobuhvatan pri-stup upravljanju sigurnošću temeljem procjene rizika koja je dinamična, te koja obuhvata sve nivoe aktivnosti sudionika i sve aspekte njihovog poslovanja;
9. Ponovna procjena. Sudionici bi trebali redovito pregledati i ponovno procjenjivati sigurnost informacijskih sistema i mreža, te poduzeti odgovarajuće izmjene u sigurnosnim politikama, praksama, mjera-ma i postupcima koji uključuju adresiranje novih i promjenu po-stojećih prijetnji i ranjivosti.

Savremeno društvo i političko uređenje države zahtijevaju određenu ravnotežu u svom djelovanju. Potreba zaštite državnog uređenja, s jedne strane, te poštivanje osnovnih ljudskih prava i sloboda građana, s druge strane, zahtijeva određenu ravnotežuo. U mnogim zemljama cyber sigurnost predstavlja relativno nov problem za učesnike iz oblasti sigurnosti, za demokratski nadzor, parlamentarni odbor i druga specijalizirna tijela, zbog konstantnog rasta i razvoja novih tehnologija, i nemogućnosti držanja koraka sa njima. Postoje brojni faktori koji pogoršavaju izazov demokratskog nadzora u vezi s mjerama cyber sigurnosti. Ženevski Centar za demokratsku kontrolu oružanih snaga (DCAF) identificirao je sljedeće izazove:

1. Problemi nadzora nastaju zbog kompleksnosti mreže. U cyber sigurnost uključen je veliki broj državnih, međunarodnih, privatnih i drugih nedržavnih učesnika. Kompleksnost mreže nadzornim tijelima, kao što su parlamentarni odbori (često s ograničenim ovlaštenjima), otežava da prate relevantne aktere, stiču saznanja o njihovom postojanju i aktivnostima.
2. Probleme nadzora pogoršava tehnička kompleksnost. Nadzorna tijela često nemaju neophodnu stručnost i kadrove koji bi mogli da ih razumiju i adekvatno nadziru.
3. Probleme nadzora pogoršava pravna kompleksnost. Cyber sigurnost nas suočava s kompleksnim pravnim pitanjima koja se odnose na pravo privatnosti i slobodu izražavanja. Još jedan problem predstavlja i činjenica da postoji napetost između zaštite

privatnosti i poboljšane identifikacije i provjere identiteta korisnika. Činjenica jeste da države i vladine institucije često bez adekvatnog demokratskog nadzora skupljaju i obrađuju veliku količinu ličnih i privatnih podataka radi vlastite sigurnosti.

4. Probleme nadzora pogoršava heterogenost aktera. U većini slučajeva institucije nadzora su organizirane kao agencije ili funkcionalno slična tijela. To rezultira velikim brojem područja u kojima nadzora ili nema ili je on neadekvatan za takvu ustanovu.
5. Probleme nadzora pogoršavaju percepcije mandata. Državna nadzorna tijela vode brigu o državnim agencijama za čiji rad su direktno odgovorne.
6. Probleme nadzora pogoršava narušavanje odnosa principal – agent. Postupci svakog državnog agenta povezani su lancem odgovornosti od principala ka agentu. Tako postoji lanac odgovornosti i nadzora između demokratskih institucija (poput parlamenta) i pojedinaca ili agencija koje provode državne direktive. Ove veze prekinute su uvođenjem privatnih aktera i stvaranjem javno-privatnih mehanizama saradnje. Ovakav odnos je mnogo složeniji i nejasniji zbog velikog broja asimetričnih informacija koje smanjuju transparentnost i sprječavaju efikasno djelovanje nadzornih organa.

Izvršioci krivičnih djela cyber kriminala su ne samo eksperti već i veliki broj lica kojima su računari danas dostupni. Najopasnije su organizovane kriminalne grupe koje angažuju najbolje eksperte za izvršenje cyber krivičnih djela. Nadležni organi prvo preduzimaju preventivne mjere za sprjčavanje i suzbijanju čestih oblika cyber kriminala, kao što su posebni kodovi i šifre. Također, potrebno je prepoznati, locirati i prikupiti sve materijale i dokaze o krivičnim djelima i njihovim učesnicima cyber kriminalu, a zatim ih i procesuirati pred nadležnim sudovima. Angažman Misije OSCE-a u Bosni i Hercegovini po pitanju cyber sigurnosti usmjeren je na unaprijeđenje kapaciteta BiH da adekvatno i učinkovito odgovori na prijetnje koje proizlaze iz cyber prostora. Ovaj angažman uključuje podršku razvoju usaglašenog strateškog okvira za cyber sigurnost, uspostavljanje timova za reagovanje u urgentnim situacijama i izgradnju i obuku svih kapaciteta za borbu protiv cyber kriminala.

Provođenje mjera zaštite cyber sigurnosti ne smije ugroziti privatnost građana koja predstavlja osnovno ljudsko pravo i slobodu. Svi građani imaju pravo na privatnost i zaštitu ličnih podataka. Bosna i Hercegovina treba da poveća broj stručnjaka iz cyber sigurnosti, ako se želi uspješno zaštititi od cyber opasnosti. Da bi se to postiglo potrebno je uvesti specijalističke studije iz ove oblasti u škole i univerzitete. Osim toga, potrebno je uvesti redovno stručno usavršavanje svih osoba nadležnih za tehničke aspekte sigurnosti informacija u svim institucijama na svim nivoima. Posebne obuke koje provode proizvođači za rad sa opremom i softverom, a koji se koriste u nekoj instituciji, treba da budu obavezne za službenike koji rade sa njima. Uz obrazovanje profesionalaca cyber sigurnosti potrebno je podići nivo znanja iz ove oblasti među građanstvom. To je proces koji treba provoditi kroz cjelokupno obrazovanje od osnovne škole do fakulteta. Na ovaj način se podiže ukupni nivo znanja i sigurnosti cijelog društva.

Danas više niko ne dovodi u pitanje činjenicu da mnoge države razvijaju ofanzivne strategije cyber ratovanja. Osim njih, i civilni sektor se dokazao u zloupotrebi informacionih tehnologija. Broj informatičkih napada na globalnom nivou svakodnevno se povećava kao i obim štete uzrokovane napadima. Zbog toga pitanja kontrole, prevencije i suprotstavljanja cyber napadima predstavljaju neke od akutnih bezbjednosnih izazova, kako na nacionalnom i subnacionalnom nivou tako i na regionalnom i gobalnom nivou. Svi kapaciteti zaštite, bilo da se radi o fizičkim ili tehničkim kapacitetima, predstavljaju prvu liniju odbrane informacionih sistema od cyber napada. Prilikom planiranja i usavršavanja fizičkog kapacitea obezbjeđenja, koristi se nekoliko metoda. Kontrola pristupa je termin koji se koristi kada se govori o mehanizmu koji reguliše pristup računarima, softveru i drugim resursima. Serveri koji čuvaju važne podatke, ruteri i druge bitne mrežne komponente trebalo bi da se nalaze u zaključanim ormanima, ili obezbjeđenim računarskim centrima. Dobro obezbjeđenje servisnog centar predstavlja fizičku prepreku za svaku osobu koja nije ovlaštena da pristupi serveru.

Bežično umrežavanje je pored eksplozije umreženih sistema, donijelo i nove bezbjednosne izazove. Lokacija je jedan od glavnih faktora koji utiču na bezbjednost bežičnih

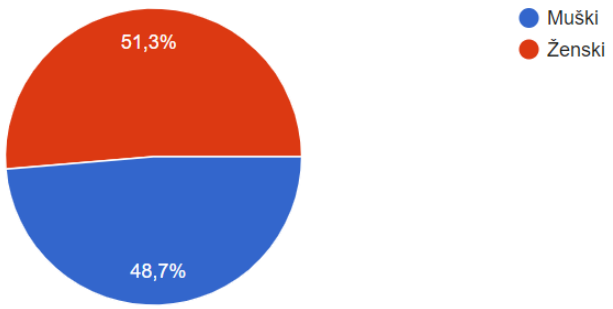
komunikacija. Kada se biraju i instaliraju komponente za bežično umrežavanje, a posebno tačke pristupa, treba ih pažljivo testirati i utvrditi operativni obim uređaja. U slučajevima kada se prenose poverljivi podaci, potrebno je da se snaga prenosa svih bežičnih uređaja obavlja na minimumu koji dozvoljava efikasno obavljanje operacija, tako da je potencijalnim špijunima van zgrade otežano povezivanje na mrežu i prisluškivanje. Drugi faktor koji može uticati na podizanje bezbjednosti bežičnih mreža jeste zaklanjanje operativnog područja. Mreža se na takav način štiti od DoS napada, koji predstavljaju najveću prijetnju za nju. Antena bi trebalo da bude postavljena u centar zgrade, što dalje od spoljašnjih zidova.

Mobilne komunikacije i tehnologija koja konstanto raste i napreduje, također ima i neograničen domet pa mnogi prenosni uređaji omogućavaju da se povežu sa mrežom koja se nalazi bilo gdje u svijetu. Za povezivanje laptopa sa mrežom se koristi Bluetooth, koji povezuje urešaje kratkog dometa a može se koristiti i mreža mobilnog provajdera Internet usluga. Zbog toga, opasnost je daleko veća jer nije potrebno da haker bude u blizini mrežnih instalacija da bi dobio pristup podacima i resursima.

8. REZULTATI ISTRAŽIVANJA

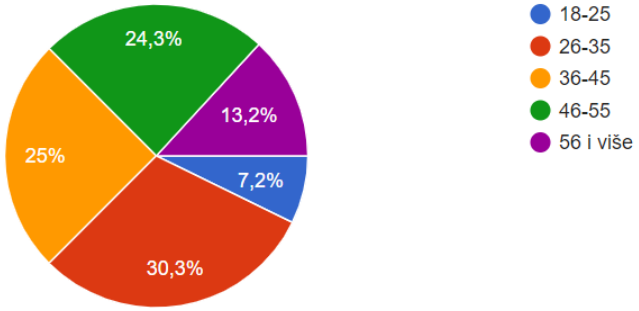
Od tehnika istraživanja koristila sam anketu (obrazac google online) kako bih dobila stavove ispitanika o ulozi Interneta i društvenih mreža u promociji i prezentaciji političkih stranaka, i njenih kandidata i njihovih djelovanja i akcija. Anketa sadrži osam pitanja, gdje su prva dva opća pitanja o spolu i starosnoj dobi. Anketa je dijeljena putem društvene mreže Facebook i putem e-maila. Popunilo ju je 100 ispitanika. S obzirom na njen kratak upitnik, smatram da su ispitanici odgovorili pouzdano i iskreno. U nastavku ću predstaviti rezultate istraživanja kroz grafički prikaz.

Pitanje br. 1.: Koji ste spol?



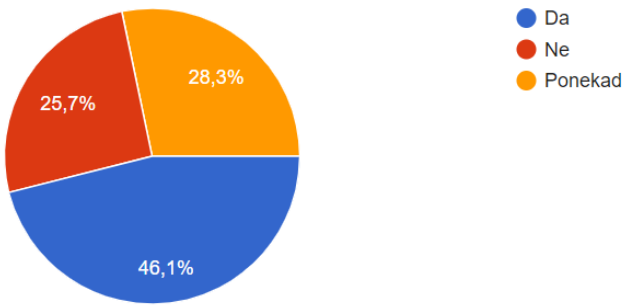
Prvo pitanje se odnosilo na spol ispitanika, gdje možemo vidjeti da je podijeljena spolna struktura anketnih ispitanika. Muškarci sa 51,30% i žene sa 48,70% učešća.

Pitanje br. 2.: Koliko imate godina?



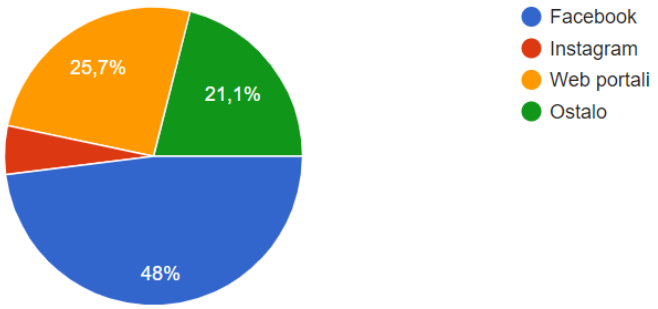
Drugo opće pitanje jeste o starosnoj dobi ispitanika, gdje su ponuđeni odgovori bili u rasponima po starosnim skupinama. Tri dobne skupine su većinskim dijelom učestvovale u odgovorima na anketu. Možemo reći da je i samo istraživanje većinskim dijelom bilo upućeno onoj starosnoj skupini u kojoj se i sama nalazim, a to je od 26 do 35 godina.

Pitanje br. 3.: Pratite li određene stranke na društvenim mrežama?



Treće pitanje se odnosilo na praćenje političkih stranaka putem društvenih medija, gdje su nam krajnji rezultati pokazali da Internet i prostor kojim raspolažemo na njemu, pa tako i društvene mreže koje služe i kao kanal komunikacije, u današnjem vremenu predstavljaju veoma bitnu platformu za oglašavanje političkih stranaka i njihovih aktivnosti i ciljeva. Vrijeme koje danas provodimo ispred računara jeste paralelno onom vremenu prije pojave interneta Interneta, gdje smo svoje vrijeme i potrebu za informacijama zadovoljavali ispred TV ekrana prateći njegov sadržaj i slušajući radio prijemnike.

Pitanje br. 4.: Na kojoj društvenoj mreži najčešće pratite političke kandidate i stranke?



Četvrto pitanje je glasilo putem kojih društvenih mreža ispitanici prate političke stranke i kandidate. Vidimo da je odgovor kod većine ispitanika bio društvena mreža Facebook. Društvene mreže postale su relevantan izvor informacija i predizbornih poruka kako za građane tako i za medije, budući da su brojni političari izjave prvo objavljivali na društvenim mrežama, a tek onda na drugim kanalima. Sve veći broj korisnika društvenih mreža ostavio je trag na političku komunikaciju. Društvene mreže poput Facebooka postale su idealan kanal putem kojeg se mogu privući novi birači, zadržati oni stari te ih potaknuti na političku participaciju na mrežnim platformama u korist stranke. Veoma je bitno napomenuti da je korištenje društvenih mreža potpuno besplatno, a ukoliko želimo da naši oglasi budu u svakom momentu dostupni javnosti, moguće je platiti oglase i tako biti siguran da se oni prezentuju svakodnevno i po nekoliko puta na dan. Servisi društvenih medija su također kreirani da budu veoma jednostavni za korištenje i pružaju pun korisnički komfor. Neke od prednosti Facebooka su:

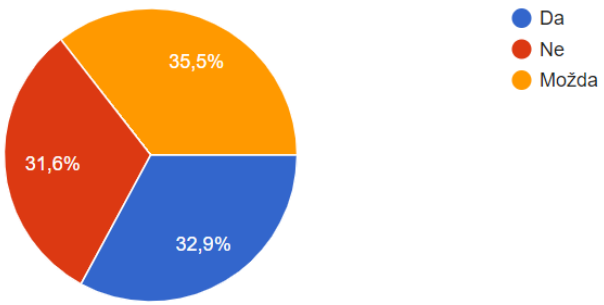
- besplatan pristup i neograničene mogućnosti povezivanja sa drugima,
- kreirajući profil korisnici stiču nove prijatelje, ali i povezuju i sa onim osobama sa kojima su izgubili kontakt
- razmjena informacija, ideja i mogućnosti u privatnom i profesionalnom svijetu putem online platformi, odnosno, žargonski rečeno, od kuće.

Shodno prednostima, izdvojili bi i, po nama, dva najznačajnija nedostatka korištenja Facebooka:

- opasnosti od zloupotrebe i krađe identiteta,

- nemogućnost potpune zaštite privatnosti, jer kompanija Facebook zadržava naše lične podatke, te ih može prosljeđivati agencijama i organizacijama koje za njih iskažu interesovanje i potrebu.

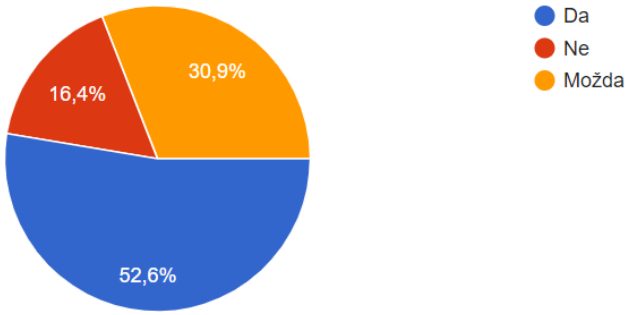
Pitanje br. 5.: Da li objave političkih stranaka na društvenim mrežama utiču na Vašu odluku prilikom glasnja na izborima?



Sljedeće, odnosno peto pitanje se odnosilo na to da li objave političkih stranaka i kandidata na društvenim mrežama mogu uticati na njihovo glasanje prilikom izbora. Odgovori su podijeljeni, ali ako uzmemo neutralan odgovor „Možda“ kao većinskim dijelom da je potvrdan, što su rezultati ankete do sada pokazali, onda ćemo reći da je i većinski odgovor na ovo pitanje, potvrdan. Sadržaj na društvenim mrežama je veoma transparentan i pristupačan svim korisnicima. Političke stranke i njihovi kandidati više nisu nedodirljivi. Putem društvene mreže možemo komunicirati sa njima i pratiti njihov rad i aktivnosti. Sljedeća činjenica jeste mogućnost jednostavne komunikacije među članovima stranke. Korisničke mogućnosti se manifestuju u tome što građani sada mogu da reaguju na sadržaj, odnosno, da iznesu svoje mišljenje i daju komentare.

Društvene mreže i mediji predstavljaju najnoviji trend u savremenom političkom komuniciranju i u velikoj mjeri mijenjaju način na koji stranke i kandidati predstavljaju sebe javnosti. Razna istraživanja pokazuju da korisnici četvrtinu svog vremena provedenog na internetu provedu na društvenim mrežama i raznim portalima.

Pitanje br. 6.: Smatrate li da su društvene mreže i stranice određenih političkih stranaka preduslov za uspješnu komunikaciju sa potencijalnim biračima?



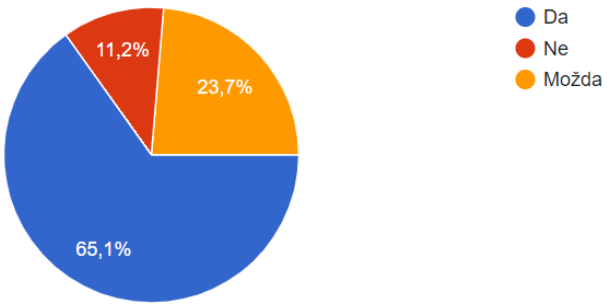
Na šesto pitanje koje je glasilo „Smatrate li da su društvene mreže i stranice određenih političkih stranaka preduslov za uspješnu komunikaciju sa potencijalnim biračima?“, od tri ponuđena odgovora da, ne i možda, ubjedljivo je potvrdan odgovor, sa 52,6%. Sagleda li se politička komunikacija putem društvenih mreža kroz kriterij transparentnosti, koristi i učinkovitosti, mišljenja su da ista mogu pridonijeti boljem rezultatu na izborima. Čovjek kao online aktivan potencijalni birač, od političkih stranaka na društvenim mrežama očekuje sadržaje koji imaju neku vrijednost za njega kao pratioca, a ne za članove stranke, te one sadržaje koji ukazuju na istinski interes i plan za napredak države, ekonomije i ljudi. Također, građani bi željeli biti uključeni u komunikaciju kada oni postavljaju pitanja, a ne onda kada su kandidati i predstavnici stranaka raspoložene ponuditi odgovore. Deset pravila dobre komunikacije:

1. Obezbijediti slaganje. Ljude nije moguće ubijediti, oni će se samo složiti sa nečim u šta već vjeruju;
2. Stalno preuzimati inicijativu;
3. Stalna dvosmjerna komunikacija sa javnošću;
4. Izgled je važan. Prilikom komunikacije, nije važno samo šta se kaže, već i kako se to kaže;
5. Djela su ubjedljivija od riječi. Ljudi treba da vide neku akciju, a ne da slušaju samo obećanja;

6. Pažljivo odabrati osobu koja će prenositi poruke;
7. Formulisati glavnu temu;
8. Biti i izvor i sredstvo informacija;
9. Osmisliti nove načine korištenja medija;
10. Postupci se moraju poklapati sa slikom kojom se stranke predstavljaju javnosti.

Komunikacija sa potencijalnim biračima putem društvenih mreža posebno odgovara manjim strankama jer ih stavlja u ravnopravan položaj sa strankama iza kojih stoje veliki igrači i ogromne količine novca. Ta ravnopravnost prilikom oglašavanja je dobra i iz razloga tog što često manje političke stranke pokazuju veću efikasnost pri prezentovanju svojih ideja i ciljeva.

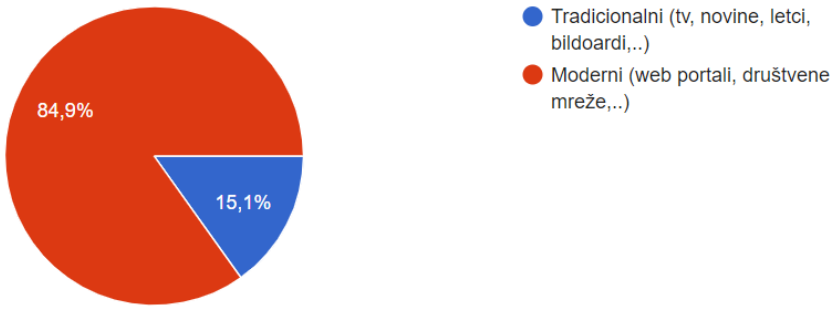
Pitanje br. 7.: Smatrate li da komuniciranje političkih stranaka sa širom narodnom masom putem društvenih mreža predstavlja dobru političku kampanju?



Ako stranke i kandidati iskoriste potencijal društvenih mreža za adekvatnu promociju ciljeva i aktivnosti, te za dvosmjernu komunikaciju sa potencijalnim i postojećm biračima, uspjeh same političke stranke i njene kampanje je zagarantovan time što su se predstavili javnosti i iznijeli jasne planove daljeg djelovanja. Grafički prikaz odgovora na sedmo pitanje nam to i potvrđuje. Ispitanici se u velikom broju odgovorili potvrdno na pitanje da li komunikacija stranaka sa javnošću doprinosi dobroj političkoj kampanji. Izrada plana komunikacije, tačnije plana za prenošenje poruka koje treba da budu saopštene u izbornoj kampanji, prvi je i osnovni korak za uspješno komuniciranje sa javnošću što podrazumijeva dobru političku kampanju.

Neposredno pred same izbore, tačnije, 24 sata prije istih, vlada izborno zatišje i zabranjena je komunikacija između političkih stranaka sa jedne, i birača sa druge strane. Zbog toga novi mediji, a prije svega društvene mreže, omogućavaju da se ova šutnja prekine. Putem novih medija mogu imati kontinuiranu komunikaciju sa svojim biračima, ali i sa svim drugim zainteresovanim građanima, ali ne preko oficijelne stranice ili profila stranke, već kao pojedinac, sa ličnim profilom i u svoje ime. Ovo možda ne predstavlja za stranku veliki korak, ali kandidati koji su kandidovani na izborima, mogu to iskoristiti u svoju korist. Naime, Centralna izborna komisija BiH je 2020. godine prvi put uvela praksu kažnjavanja stranaka koje su koristile oglašavanje na internetu prije službenog početka izborne kampanje, kao i za vrijeme izborne šutnje. Ovo je praksa većine zemalja svijeta, u zavisnosti od same regulative izbornog procesa te zemlje.

Pitanje br. 8.: Koji način oglašavanja političkih stranaka je po Vašem mišljenju efikasniji?



U prošlosti su se političke stranke uglavnom fokusirale na oglašavanje putem televizije i na taj način prenosile poruke široj javnosti. Međutim, znamo da je oglašavanje putem ovog medija skupo jer podrazumijeva plaćanje produkcije, organizaciju grupe kandidata u smislu šminke, dnevnica i gardarobe koju će nositi tokom promotivnog oglasa, a tek na kraju i najveći zalogaj u smislu finansijskog izdatka, kada je zakup oglasnog prostora kod određene televizijske kuće u pitanju. Internet se u poređenju s televizijskim, radijskim i novinskim oglašavanjem pokazao kao

najjeftiniji oglasni prostor, pa možemo reći da danas spada u vodeće informativno tijelo. To posebno vrijedi kod mlađe populacije koja više od polovine svog slobodnog vremena provedu ispred računara, konkretno, na društvenim mrežama kao što je Facebook. Danas bez interneta stranka ne može pobijediti na izborima. Posebno za mlade, Internet je posljednjih godina postao medij broj jedan i nadmašio je televiziju i dnevne novine. Uz to, blogovi i društvene mreže postaju sve važniji za političku kulturu jer omogućuju dvosmjernu komunikaciju između građana i političara.

Ipak, staromodni način političke kampanje nije potpuno nestao. Politički kandidati i dalje uključuju televizijske oglase i izborne plakate u svojoj strategiji promocije kampanje, ali im se ujedno povećava i broj oglasa objavljenih na Facebook ili Instagram stranicama, kao i YouTube kanalima i ostalim društvenim medijima.

Reklame u novinama, vizit karte, posteri, tv i radio reklame, billboard i slično su oblici tradicionalnog oglašavanja. Ljudi još uvijek vjeruju klasičnom marketingu jer je prisutan mnogo godina – lakše ga razumiju, upoznati su kako funkcionira i više mu vjeruju. Nemaju vremena ni volje naučiti nešto novo ili analizirati podatke do kraja da bi digitalno oglašavanje imalo smisla. Ovoj grupi uglavnom pripada starija populacija stanovništva, ali na žalost, kada je Bosna i Hercegovina u pitanju i izborni proces, upravo starija populacija i izlazi na iste da da svoj glas. Odaziv mlađe populacije je sramotno mali, što našu zemlju i dugogodišnju situaciju u kojoj se nalazimo, stavlja u sramotan položaj.

Prisustvo u medijima jedna je od bitnih pretpostavki da stranke i njihovi kandidati uđu u svijest birača, jer mediji, u prvom redu televizija i društvene mreže, predstavljaju najvažniji, a često i jedini izvor informacija pomoću kojeg se formira mišljenje potencijalnih i stalnih birača. Svi znamo da su televizijske reklame iznimno skupe i reklamiraju se samo velike kompanije koje imaju budžet za taj segment. Ograničenja koja tradicionalni mediji pružaju su najveća mana ovakvog načina promocije. Neka od njih su: nemjerljivi rezultati, nije dostupan svima, tv reklama je iznimno skupa.

9. ZAKLJUČAK

Na samom kraju istraživačkog rada, ostaje nam još generalni osvrt i analiza onoga što smo pisali i dobili putem istraživanja. Nakon uvodnih razmatranja i metodološkog dijela, prva izlaganja smo posvetili samom fenomenu nastanka i ekspanzije novih medija, politički marketing i političko komuniciranje u uslovima novih trendova, a posebno nove i tehnologije koja napreduje iz dana u dan. Internet je povećao mogućnost prenošenja informacija većem auditoriju za puno kraće vrijeme nego što se to radilo putem tradicionalnih vidova oglašavanja kao što su štampa, televizija, radijo i slično.

Novi mediji, globalno umrežavanje ljudi, dostupnost i količina informacija na Internetu, odnosno cyber prostor predstavlja izazov pred strankama i članovima, jer sam taj virtuelni prostor još uvijek za naše političare predstavlja nedovoljno istražena područja. Cyber prostor možemo predstaviti kao sve više zamjenski prostor u kome se odvija širok spektar aktivnosti iz naših života. U protekloj godini smo svjedočili o veličini i moći cyber prostora. U njega su premješteni svi komunikacijski kanali, cjelokupni obrazovni sistemi, radna okruženja, prodaja, kupovina, društvena događanja, kao i muzički, filmski i pozorišni festivali. Cyber prostor je postao središte svih zbivanja, pa o njegovoj veličini, mogućnostima, ali i prijetnjama, uvijek se može diskutovati.

Nagli razvoj informacione tehnologije doveo je mnoge naučnike, stručnjake i analitičare iz ove oblasti, u situaciju gdje istraživanja koja sprovode, ne mogu stići dati odgovore a da se već neka druga inovacija ne dogodi. Drugim riječima, teško je držati korak sa fenomenom zvanim tehnologija. Ono što novo u odnosu na desetak godina iza nas, jeste razvoj Interneta i masovnih medija. Mediji poput televizije, radija i dnevne štampe su danas postali nezamislivi bez svoje digitalne verzije i prisutnosti u obliku Web stranica, ili stranica na društvenim mrežama. Razvojem i ekspanzijom društvenih mreža, političke stranke imaju mogućnost biranja društvene

mreže na kojoj žele da se oglašavaju i putem koje žele da se odvija njihova spoljna komunikacija. Sve političke stranke danas koriste internet za prenošenje informacija o izbornom procesu, kandidatima i radnjama koje namjeravaju preduzet u slučaju pobjede na izborima.

Društvene mreže su postale sastavni dio svakog pojedinca, te jak instrument u komunikaciji, promociji i informisanju politike i političkog angažmana. Oglašavanje usmjereno na društvene mreže i oglasne mogućnosti koje one pružaju, predstavlja posebnu tehniku internetskog oglašavanja. Razvojem društvenim mreža te rastom broja korisnika, jačao je i interes političkih subjekata za primjenu društvenih mreža u marketinškim aktivnostima. Ko želi da nešto postigne u politici i društvu, mora da poznaje pravila komunikacije i upotrebe novih medija. Političke stranke predstavljaju bitnog aktera političkog sistema. One su glavna spona između građana i države. Danas skoro da i nema političke stranke ili kandidata koji u svojoj kampanji se ne služi Internetom i potencijalima i prilikama koje on pruža kao kanal oglašavanja i promocije svojih ciljeva, akcija i djelovanja. Internet je povećao mogućnost prenošenja informacija većoj ciljanoj skupini za puno kraće vrijeme nego što se to radilo putem štampe, televizije, radija, plakata i letaka. Sve političke stranke danas koriste internet za prenošenje informacija o izbornom procesu, kandidatima i akcijama koje namjeravaju preduzet u slučaju pobjede na izborima. Direktna i dvosmjerna komunikacija u cyber prostoru danas je uobičajena između političkih stranaka i birača u razvijenim zemljama svijeta. Mnoge političke stranke i njihove akcije su danas dostupne široj javnosti putem stranica na kojima se oglašavaju, kao što su društvene mreže, te se putem njih može doći do onih informacija koje prije nisu bile dostupne. Internet pruža globalni prostor za komunikaciju, gdje se svaka osoba može informisati o političkoj, socijalnoj, ekonomskoj, i drugoj situaciji koja se tiče direktno svakog pojedinca.

O političkim sposobnostima i aktivnostima kandidata, o planovima i ciljevima stranaka, birači mogu da čuju isključivo putem medija, bilo da se radi o tradicionalnim (televizija, radijo, dnevna štampa,..) ili modernim medijima (web portal, društvene mreže,...), koji su posljednih godina znatno više zastupljeni. Upravo iz tog razloga, i sama politika i politički sistem kao bitna karika održivosti i razvoja, trebaju da se okrenu i prilagode novim trendovima i napretku informacione tehnologije. U samo par godina, ekspanzija društvenih mreža je dovela do toga da

su se predizborne kampanje i politička oglašavanja koja su se vodila putem televizije, radija, i plakata, orijentisala na vid oglašavanja i promocije putem ovog novog medija. Ako stranke i kandidati iskoriste potencijal koje novi mediji pružaju, zagarantavano će i njihovi rezultati na izbrima biti znatnoInternet pridonosi boljim rezultatima na izborima samo ako stranke i kandidati iskoriste njezin potencijal za dvosmjernu komunikaciju. Ukoliko za komunikaciju sa svojim članovima i biračima koriste nove društvene medije kao što su društvene mreže, ostvarit će bolju stranačku poziciju, a time i veći broj glasova na izborima. Dobro isplanirane političke aktivnosti, uspješna i adekvatna organizacija, mogu da olakšaju izbornu pobjedu, čak i onim strankama koje nemaju veliku finansijsku moć.

Zaključno sa ovim dijelom, potvrđujemo i glavnu hipotezu istraživačkog rada koja glasi: „Cyber prostor pruža veliki broj prednosti upravljanja političkim pitanjima, adekvatne kulture unutar političke stranke, ali donosi i određeni broj nedostataka i prijetnji. Internet predstavlja moderni kanal komunikacije kojim je moguće unaprijediti već postignute rezultate, ali ujedno i pruža mogućnost manjim strankama da steknu ista ili približna promotivna dejstva. Putem interneta veliki auditorij je u prilici da vidi promotivne poruke političkih stranaka, neovisno o broju njenih kandidata, kao i finansijskoj potpori koja stoji iza iste“.

Specifičnosti cyber prostora i informacionih tehnologija čine da se se državni i individualni akteri nalaze u istim ravnima djelovanja, a činjenica da se ista sredstva, tehnike i metode često primjenjuju za kriminalne, terorističke, obavještajne i ratne aktivnosti. Posljedica toga jeste da u oblasti cyber sugurnosti trenutno vlada nedostatak općeprihvaćenog referentnog sistema vrijednosti, čak i u pogledu osnovnih pojmova i koncepata, na nacionalnom i međunarodnom nivou. To može imati ozbiljne posljedice ako se ima na umu činjenica da su vodeće sile svijeta u svojim vojnim doktrinama za cyber ratovanje predvidile mogućnost vojnog odgovora fizičkom silom na cyber napad u zavisnosti od posljedica koje taj napad izazove. Tu okolnost dodatno komplikuje i otežava činjenica da pasivna odbrana od cyber napada ne može biti dovoljna za odbranu, jer nema moć, kao ni mogućnosti sprječavanja napada, već isključivo ublažavanja i minimiziranja njihovog efekta i učestalosti, zbog čega uglavnom razvijene državne

doktrine stavljaju naglasak na aktivnu, promišljeni i preventivnu odbranu i odvraćanje. To se u praksi skoro u potpunosti eliminiše i ne pravi razliku između odbrane, napada i obaveštajnih aktivnosti.

Na žalost, u Bosni i Hercegovini političari još uvijek u jako malom broju koriste mogućnosti za komuniciranje koje pružaju društvene mreže. Političke stranke se promovišu po principima ekonomskog marketinga jer političke stranke i kandidati ne reprezentuju interese građana već svoje lične interese, koje kao takve nude svojim biračima. U političkim kampanjama nema prezentacije bitnih sadržaja djelovanja, kao i onoga što je stvarni interes građana, nego se govori o beznačajnim stvarima. Stranke i kandidati žele imati kvalitetnu komunikaciju s javnošću i potencijalnim biračima, ali ne uspijevaju sve u tome. Internet kao novi medij sve je važniji u predstavljanju političara koji na taj način dokazuju svoju savremenost, napredak u komunikaciji i želju da se približe građanima. Jednostavnost korištenja i veliki broj mogućnosti koji pružaju društvene mreže mnogi kandidati su iskoristili kako bi se biračima i javnosti predstavili ne samo kao političari, već i kao porodični ljudi koji drže do određenih moralnih vrijednosti. Međutim, kada su u pitanju angažovanja pojedinaca u cyber prostoru u smislu online oglasnih poruka, komunikacije sa biračima i javnošću, svakodnevno slanje poruka upućenim biračima, moramo reći da naši političari idu nekoliko koraka iza prosječnog političara neke druge zemlje. Razlog tome jeste i činjenica da se već dugi niz godina stanje u Bosni i Hercegovini, kada je u pitanju vlast, ne mijenja. Možemo reći da vlada monopolistički režim kada je upravljanje ovom državom u pitanju. Da li potencijalni kandidati različitih stranaka ulaze u izbornu borbu sa već jasnim rezultatima istih, ili neobrazovanje i nekultura doprinose tome da se ne prezentuju građanima na način prihvatljiv za jedno savremeno demokratsko društvo. Većina ih se vodi ličnom korišću, kao što je radno mjesto koje mogu obezbjediti samim članstvom u neku određenu stranku, a zatim i kandidaturom na izborima, smatraju kao svoju ličnu promociju. Većina građana Bosne i Hercegovine nije zadovoljna radom i uslugama koje im pruža vlada, odnosno vladajuća stranka. Politička dominacija i učešće u vlasti u našoj zemlji se nije mijenjala godinama, sa istim nacionalnim strankama koje pobjeđuju na izborima i relativno niskoj

izlaznosti glasača. Možemo reći da se naziru promjene od prošlogodišnjih lokalnih izbora, ali dok se taj trend ne poonovi makar nekoliko puta, ne smijemo iznositi takve tvrdnje.

10. LITERATURA

1. Anić, V.; Goldstein, I. (2004): Rječnik stranih riječi, Zagreb, Algoritam
2. Baines, P.R., Egan, J.(2001): Marketing and political campaigning: mutually exclusive or exclusively mutual?, Qualitative Market Research: An International Journal, Vol. 4, No. 1
3. Berčić, B. (2012): Filozofija, Zagreb, Ibis
4. Blumer, J. G., Kavanagh, D. (1999): The Third Age of Political Communication: Influences and Features, Political Communication, vol. 16
5. Čekić, E. (2019): Uloga psihologije i unapređenje cyber sigurnosti, Kriminalističke teme, Broj 5, Sarajevo, Zbornik radova
6. Čukić, B. (2005): Organizaciono ponašanje u ulogama i grupama, Kruševac, ICM+
7. Dragičević D.,(2004): Kompjuterski kriminalitet i informacijski sustav, Zagreb, IBS
8. Fejzić, F. (2004): Medijska globalizacija svijeta, Proocult, Sarajevo, GIK „Oko“
9. Franceško, M. (2003): Kako unaprijediti menadžment u preduzeću, psihologija i menadžment, Novi Sad, Prometej
10. Jurković, Z., Marošević, K. (2013): Utjecaj informacijske tehnologije na poslovnu komunikaciju, Sveučilište J. J. Strossmayera, Osijek, Pravni fakultet Osijek
11. Grbeša, M. i Lalić, D. (2003): Osnove političke komunikacije /skripta/, Zagreb, Fakultet političkih znanosti
12. Labaš, D. (2009): Međuljudska komunikacija, novi mediji i etika; Novi mediji – nove tehnologije – novi moral, Zagreb, Hrvatski studiji Sveučilišta u Zagrebu
13. Lewis, J. A. (2006): Cybersecurity and Critical Infrastructure Protection, Washington, DC: Center for Strategic and International Studies

14. Marić, S. (2012): Terorizam kao globalni problem, Vol. 6, Medianali
15. Panian, Ž. (2000): Internet i malo poduzetništvo, Zagreb, Informator
16. Robbins, S.P., Judge, T.A. (2009): Organizacijsko ponašanje, Zagreb, Mate d.o.o.
17. Stiglitz, E. J. (2009): Uspjeh globalizacije – novi koraci do pravednog svijeta, Zagreb, Algoritam
18. Varagić, D., (2002): Vodič kroz raj i pakao Internet marketinga, Beograd, Prometej.

Članci sa interneta:

1. CoE (2001): https://www.euromedstice.eu/en/system/files/20090130113546_ConventiononCybercrime.pdf
2. Clarke R., Knake R. (2010): Cyber War: The Next Threat to National Security And What To Do About It, HarperCollins e-books
3. Duggan P. (2015): Harnessing cyber-technology's human potential, The Professional Bulletin of the John F. Kennedy Special Warfare Center & School
4. UN. General Assembly (2004:58th sess.), Creation of a global culture of cybersecurity and the protection of critical information infrastructures: resolution/adopted by the General Assembly, UN, 30 Jan. 2004; Preuzeto sa: http://www.worldlii.org/int/other/UNGA/2003/328.pdf

11. POPIS SLIKA I GRAFIKONA

Naziv odsjeka i/ili katedre: Politologija
Predmet:

IZJAVA O AUTENTIČNOSTI RADOVA

Ime i prezime:	Alma Draganović
Naslov rada:	ELEMENTI POLITIČKOG UPRAVLJANJA U CYBER PROSTORU
Vrsta rada:	Završni magistarski rad
Broj stranica:	81

Potvrđujem:

- da sam pročitao/la dokumente koji se odnose na plagijarizam, kako je to definirano Statutom Univerziteta u Sarajevu, Etičkim kodeksom Univerziteta u Sarajevu i pravilima studiranja koja se odnose na I i II ciklus studija, integrirani studijski program I i II ciklusa i III ciklus studija na Univerzitetu u Sarajevu, kao i uputama o plagijarizmu navedenim na web stranici Univerziteta u Sarajevu;
- da sam svjestan/na univerzitetskih disciplinskih pravila koja se tiču plagijarizma;
- da je rad koji predajem potpuno moj, samostalni rad, osim u dijelovima gdje je to naznačeno;
- da rad nije predat, u cjelini ili djelimično, za stjecanje zvanja na Univerzitetu u Sarajevu ili nekoj drugoj visokoškolskoj ustanovi;
- da sam jasno naznačio/la prisustvo citiranog ili parafraziranog materijala i da sam se referirao/la na sve izvore;
- da sam dosljedno naveo/la korištene i citirane izvore ili bibliografiju po nekom od preporučenih stilova citiranja, sa navođenjem potpune reference koja obuhvata potpuni bibliografski opis korištenog i citiranog izvora;
- da sam odgovarajuće naznačio/la svaku pomoć koju sam dobio/la pored pomoći mentora/ice i akademskih tutora/ica.

Mjesto, datum **Potpis**
Sarajevo,3.2.2022.