

Pregledni rad
Review paper

JEL Classification: K22, K40, L16

Tanja Gavrić* • Nataša Kapetan • Dario Plavčić^{1***}**

RAZLIKE IZMEĐU LEGALNOG PRIKUPLJANJA INFORMACIJA OD KONKURENCIJE I INDUSTRIJSKE ŠPIJUNAŽE

DIFFERENCES BETWEEN LEGAL INFORMATION COLLECTION ABOUT COMPETITION AND INDUSTRIAL ESPIONAGE

Sažetak

Primarni cilj ovog rada je poboljšati razumijevanje razlike između četiri dijagnostičke komponente analize konkurencije prema Michaelu Porteru (budući ciljevi, trenutna strategija, pretpostavke i mogućnosti) i tehnika korištenih u industrijskoj špijunaži. Analizirat će se i opisati tehnike prikupljanja znanja i informacija s natjecanja, što je posebno važno u doba široke upotrebe društvenih medija i mobilne tehnologije u organizacijama. Granica između analize konkurencije i korporativne špijunaže granica je između legalnog i ilegalnog, etičkog i neetičkog. Budući da je ova linija često nejasna, svrha istraživanja je u konačnici dati preporuke za prikupljanje vrijednih informacija o konkurenciji na pravni i etički način. U radu se koristi teorijski pristup i pregled literature iz područja strateškog upravljanja i konkurentnih strategija kako bi se istražio taj kritični proces i analiziralo kako se njime može učinkovito upravljati. Ovaj konceptualni okvir pruža sredstvo za razumijevanje tehnika prikupljanja informacija od konkurencije koje postaju osnova za razvoj konkurentne prednosti. Ključne riječi: tehnike prikupljanja informacija, industrijska špijunaža, etika, ilegalno.

Abstract

The purpose of this paper is to improve understanding of the difference between the Michael Porter's four diagnostic components to a competitor analysis (future goals, current strategy, assumptions and capabilities) and the techniques used in industrial espionage. We will analyze and describe the techniques of compiling knowledge and information from the competition, which is particularly important in the widespread use of social media and mobile technology in organizations. The boundary between analyzing competition and corporate espionage is the boundary

between legal and illegal, ethical and unethical. As this line is often misted, the purpose of the research is to give recommendations for collecting valuable information about competition in a legal and ethical manner. This paper uses theoretical approaches from the strategic management field and competitive strategy literature to investigate this critical process and analyze how it can be effectively managed. This conceptual framework provides a means of understanding information gathering techniques that are the basis for the development of competitive advantage.

Key words: *information gathering techniques, industrial espionage, ethics, illegal.*

UVOD

Glavne odlike suvremenog razdoblja međunarodne ekonomije su: globalizacija, informatička revolucija i gospodarske integracije (Bazdan, 2016). Ubrzano vrijeme i akceleracija u tehnološkom razvoju dovodi kompanije u stanje da ne mogu osigurati svu potrebnu tehnologiju. Slično tome, porast svjetske trgovine, posebno industrijskim proizvodima, zajedno s tehnologijama koje se brzo mijenjaju, stavio je pitanje zaštite intelektualnog vlasništva u prvi plan. Konkurentska prednost industrijaliziranih zemalja počiva na njihovoj tehnološkoj superiornosti. Stoga se tehnološke inovacije ne moraju samo poticati, nego moraju biti i zaštićene. Razmatrano u tom svjetlu, briga za zaštitu prava intelektualnog vlasništva usko je povezana s većom zabrinutošću zbog mogućnosti inoviranja i natjecanja na sve konkurentnijem globalnom tržištu (Kotabe i Aulakh, 2002).

U tom kontekstu može se govoriti o industrijskoj špijunaži kao organizacijskom fenomenu. Međutim, kada se pomisli na špijunažu, mnogi će se sjetiti špijunskih trilera i Bondovih filmova. Malo će ljudi pridati ozbiljnu pozornost tom fenomenu, posebice u razmatranju ozbiljnijeg posla. Ipak, špijunaža, kao što će se kasnije vidjeti, ima vrlo dugu povijest i pedigree (Simm i Ferdinand, 2006). Različiti autori daju različite definicije i nazive industrijskoj špijunaži. Wright i Roy (1999), nazivaju ga korporativnom ili ekonomskom špijunažom i industrijskom inteligencijom. Søilen (2016) razlikuje ekonomsku i industrijsku špijunažu objašnjavajući da je posljednja izuzeta od uključivanja vlade u prikupljanje informacija i krađu znanja.

Po sebi, vojska koristi verziju ekonomske špijunaže kao vrstu ratovanja putem interneta kako bi uništila temeljne infrastrukture zemlje neprijatelja. U ovom radu, bavite ćemo se industrijskom špijunažom bez uključivanja u prikupljanje informacija. Suština industrijske špijunaže je u „krađi“ tuđeg znanja ili intelektualnog vlasništva. Znanje je veoma kompleksno i hvatanje organizacijskog znanja ili cijelog sistema menadžmenta znanja može biti jako teško. Izgradnja konkurentске prednosti podrazumijeva stvaranje i stjecanje novih znanja, šireći ga uprikladne dijelove poduzeća, tumačeći ga i integrirajući ga s postojećim znanjem te ga, ukonačnici, koristiti za postizanje superiornih učinaka (Turner i Makhija, 2006). Značajne aktivnosti ili prednosti su sredstvo kroz koje se organizacije natječu na tržištu. Uspon ekonomije utemeljene naznanju pokazao je kako je intelektualni kapital, kao četvrti čimbenik proizvodnje, od ključne važnosti za inovacije i postizanje konkurentске prednosti poduzeća (Martín-de Castro et al., 2011).

Imovina znanja je najvrjedniji resurs poduzeća i primarni izvor rente koja se generira. Učinkovito korištenje resursa zahtijeva od poduzeća iskorištavanje znanja, koje posjeduje unajvećoj mogućoj mjeri u aktivnostima stvaranja unutarnjih vrijednosti (tj. ugradnja u proizvode/usluge) i/ili komercijalizaciju u vanjskim tržištima znanja (npr. licenciranjem). Prema Barneyjevom (2001) pogledu, temeljenu na resursima poduzeća (resource-based view), resursi su konkurentna prednost za poduzeće kada su takvi resursi vrijedni, rijetki, neusporedivi i ne mogu se zamijeniti. Špijunaža nije nešto novo. Ono što je novo je način na koji se krade intelektualno vlasništvo (IP – *Intellectual Property*). Cyber napadi su najčešće korištena metoda koju koriste druge nacije, tvrtke i kriminalci kako bi ukrali IP i druge vrijedne ili osjetljive informacije.

Naša povećana ovisnost o IT (Informacijske tehnologije) sustavima i mrežama stvara ranjivosti, iako postoje takve očite prednosti i koristi od njih. Postojeća literatura objašnjava nit koju su izazvali industrijski špijuni. Prema Winkleru (1997), aspekti ranjivosti organizacije moraju se sveobuhvatno analizirati kako bi se smanjili rizici iz različitih kanala informatičkih napada od industrijskih špijuna. Cornwall (1991) daje naglasak na objašnjenju metoda i tehnika za praktični pristup prikupljanja obavještajnih podataka od poduzeća na "civiliziran" način. Nasuprot Cornwallu, postoje istraživači poput Rustmanna (2002) koji industrijsku špijunažu opisuju kao cinično ciljnoposlovanje koja daje sjajne primjere neetičkih operacija CIA-e. Svakako da postoje razni pristupi analiziranja i istraživanja industrijske špijunaže. Međutim, u daljnjem tekstu, obraditi će se legalne i ilegalne metode i tehnike analiziranja konkurencije kao u prikupljanju informacija od istih i nastojati dati smjernice u ovom složenom informatičkom okruženju, upotpunivši Porterov (2008) sveobuhvatan strukturni okvir i analitičke tehnike koje pomažu tvrtkama da analiziraju svoju industriju i razumiju konkurente i vlastiti položaj.

U razradi ove teme nameću se tri istraživačka pitanja na koja će se nastojati odgovoriti:

1. Na koji način se može analizirati konkurencija i koji je cilj takve analize?
2. Što je industrijska špijunaža i koje se tehnike pri tom koriste?
3. Gdje zakonito prikupljanje informacija od konkurencije prelazi u industrijsku špijunažu?

Drugi dio ovoga rada odgovoriti će na prvo istraživačko pitanje, a koje će se najviše bazirati na Porterove (2008) četiri dijagnostičke komponente za analizu konkurencije. Treći dio rada objašnjavanja pojam industrijske špijunaže i tehnike koje se koriste za krađu informacija od konkurencija, dok se u četvrtom dijelu raspravlja o tome može li legitimno prikupljanje informacija od konkurencije preći u protuzakonite radnje i gdje je ta linija?

1. ANALIZIRANJE KONKURENCIJE

Zahra i Chaples (1993) definiraju konkurentsku analizu kao "proces kojim tvrtka pokušava definirati i razumjeti svoju industriju, identificirati svoje konkurente, odrediti prednosti i slabosti svojih konkurenata te predvidjeti njihove poteze." Takav sustavan proces organizira protok kritičnih informacija i usredotočuje se na operativna i strateška pitanja i odluke (Hohhof, 1994). Analiza konkurencije ima za cilj pružiti dubinsko razumijevanje konkurentskih snaga koje se mogu naći u konkurentskom okruženju

pojedine organizacije. Pokušava se razumjeti industrija u kojoj organizacija djeluje, njezin konkurentski položaj u njoj, preduvjete za opstanak i prosperitet te prirodu konkurencije i tržišnog procesa (Teach i Schwartz, 1994).

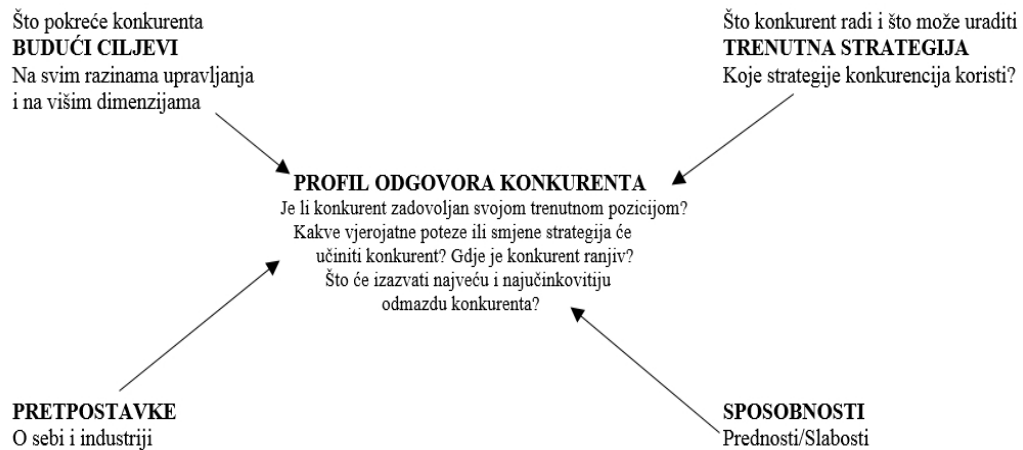
Analiza također nudi menadžmentu forum na kojem može raspravljati i procjenjivati svoje pretpostavke o sposobnostima organizacije, tržišnoj poziciji i konkurentima (Adom et al. 2016). Osoba koja se najčešće povezuje s analizom konkurencije je Michael Porter koji je učinio izvrstan posao u povezivanju niti analitičkog razmišljanja o analiziranju industrije, a zatim je nastavio razvijati koncept lanca vrijednosti (Hussey, 2007). Konkurentska strategija uključuje pozicioniranje tvrtke kako bi se povećala vrijednost sposobnosti koje ju razlikuju od konkurenata. Iz toga slijedi da je središnji aspekt formuliranja strategije perceptivna analiza konkurenta.

Cilj analize konkurenta je razviti profil uspjeha vjerojatnih promjena strategije koje svaki konkurent može napraviti, vjerojatni odgovor svakog konkurenta na raspon mogućih strateških poteza koje bi druge tvrtke mogle pokrenuti, a vjerojatna reakcija svakog konkurenta na polje promjene u industriji i šire promjene u okolini koje se mogu pojaviti (Porter, 1980). Unatoč jasnoj potrebi za sofisticiranom analizom konkurenta u formuliranju strategije, takva se analiza ponekad ne provodi eksplicitno ili sveobuhvatno u praksi.

Daljnja poteškoća je u tome što dubinska analiza konkurenta zahtijeva velik broj podataka, koje nije lako pronaći bez napornog rada. Glavna odrednica uspjeha u konkurentnom informacijskom sistemu leži u stavovima, naporima i vještinama onih koji upravljaju tim sistemom (Hohhof, 1994). Mnoge tvrtke ne prikupljaju informacije o konkurentima na sustavan način, već djeluju na temelju neformalnih dojmova, nagađanja i intuicije stečene uz pomoć informacija o konkurentima koje svaki menadžer kontinuirano prima. Ipak, nedostatak dobrih informacija otežava sofisticiranu analizu konkurenta (Porter, 2008).

Prema Porteru (2008), postoje četiri dijagnostičke komponente za analizu konkurencije (vidi sliku 1): *budući ciljevi*, *trenutna strategija*, *pretpostavke* i *sposobnosti*. Razumijevanje tih četiriju komponenti omogućit će predviđanje ponašanja konkurencije. Većina tvrtki razvija barem jedan intuitivan osjećaj za trenutne strategije njihovih konkurenata kao i njihove snage i slabosti (prikazane na desnoj strani slike 1). Mnogo manje pozornosti je usmjereno na lijevu stranu ili razumijevanje onoga što uistinu pokreće ponašanje konkurencije, njihove buduće ciljeve i pretpostavke koje imaju o vlastitoj situaciji i prirodi svoje industrije. Ove faktore je mnogo teže uočiti nego što je stvarno ponašanje konkurencije, ali oni često određuju kako će se konkurent ponašati u budućnosti.

Slika 1. Komponente pri analiziranju konkurencije



Izvor: Porter (1998), str. 49.

Razumijevanje četiri komponente, omogućit će predviđanje profila odgovora konkurencije, kao artikulaciju na ključna pitanjima postavljenim na slici 1.

1.1. Budući ciljevi

Ciljevi su prva komponenta analizi konkurencije. Poznavanje ciljeva omogućit će predviđanja zadovoljstva konkurenta sadašnjim stanjem i financijskim rezultatima, a time i vjerojatnost da će konkurent promijeniti strategiju i snagu s kojom reagirat na vanjske događaje (npr. poslovne cikluse) ili na poteze drugih tvrtki (Downey, 2005). Iako se najčešće misli na financijske ciljeve, sveobuhvatna dijagnoza ciljeva konkurencije obično uključuje mnoge više kvalitativnih čimbenika, kao što su ciljevi u smislu tržišnog vodstva, tehnološke pozicije, društvenog učinka i slično. Dijagnoza ciljeva također treba biti na višestrukim razinama upravljanja. Postoje ciljevi koji se odnose na cijelu tvrtku, ciljeve poslovnih jedinica, ciljevi za pojedinačna funkcionalna područja i ključne rukovoditelje (Porter, 2008). Dobri pokazatelji ciljeva konkurencije se mogu temeljiti na njihovoj povijest poslovanja. Sljedeća pitanja sugeriraju neke od načina ispitivanja ovih područja:

- Koji je trenutni financijski učinak konkurenta i udio na tržištu, u usporedbi s relativno novijom prošlošću?
- Koja je povijest konkurencije na tržištu tijekom vremena?
- U kojim područjima je konkurent počeo ili uspio kao tvrtka? U uvođenju novih proizvoda? Inovativni marketing? Tehnike? Drugo?
- Kako je natjecatelj reagirao na određene strateške poteze ili promjene u industrijske u prošlosti? Racionalno? Emotivno? Polako? Brzo?

Analiziranje ciljeva konkurencije pomaže u razumijevanju njihova zadovoljstva trenutnim radom i tržišnom pozicijom. To pomaže predvidjeti kako bi mogli reagirati na vanjske sile i koliko je vjerojatno da će promijeniti strategiju.

1.2. Pretpostavke

Percepcije i pretpostavke koje konkurent ima o sebi, industriji i drugim tvrtkama utjecat će na njezine strateške odluke. Analiza tih pretpostavki može pomoći identificirati konkurentske pristranosti i slijepe točke. Pri toj analizi, može se razmišljati o sljedećim točkama (Downey, 2005):

- Što konkurenti misle o sebi i o svijetu u kojem djeluju?
- Koje su pretpostavke napravili o vlastitim snagama i slabostima u odnosu na svoje konkurente?
- Je li izvjesno da će njihova strategija biti proaktivna ili reaktivna? Agresivna ili obrambena?

Svaka tvrtka djeluje na skupu pretpostavki o vlastitoj situaciji. Na primjer, može sebe smatrati društveno svjesnom tvrtkom, kao što je lider u industriji, kao proizvođač s niskim troškovima, ima najbolju prodajnu snagu, i tako dalje. Te pretpostavke o vlastitoj situaciji će voditi način na koji se tvrtka ponaša i način na koji reagira na događaje. Ako vidi sebe kao proizvođača s niskim troškovima, na primjer, može pokušati disciplinirati rezače cijena vlastitim sniženjem cijena (Porter, 1998).

1.3. Trenutne strategije

Treća komponenta analize konkurenta je razvoj trenutne strategije svakog konkurenta. Znanje o trenutnoj konkurentske strategiji se smatra najkorisnijom ključnom poslovnom politikom u svakom funkcionalnom području poslovanja (Porter, 1998). Strategija tvrtke određuje kako se konkurent natječe na tržištu. Međutim, može postojati razlika između „planirane strategije“ (strategija koja je navedena u godišnjim izvješćima, intervjuima i javnim izjavama) i „ostvarene strategije“ (strategija koju tvrtka slijedi u praksi, kao što može biti vidljivo iz akvizicija, kapitalnih izdataka i razvoja novih proizvoda). Tamo gdje trenutna strategija daje zadovoljavajuće rezultate, razumno je pretpostaviti da će se organizacija nastaviti natjecati na isti način kao i sada. U tom smislu, mogu se razmatrati sljedeće točke (Downey, 2005):

- Kako konkurenti zapravo djeluju i jesu li zadovoljni u svojim postupcima?
- Postoji li jaz između planirane strategije i ostvarene strategije?
- Postoji li vjerojatnost da će njihova strategija biti promijenjena zbog trenutnog nedostatka uspjeha ili će se vjerojatno nastaviti kretati u istom smjeru?

1.4. Sposobnosti

Ciljevi, pretpostavke i strategija organizacije će odrediti prirodu, vjerojatnost i vrijeme djelovanja konkurenta (Porter, 1998). Međutim, sposobnosti organizacije će odrediti njegovu sposobnost da inicira ili reagira na vanjske sile, kao na primjer (Downey, 2005): Koje su njihove najbolje opcije za odgovor svojim rivalima? Na primjer: Je li vjerojatnije da će odgovoriti padom cijene ili agresivnim usmjeravanjem svoje distribucijske mreže?

2. INDUSTRIJSKA ŠPIJUNAŽA

Uz jačanje globalne konkurencije, saznanje o proizvodima i procesima rivalasu postali veliki posao - i konkurentno prikupljanje obavještajnih podataka se sve više smatra važnim i uglavnom prihvatljivim oblikom istraživanja tržišta (Crane, 2003). Iako predstavnici industrije, tvrde da je industrijska špijunaža ili špijuniranje neetično i nezakonito, ponekad postoji tanka linija između „legitimne“ taktike konkurentnosti prikupljanje obavještajnih podataka i „nezakonita“ praksa industrijske špijunaže (Shing i Spence 2002). Međutim, sada kada mnoge tvrtke prebacuju svoje korporativne informacije na web, moraju shvatiti kako računalni sustavi nikada nisu bili namijenjeni da budu sigurni, i to bi trebao biti razlog za briga (Rothke, 2001). Špijunaža je prikupljanje, uspoređivanje i analiza nezakonito stečenih informacija. U slučaju industrijske špijunaže, najčešći ciljevi su utvrđivanje konkurentskih aktivnosti s obzirom na nove proizvode, formulacije, područja istraživanja, proizvodnu metodologiju, proizvodne količine, promotivne programe, distribuciju i ekonomiju. Često kompanije budu žrtve takvih aktivnosti bez znanja ili metodologije učinkovitog suprotstavljanja istom (Rothke, 2001).

Ljudi su se oduvijek bavili krađom tuđih tajni, ideja i pronalazaka. Povijest je zabilježila puno takvih primjera, Trojanski konj je možda jedna od najboljih priča o špijunaži. To su bile nevidene vojne tehnike starih Grka. To je omogućilo Grcima da zauzmu jako utvrđeni grad Troju i sabotiraju njihov obrambeni sustav. Što se tiče računalne sigurnosti, digitalni trojanski konj funkcionira točno kao ovaj povijesni primjer (Alavi, 2018). Iako postoje etičke sumnje oko ove metode zbog nelegalnih aktivnosti koje su poznate kao kriminalne radnje, ipak, ponekad mogu postati logična odluka kako bi se pribavile određene informacije i tehnologija. Ova metoda se često koristi u visoko-tehnološkim industrijama sa progresivnim tržištem i tehnologijama. Industrijsku špijunažu ponekad vrše kompanije i njihovi eksperti, a ponekad i informacijski brokери koji posjeduju određene informacije od jednog izvora, a koje prodaju organizaciji koja želi imati te informacije (Pezeshki i Zandhessami, 2011).

2.1. Tehnike u industrijskoj špijunaži

Metode industrijske špijunaže ograničene su samo maštom špijuna. Međutim, fizička krađa podataka vrlo je učinkovita i može dati špijunima informacije koje ne bi prikupili na drugi način. Može se napraviti provalomzgrade i ureda, spajanje na kablove, preuzimanje datoteka na flash pogon ili na disk. Špijuni mogu također koristiti kopanjepo smeću kako bi prikupili informacije (Bhatti i Alymenko, 2017). U mnogim slučajevima, želja za dobivanjem informacija tjera konkurenciju da ukradu ili kopirajubez dopuštenja. Vrlo često se insajderi koriste za pristup kompaniji.

Tradicionalno, krtica ili netko s dobrim kontaktima u kompaniji tko je voljan surađivati s kriminalcima. Ti ljudi često imaju pristup potrebnim informacijama ili mogu omogućiti špijunima pristup u zamjenu za novac. U nekim slučajevima zaposlenici mogu biti inicijatori za kriminalna informiranja, nudeći korporativne tajne konkurentima (Bhatti i Alymenko, 2017). Dok su na poslovnom putovanju, djelatnici kompanije mogu postati subjekti sofisticirane špijunske metode. Postavlja se pitanje, koje se tehnike industrijske špijunaže danas koriste? Svakako se može tvrditi kako je napredak tehnologije i

informatizacija u poslovanju revolucionalizirao industrijsku špijunažu. U nastavku slijedi pojašnjenje nekoliko tehnika koje se koriste u industrijskoj špijunaži (Pezeshkietal. 2010):

- *Krađa prijenosnih računala*: jedna od tehnika koja koristi prednosti novih tehnologija koje se trenutno koriste je krađa prijenosnih računala i računala.
- *Spyware*: Još jedna tehnika koja se opsežno koristi je postavljanje špijunskog softvera. Špijunski softver je softver koji se instalira potajno na ciljno računalo, obično radi praćenja ponašanja korisnika ili prikupljanja niza informacija i pohranjivanja ili prijenosa na određeno mjesto.
- *KeyLogger*: KeyLogger bilježi tipke korisnika i obično se koristi za snimanje informacija kao što su korisnička imena i lozinke.
- *Backdoors*: Tehnika koja je draga mnogim ljudima koji pokušavaju dobiti pristup računalnim sustavima u ovom trenutku je postavljanje softvera koji stvara stražnja vrata na računalo, a što omogućuje zločincima da kontrolira računalo. Jednom kada imaju kontrolu nad računalom, mogu kopirati željene informacije, pratiti što se događa i koristiti računalo za vlastite ciljeve, možda čak i pomoću njega da bi špijunirali konkurente ciljne kompanije i svaliti krivnju na njih.
- *Steganografija*: Ako osoba ima pristup računalo (netko od pouzdanog osoblja), tehnika koja se može koristiti za dobivanje informacija je skrivanje informacija u drugoj, naočigled nebitnoj datoteci. Ovo je poznato kao Steganografija (tajno pisanje) i zločincu daje mogućnost slanja datoteka koje izgledaju potpuno nebitne - možda glazbeni isječak ili slika koja također sadrži velike količine osjetljivih informacija. Iako u industrijskoj špijunaži nema otkrivenih slučajeva Steganografije, to je vjerojatno samo pitanje vremena.
- *Nadzor*: Postoje tehnike kao što su prisluškivanje i presretanje bežičnog signala, gdje se signal koji se prenosi presreće na putu. Alternativno, tu su i dobre staromodne tehnike nadzora pomoću moderne tehnologije kao što su usmjereni mikrofoni, laserski mikrofoni, prisluškivanje telefona i prisluškivanje soba.
- *Nevidljiva kopija i premještanje*: Moderni mobilni telefoni imaju značajnu mogućnost pohranjivanja podataka, zajedno s fotoaparatom visoke rezolucije i mogu komunicirati putem infracrvene veze, Bluetootha i Wi-Fi mreže uz očekivanu GSM vezu. Prijenosno računalo koje je u mnogim slučajevima jedino računalo koje će zaposleni koristiti, sada također ima sve, ili većinu, tih komponenti. USB uređaji za pohranu, mikro pogoni i flash memorijske kartice zamijenili su skromni disketni pogon i, osim što su manji i lakši za skrivanje, također imaju znatno veće kapacitete pohrane.

Poslovno-obavještajna služba ima funkciju radara – kako je to običavao reći profesor Stevan Dedijer, jedan od osnivača poslovno-obavještajne službe u svjetskim razmjerima. Tvrdio je da će gospodarska špijunaža biti velika tema 21. stoljeća i da će napredovati samo one države kojima elite to navrijeme shvate (Bazdan, 2016).

3. UPRAVLJANJE TEHNIKAMA PRIKUPLJANJA INFORMACIJA OD KONKURENCIJE

Korporacije imaju poslovne tajne, patente i intelektualnesvojstva koja im daju konkurentsku prednost na svjetskoj sceni (Alavi, 2018). Korporacije su vrijedne poslovne jedinice koje imaju veliki ekonomski i politički utjecaj na društvo (Bhatti i Alymenko, 2017). Nasheri (2005) objašnjava strateške veze između vladinih obavještajnih jedinica i uspjeha te nacije. Prvi pomaci u metodama industrijske špijunaže započele su zajedno s postojanjem informacijskog doba i svjetske globalizacije. Zakon o ekonomskoj špijunaži u SAD-u opisuje pravne aspekte industrijske špijunaže ostavljajući otvorenu raspravu o tome da li čuvati poslovne tajne ili se kretati naprijed u otvoreno globalno društvo (Bhatti i Alymenko, 2017).

U ovom radu se želi naglasiti kako sve organizacije prikupljaju i koriste neku vrstu informacija o svojim konkurentima i drugim organizacijama, bilo kroz skeniranje tržišta, profiliranje u industriji, ili jednostavno ispitivanjem voditelja regrutiranih od konkurenata. Doista, takve aktivnosti prikupljanja obavještajnih podataka su u velikoj mjeri standardni aspekt konvencionalnog istraživanja tržišta i konkurentskog benchmarkinga, te omogućuju učinkovito konkurentno ponašanje. Moglo bi se, stoga, tvrditi da je bilo koji način prikupljanja informacija prihvatljiv u konkurentskom kontekstu. Iako se tvrdikako je industrijska špijunaža ili špijuniranje neetično i protuzakonito, ponekad postoji tanka linija između „legitimne“ taktike prikupljanja informacija o konkurenciji i „nezakonite“ prakse industrijske špijunaže (Crane, 2008). U nastavku će se odgovoriti na treće istraživačko pitanje, a to jeste na dilemu gdje legalno prikupljanje podataka o konkurenciji prelazi u industrijsku špijunažu?

Korporativna špijunaža je do određene mjere poznata kao konkurentna inteligencija. Dok je konkurentska inteligencija legitiman i strateški poslovni alat, ali kada se koristi previše postaje korporativna špijunaža. Postoji nekoliko vrsta zakonske industrijske špijunaže. Mogu se kupiti proizvodikonkurenta, čime se dobiva prototip ili radna tehnologija za istraživanje. Kupnja kompanije je još jedan pravni način za stjecanje ključne tehnologije. Ova metoda se široko primjenjuje u Globalnoj svjetskoj ekonomiji gdje nitko od menadžmenta ne može stvoriti zaštitu i spriječiti dobivanje informacija na ovaj način (Bhatti i Alymenko, 2017). U slučaju spremnosti kompanije da uđe na inozemno tržište, moguće je koristiti drugi način stjecanja pravnih informacija: kompanija može biti pod pritiskom Vlada ili partnerske inozemne kompanijeda obuci lokalne radnika i menadžerekritičnoj tehnologiji (House, 1995). Često se mogu prikupiti vrijedne informacije o intelektualnom vlasništvu konkurenta, dakle o njegovim: autorskim pravima, patentima iz javnih, tzv. legalnih izvora. A kada ih dijelimo prema izvorima, razlikuju se primarne i sekundarne informacije.

Primarni izvori informacija odnose se na sve one čelne ljude koji rukovode određenim poslovnim subjektom čije je poslovanje meta analize. Njihovi nastupi, govori i intervjui posebno se analiziraju. Dakako, zanimljivi su i svi oni koji su na nižim razinama rukovođenja, pa i njihovi nastupi, intervjui i govori podliježu analizi. U skupinu primarnih izvora informacija ubrajaju se i javno dostupna analitička izvješća, ona s redovitih, ali posebno s izvanrednih skupština dioničara. Sekundarni izvori informacija

su: internet, on line i digitalne baze podataka, monografije, članci u novinama i magazinima, TV i radijske emisije i sl. Do informacija ovoga tipa može se doći i prateći sajmove, burze (turističke i sl.) i stručne skupove na kojima nastupaju predstavnici određenoga gospodarskog subjekta koji je predmet pozornosti i analize obavještajne službe. Smatra se da legalni izvori čine oko 90 posto traženih informacija. Dakle, toliki postotak podataka može se naći na takav način (Bazdan, 2016).

Postoje tri načina pomoću kojih se može odrediti prihvatljivost ili neučinkovitost uključenih radnji i utvrditi jesu li nastali etički problemi u prikupljanju obavještajnih podataka. Konkretno, može se sugerirati kako se etički problemi pojavljuju kada dođe do jednog ili više sljedećih razloga (Crane, 2008):

- *Taktike* korištene za osiguravanje informacija su upitne jer se čini da nadilaze ono što se može smatrati prihvatljivim, etičkim ili pravnim poslovnim običajima;
- *Priroda* informacija koje se traže mogu se smatrati na neki način privatnim ili povjerljivim;
- *Svrha* za kojuće se informacija koristiti je u suprotnosti s javnim interesom.

Ova tri testa se međusobno ne isključuju, i često je teško odvojiti jedan od drugog. Ipak, oni predstavljaju važne prve korake u procjeni etičnosti industrijske špijunaže.

Upitna taktika. Može poprimiti mnoge oblike, od ilegalnih, kao što su razbijanje i ulazak u urede konkurenata za krađu informacija ili instaliranje uređaja za prisluškivanje, do sivih područja. To uključuje pretraživanje smeća konkurenata, unajmljivanje privatnih detektiva kako bi pratili konkurentsko osoblje, infiltriranje u konkurentске organizacije industrijskim „špijunima“, prikriveno nadziranje putem špijunskih kamera, kontaktiranje konkurenata u lažnom izgledu kao što je potencijalni kupac ili dobavljač, intervjuirajući zaposlenike konkurencije lažno radno mjesto i pritisak na kupce ili dobavljače konkurenata da otkriju osjetljive informacije o njihovom poslovanju. To su sve taktike kojei dalje koriste inteligentni sakupljači u industriji. Takve su taktike sumnjive etičke naravi, prvenstveno zato što je upitno poštenje i istinitost u poslovanju. Pitanja upitne taktike prvenstveno su problemi koje je pokrenuo slučaj Unilever,¹ budući da su obavještajci koje su unajmili njihovi konkurenti prekoračili granicu u načinu na koji su tražili podatke (Crane, 2008).

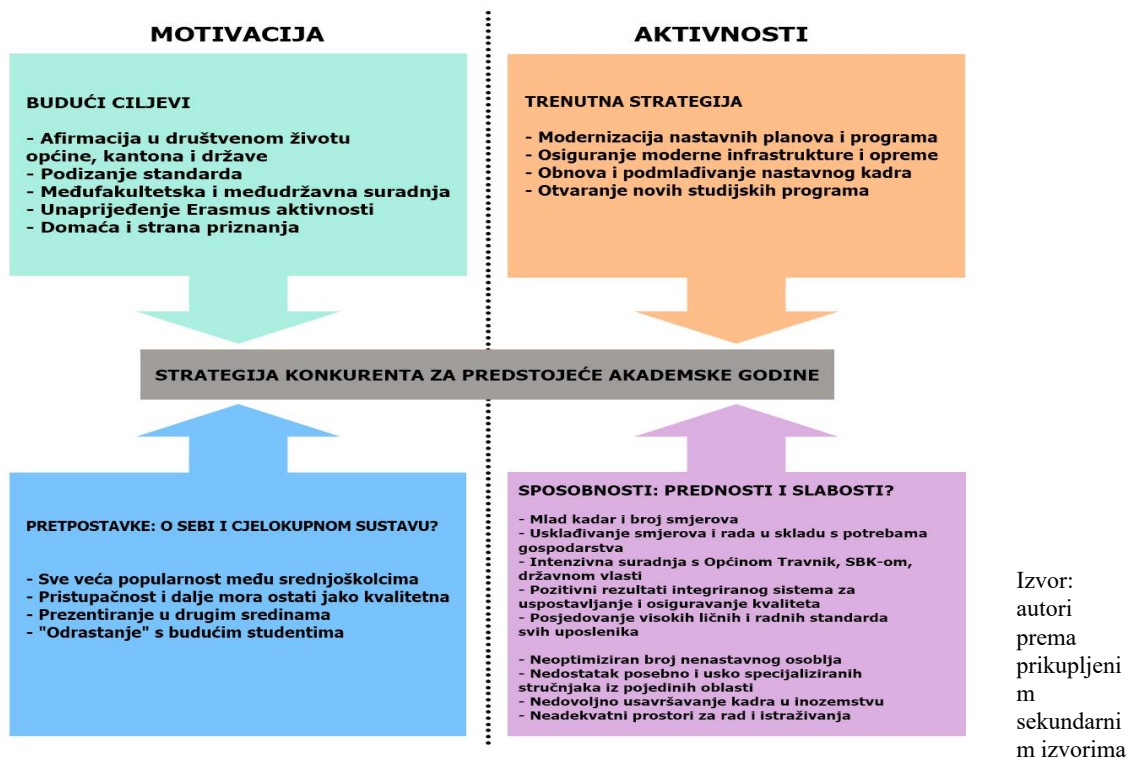
Privatne ili povjerljive informacije mogu se odnositi na bilo koju vrstu informacija za koju organizacija smatra da ne bi trebala biti slobodno dostupna strancima i koja bi stoga trebala biti neka vrsta moralne ili pravne zaštite. Dok se u načelu to čini sasvim razumno, teže je uspostaviti pravo korporacije na privatnost nego što je to za pojedinca - i svakako, provedba privatnosti je znatno složenija. To se osobito odnosi na poslovne tajne, patente, autorska prava i zaštitne znakove - što je u određenoj mjeri zakonski provedivo intelektualno vlasništvo koje pripada organizaciji (Crane, 2008). Jedan od primjera koji potiče na etičku raspravu o pitanjima zaštite intelektualnog vlasništva je i slučaj Canal Plus² koji ilustrira probleme pripisivanja vlasništva nematerijalne imovine.

Konačno, problemi *javnog interesa* mogu se pojaviti kada se informacije prikupljene preko obavještajnih podataka stavljaju u svrhe poput antikonkurentskog ponašanja, uključujući namjerno uklanjanje ili uništenje konkurenata, inflaciju cijena, ili utvrđivanje monopolskog položaja. Pitanja od javnog interesa mogu se pojaviti i kada je korporativna inteligencija važna za nacionalnu ili međunarodnu sigurnost ili domaći ekonomski učinak. Špijuniranje povezano s vojnim ili drugim

osjetljivim informacije mogu štetiti javnosti kroz povećanu izloženost različitim vrstama rizika. To su bili glavni problemi koji su pokrenuli slučaj Ericsson.¹

Slika 2 prikazuje primjer analize četiri dijagnostičke komponente za analizu konkurencije koji uključuje stratešku analizu suparničkog Univerziteta, odnosno, direktnu konkurenciju Sveučilištu „Vitez“ na području Srednjobosanskog kantona. Cilj prikupljanja ovih podataka je ukazivanje na važnost analiziranja konkurencije, te predstavljanje informacija koje su dostupne iz legalnih izvora, a koje također mogu biti dobra polazna točka za naredne korake koje Sveučilište „Vitez“ treba poduzeti u cilju formiranja adekvatne strategije pozicioniranja.

Slika 2. Strategije kojima se koriste konkurenti Sveučilišta "Vitez"



podataka

Analiza prikazana na slici 2 omogućuje procjenu namjere, ciljeva, prednosti i slabosti konkurencije za postizanje onoga što želi.

- Kako se može vidjeti, cilj konkurenta je liderstvo u privatnom obrazovanju u Bosni i Hercegovini; afirmacija u društvenom životu općine, kantona i države; podizanje standarda; međufakultetska i međudržavna suradnja; unaprijeđenje Erasmus + aktivnosti; domaća i strana priznanja.
- Ono što konkurent pretpostavlja o sebi je sljedeće: sve veća popularnost među srednjoškolicima; pristupačnost i dalje mora ostati jako kvalitetna; prezentiranje u drugim sredinama; "odrastanje" sa budućim studentima
- Trenutna strategija podrazumijeva: modernizaciju nastavnih planova i programa; osiguranje moderne infrastrukture i opreme; obnova i podmlađivanje nastavnog

– kadra; otvaranje novih studijskih programa

- Prednosti: mlad kadar; usklađivanje smjerova i rada u skladu s potrebama gospodarstva; intenzivna suradnja s općinom Travnik, SBK-om, državnom vlasti; pozitivni rezultati integriranog sistema za uspostavljanje i osiguravanje kvaliteta; posjedovanje visokih ličnih i radnih standarda svih uposlenika
- Slabosti: neoptimiziran broj nenastavnog osoblja; nedostatak posebno i usko specijaliziranih stručnjaka iz pojedinih oblasti; nedovoljno usavršavanje kadra u inozemstvu, neadekvatni prostori za rad i istraživanja.

Bez obzira na razinu sofisticiranosti prikupljanja podataka o konkurentima, važnost komunikacijske funkcije ne može se dovoljno naglasiti. Prikupljanje podataka je gubljenje vremena, osim ako se ne koristi u formuliranju strategije, a kreativni načini moraju se osmisлити kako bi se ti podaci stavili u jezgrovit i upotrebljiv obrazac do najvišeg rukovodstva.

4. ZAKLJUČAK

Informacije su sada pristupačnije nego ikad. Kompanije diljem svijeta koriste tehnologiju za aktivno istraživanje konkurencije. Sve veći broj kompanija troši stotine tisuća, ponekad i milijune dolara kako bi stekli konkurentsku inteligenciju. Njihova investicija je usmjerena na stjecanje prednosti iz podataka prikupljenih od konkurencije (Fine, 1995). Sastavljanje podataka za sofisticiranu analizu konkurenta vjerojatno zahtijeva više od napornog rada. Da bi bila učinkovita, postojipotreba za organiziranim mehanizmom - nekom vrstom konkurentskog obavještajnog sustava - kako bi se osiguralo da je proces učinkovit. Elementi sustava inteligentne konkurencije mogu varirati u skladu s potrebama određene kompanije, na temeljunjene industrije, sposobnosti osoblja, interesa i talenatamenadžmenta. Prečesto, međutim, nitko nije odgovoran za analizu konkurencije.

Čini se da ne postoji niti jedan ispravan način prikupljanja konkurentskih podataka, ali je jasno da netko mora preuzeti aktivni interes ili će se izgubit mnogo korisnih informacija (Porter, 1998). U današnjem svijetu preopterećenom informacijama, prikupljanje podataka ili informacija nije ključno pitanje. Umjesto toga, ključno je ispitivanje i procjena informacija putem analize koja je ključna za definiranje odgovarajućih strategija. Ovaj proces zahtijeva vještinu, vrijeme i trud. Dok većina organizacija prikuplja neke oblike konkurentnih informacija, malo ih formalno analizira i integrira rezultate u svoju poslovnu strategiju. Veoma često kompanija ne može shvatiti vrijednost informacije koju posjeduje (House, 1995). U konkurentskom okruženju temeljenomna znanju, poticaji za prekoračenje granice u prikupljanju obavještajnih podatakaznačajno su se povećali, te s napretkom u informacijskoj i komunikacijskojtehnologiji, mogućnosti za takve aktivnosti su se multiplicirale. Osim toga, granice definiranja prihvatljive prakse također postaju sve višezamagljene, pogotovo sada kada su te tehnologije i druge “špijunske” tehnike postale tako lako dostupnekompanijama.

LITERATURA

1. Alavi, R. (2018). *Countering Espionage: An Enterprise Risk Management View*. Reaserch Gate.
2. Barney, J. B. (2001). Resource-based theorie sofcompetitive advantage: A ten-year retrospective on there source-based view. *Journal of management*, 27(6), 643-650.
3. Bazdan, Z. (2016). Poslovno – obavještajne službe, industrijska i gospodarska špijunaža u međunarodnoj ekonomiji. *Zbornik Sveučilišta u Dubrovniku*, (3), 49-72.
4. Bhatti, H. J., & Alymenko, A. (2017). A Literature Review: Industrial Espionage.
5. Cornwall, H. (1991). *The industrial spionage handbook*. Century.
6. Crane, A. (2003). In the company of spies: Theeth ics of industriale spionage, Research Paper Series, No. 15-2003 ICCSR.
7. Downey, J. (2005). Strategic AnalysisTools: Topic Gateway Series No. 34. *London: CIMA*.
8. Fine, N. (1995). Competitive intelligence: an external threat andaninternal requirement. *COMPUTER SECURITY JOURNAL*, 11, 75-78.
9. Hohhof, B. (1994). Developing in formation-systems for competitive intelligence support, „Library Trends“ 43(2).
10. House, W. (1995). AnnualReport to Congress on Foreign Economic Collection and Industrial Espionage. *Washington, DC: Government Printing Office*.
11. Hussey, D. E. (2007). *Strategic management: from theory to implementation*. Routledge.
12. Kotabe, M., & Aulakh, P. S. (eds.). (2002). *Emerging issues in international business research*. Edward ElgarPub.
13. Martín-de-Castro, G., Delgado-Verde, M., López-Sáez, P., & Navas-López, J. E. (2011). Towards ‘anintellectualcapital-basedviewofthefirm’: originsand nature. *Journal of Business Ethics*, 98(4), 649-662.
14. Naseri, H. (2005). *Economic espionageand industrial spying*: Cambridge University Press.
15. NgKwetShing, M., & Spence, L. J. (2002). Investigating the limits of competitive intelligence gathering: is my stery shopping ethical? *Business Ethics: A European Review*, 11(4), 343-353.
16. Pezeshki, P. M., Zandhessami, H., & Moradian, A. (2010). Industrial Espionagein Iran and Prevention Methods.
17. Porter, M. E. (2008). *Competitivestrategy: Techniques for analyzing industries and competitors*. Simon andSchuster.
18. Rothke, B. (2001). Corporate espionage and what can bedone to preventit. *Information system ssecurity*, 10(5), 1-7.
19. RustmannJr, F. W. (2002). *CIA, Inc.: Espionage and the craf tof business*

-
- intelligence*. PotomacBooks, Inc..
20. Simm, D., & Ferdinand, J. (2006). Economic and industrial espionage: A different perspective on inter-organizational learning.
 21. Søylen, K. S. (2016). Economic and industrial espionage at the start of the 21st century—Status quaestionis. *Journal of Intelligence Studies in Business*, 6(3).
 22. Teach, R. D., & Schwartz, R. G. (1994). *Pricing for Entrepreneurial Firms*. Westport, CT: Quorum
 23. Turner, K. L., & Makhija, M. V. (2006). The role of organizational controls in managing knowledge. *Academy of management review*, 31(1), 197-217.
 24. Winkler, I. (1997). Corporate Espionage. *Inc.*, 19(8), 91-93.
 25. Wright, P. C., & Roy, G. (1999). Industrial espionage and competitive intelligence: one you do; one you do not. *Journal of Workplace Learning*, 11(2), 53-59.
 26. Zahra, S. A., & Chaples, S. S. (1993). Blindspots in competitive analysis. *Academy of Management Perspectives*, 7(2), 7-28.
 27. Zandhessami, H., Pezeshki, P. M., & Moradian, A. (2011). Industrial Espionage as a Method of Technology Transfer and How to Prevent it. *Asian Journal of Information Technology*, 10(5), 170-179.