SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Marija Zemljić

INDUSTRIJSKA ŠPIJUNAŽA

ZAVRŠNI raD

Varaždin, 2014.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Marija Zemljić

Izvanredni student

Broj indeksa: 37082/08 izv

Preddiplomski studij

INDUSTRIJSKA ŠPIJUNAŽA

ZAVRŠNI RAD

Mentor:

Doc. dr. sc. Markus Schatten

Varaždin, rujan 2014.

Sadržaj

1. Uvod 1

2. Industrijska špijunaža 2

2.1. Općenito o obavještajnim službama 2

2.2. Važnost i vrijednost poslovnih informacija 3

2.2.1. Shannonov kvantitativni pristup 5

2.2.2. Hammingov vremenski pristup 6

2.2.3. Liautaudov poslovno-pragmatički pristup 7

2.3. Povijest i rasprostranjenost 9

3. Motivacija i ciljevi, metode, tehnička podrška, zaštita podataka 12

3.1. Motivacija i ciljevi industrijske špijunaže 12

3.2. Metode i načini provođenja industrijske špijunaže 12

3.3. Legalnost postupaka u industrijskoj špijunaži 16

3.3.1. Legalni postupci 16

3.3.2. Ilegalni postupci 17

3.4. Tehnička podrška 18

3.5. Zaštita podataka 18

4. Povezanost upravljanja znanjem sa industrijskom špijunažom 21

5. Primjeri industrijskih špijunaža 23

5.1. Renault 23

5.2. McLaren protiv Ferrarija 24

5.3. Ericson 26

5.4. Hewlett-Packard špijunirao je sam sebe 26

5.5. Hakerski napad na račune poduzeća u RH 27

5.6. Sony PlayStation Network 28

5.7. Farmaceutske kuće koriste NSA-u da bi dobile podatke 29

6. Zaključak 31

Literatura 32

# 1. Uvod

Svijet je prepun podataka i informacija, koje u poslovnom svijetu imaju vrijednost. Do informacija uvijek želimo doći, ali ne možemo ih uvijek imati u ključnom trenutku kada nam nužno trebaju. O informacijama može ovisiti poslovanje nekog poduzeća, te se zbog toga informacije sve češće prodaju ili čak pokušavaju lažirati i ukrasti kako bi se spriječilo konkurenciju da napreduje.

Ovaj rad bavi se tematikom industrijske špijunaže koju rade obavještajne službe u svrhu raznih interesa poduzeća iz neke države.

U radu će biti objašnjeni pojmovi vezani uz industrijsku špijunažu, važnost i vrijednost poslovnih informacija, ukratko će se osvrnuti na povijest i rasprostranjenost industrijske špijunaže.

Isto tako, u radu će biti navedeni neki od motiva i razloga za postupak industrijske špijunaže, navest će ciljevi kompanija koje plaćaju obavještajnim službama da za njih rade, bit će navedene strategije i metode koje koriste obavještajne službe, tehnička podrška, legalnost postupaka te se ukratko bude objasnila zaštita podataka.

Kako bi se navedene teme bolje prikazale, budu potkrijepljene primjerima uspješnih i neuspješnih industrijskih špijunaža. Na kraju, nalazit će se osvrt autorice rada na cijelu temu u obliku zaključka.

# 2. Industrijska špijunaža

## 2.1. Općenito o obavještajnim službama

Obavještajno sigurnosne službe postoje od davnina, te su se s vremenom zbog različitih potreba razvile, i mogu se podijeliti na vojne, političke i industrijske. Obavještajno sigurnosne službe u većini demokratskih država postoje kao zaštita državi te nisu dužne pomagati sudskoj vlasti, osim ukoliko je to u interesu države. Za praćenje, nadzor i prisluškivanje ne trebaju tražiti posebne dozvole od države, jer je to regulirano zakonom. Izvještaje podnose najvišoj izvršnoj vlasti. Najčešće su organizirane u više odjela, čiji se obavještajci međusobno ne poznaju. Neki od najčešće odjela su: odjel za mobilizaciju i obuku, odjel za prikupljanje podataka, odjel za analizu podataka, odjel za širenje dezinformacija, odjel za provokacije, odjel za planiranje, odjel za terorističke operacije, odjel za unutrašnju zaštitu, te odjel za financiranje. Napoznatije i intelektualno najjače obavještajne službe su izraelski Mosad i britanska služba, MI6, dok su tehnički najbolje opremljene amer ičke službe CIA i NSA. [Čuljak]

Zbog zaštite interesa poduzeća, razvile su se i protuobavještajne službe, kojima su ciljevi obrana i sigurnost, usmjerene su na zaštitu vlastitog obavještajnog djelovanja i tajni, a to rade na način da sprječavaju obavještajno djelovanje drugih te manipuliraju obavještajnim službama. Otkrivaju akcije „napadačkih“ obavještajnih službi, neutraliziraju ih, to jest sprječavaju njihovo djelovanje. Često šire dezinformacije kako bi se zbunilo „napadača“. [Javorović, Bilandžić, 2007, str. 177-178]

Važno je razlikovati pojam obavještajne službe od industrijske špijunaže. Obavještajne službe rade većinom legalne radnje obavještavanja, ali mogu se baviti i industrijskom špijunažom, koja je uglavnom kažnjiva. Mnogi autori slažu se kako je industrijska špijunaža, kao obavještajna djelatnost, proces davanja pristupa informacijama nekome nevezanome uz poduzeće, otkrivanje poslovnih informacija, poput informacija o proizvodnji i proizvodima, poslovnih planova, informacija o klijentima i slično. Dakle, radi se o prikupljanju zaštićenih podataka nekog poduzeća. Vrlo je čest slučaj da se otkrivaju poslovne tajne te se zaposlenici zbog dodatnih zarada ili ucjena često upliću u takve postupke davanja podataka drugima, koji su kažnjivi. Moglo bi se reći da je industrijska špijunaža korištenje usluga obavještajnih službi u interesu poduzeća iz neke države, i pritom se koriste legalni i ilegalni postupci prikupljanja podataka, s ciljem onemogućavanja konkurentske tvrtke da obavi svoj posao kako je planirano ili da se nabave informacije prije konkurentskog poduzeća, kako bi ga se preteklo, ili uklonilo s tržišta.

Isto tako, uz pojam obavještajnih djelatnosti, često se pojavljuje pojam „business intelligence“, koji je u prvotnom konceptu označavao razne načine istraživanja, prikupljanje i analizu informacija. U modernom značenju, business intelligence označava legalnu aktivnost prikupljanja javnih podataka, koji su svima dostupni, a ti podaci mogu biti objavljeni i neobjavljeni, a sve s ciljem stjecanje konkurentske prednosti. Prema Javoroviću i Bilandžiću, business inteligence kao obavještajna djelatnost ima tri značajke, a to su:

1. Proces prikupljanja podataka i informacija, te njihova obrada i analiza nakon koje postaju „znanje“
2. Usmjerenost na informacije iz kojih se mogu predvidjeti ili predočiti budući procesi, događaji, akcije ili kretanja
3. Potporna uloga u procesu odlučivanja

Postoji mnogo business intelligence alata koji se danas koriste, postaju sve popularniji jer olakšavaju poslovanje. [Javorović B., Bilandžić M., 2007, str. 201].

## 2.2. Važnost i vrijednost poslovnih informacija

## 

Informacije postoje od početka čovječanstva, te su se s vremenom razvijali načini zapisivanja, čuvanja i prenošenja informacija. Svakodnevno čovjek iz okoline dobiva mnogo informacija, nužnih, bitnih i nebitnih, vezanih uz posao ili privatni život, te čovjek postaje ovisan o informacijama. Zapravo, moglo bi se reći da čovjek saznaje podatke, a tek kada su mu ti podaci potrebni da se pomoću njih odluči napraviti neku akciju, tada je to informacija. Neke podatke će čovjek samo ignorirati, a neke će s veseljem prihvatiti, ili ih čak s nestrpljenjem čekati.

Javorović i Bilandžić[[1]](#footnote-2) su informacije podijeli u deset kriterija s podkriterijima:

* Prema nastanku
  + Izvorne
  + Izvedene
* Prema učinku
  + Korisne
  + Nekorisne
* Prema izvoru
  + Vlastite, unutarnje
  + Tuđe, vanjske
* Prema pojavnom obliku
  + Glasovne
  + Pisane
  + Slikovne
  + Zvukovne
  + Znakovne
* Prema vjerodostojnosti
  + Točne, istinite
  + Krive, neistinite
* Prema području djelovanja
  + Gospodarske
  + Društvene
  + Političke
  + Odgojno-obrazovne
  + Sigurnosne
  + Vjerske
  + Zdravstvene
  + Kulturne
  + Znanstvene
  + Informacijsko-komunikativne
* Prema otvorenosti
  + Javne
  + Tajne
* Prema razini
  + Lokalne
  + Subregionalne
  + Državne, nacionalne
  + Regionalne
  + Planetarne, svjetske, globalne
* Prema sadržaju
  + Osobne
  + Opće
  + Poslovne, funkcionalne
* Prema dospijeću
  + Pravovremene
  + Zakašnjele, zastarjele

Gledajući iz aspekta poslovnog svijeta, sve informacije su važne, čak i one nekorisne mogu drugima biti korisne. Informacije mogu biti podloga za razne aspekte poslovanja, poput lakšeg procesa odlučivanja, predviđanja, poslovnog djelovanja, pružaju veću sigurnost, olakšavaju pregovaranje i tako dalje. Zbog toga je vrlo teško točno i objektivno procijeniti koliko zapravo informacija vrijedi, to ovisi o više kriterija, poput vremena dobivanja informacije, ciljeva, korisnosti informacije, subjektivnom doživljaju važnosti informacije, i slično. Panian i Klepac[[2]](#footnote-3) navode tri pristupa vrednovanja informacija, a to su:

1. Shannonov kvantitativni pristup
2. Hammingov vremenski pristup
3. Liautaudov poslovno-pragmatički pristup

Svaki od pristupa ukratko je objašnjen kroz sljedeća tri poglavlja.

### 2.2.1. Shannonov kvantitativni pristup[[3]](#footnote-4)

Claude Elwood Shannon došao je do spoznaje da se količina informacija zapravo može nazvati entropijom polja slučajnih događaja koje generira, to jest stvara informaciju, te je postavio formulu za izračun entropije koja glasi:

H(X) označava entropiju polja slučajnih događaja X, pi označava vjerojatnost i-tog događaja iz polja X, dok je ld pi dualni logaritam vrijednosti vjerojatnosti i-tog događaja iz polja X.

Shannon je kasnije još dorađivao svoj prijašnji zaključak, te dok je pokušavao izvesti vrijednost informacije iz njezine količine polazi od pretpostavke da polje X prije i-tog događaja karakterizira vrijednost prethodne entropije, to jest H(X, 1), a nakon što se dogodi i-ti događaj, polje X ima vrijenost entropije H(X, 2). Razlika entropija I(X) prije i poslije i-tog događaja je količina informacija koja se generira tim događajem, to jest vrijedi:

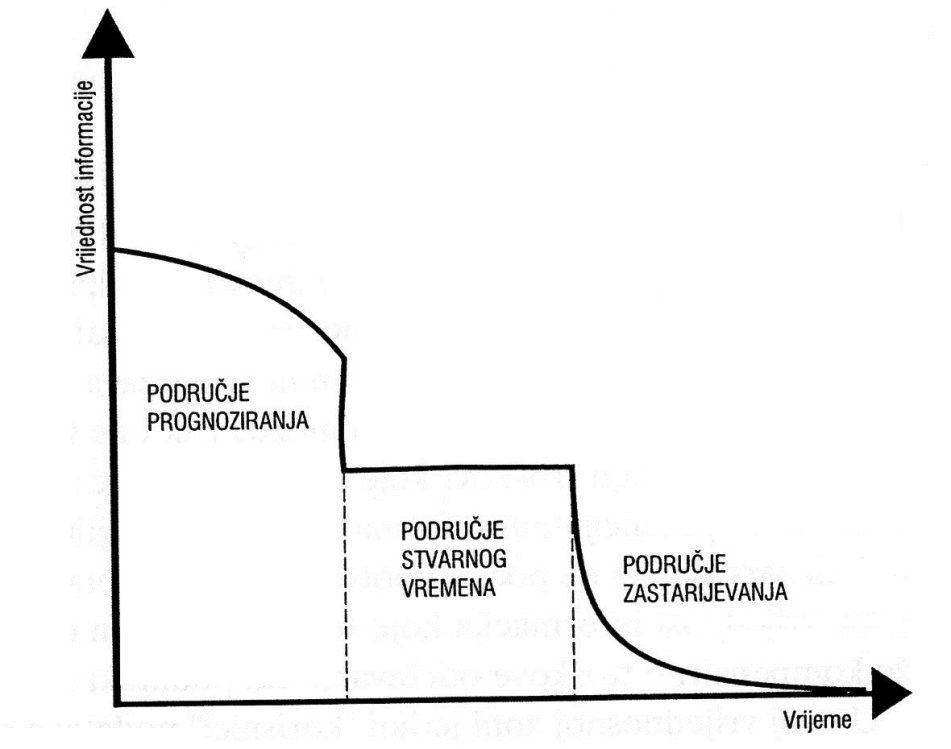
Rangovi koje Shannon postavlja kao vezu između količine informacija i vrijednosti informacija su sljedeći:

* Ako je , tada je generirana potpuna, savršena informacija
* Ako je , tada je generirana nepotpuna informacija
* Ako je , tada je generirana nulta informacija
* Te ako je , tada je generirana negativna informacija, to jest dezinformacija

Shannon je djelomično uspio u povezivanju količine informacija s njihovom vrijednošću, jer je postavio samo četiri ranga, ali je time dao velik doprinos razvoju znanstvenih spoznaja u području vrednovanja informacija.

### 2.2.2. Hammingov vremenski pristup[[4]](#footnote-5)

Richard Hamming postavio je koncept životnog ciklusa informacije, koji govori da svaka informacija ima trenutak nastajanja, vrijeme trajanja te vrijeme isteka nakon kojeg nestaje, to jest postaje irelevantna i nebitna. Vrijednost informacije je funkcija vremena. Grafički Hamming to prikazuje kao što je prikazano na slici 2.1.



**Slika 2.1. Vrijednost informacije u vremenu [Panian, Klepac, 2003, str. 42]**

Na grafu kojeg slika prikazuje vidljivo je kako informacija ima tri karakteristična razdoblja, to jest područja – područje prognoziranja, područje stvarnog vremena te područuje zastarijevanja. Karakteristika područja prognoziranja je to što se informacija dobiva i prije nego je nužno potrebna, primjerice za donošenje odluke. U toj fazi informacija ima najveću vrijednost te s vremenom pada nelinearno. Karakteristika područja stvarnog vremena je ta što se informacija pojavljuje upravo onda kada je zaista potrebna, i vrijednost informacije ostaje konstantna sve do područja zastarijevanja, za koje je karakteristično da se informacija dobiva prekasno, informacija nije relevantna ili postojeća koja se prenosi iz prošlog područja također nije relevantna ili potrebna. U tom zadnjem području vrijednost informacije naglo eksponencijalno pada.

Hammingova istraživanja dala su više rezultata i imala su jači odjek nego Shannonova, najviše u području menadžmenta, pošto suvremeni menadžment zahtjeva informaciju u pravo vrijeme ili nešto ranije. Pokazalo se da treba dati dozu opreza području prognoziranja, jer se još uvijek ne poznaju dobro prognostičke metode, te je savjet težiti tome da se informacija posjeduje u području stvarnog vremena, pošto se tada omogućuje pravovremeno donošenje kvalitetnih odluka.

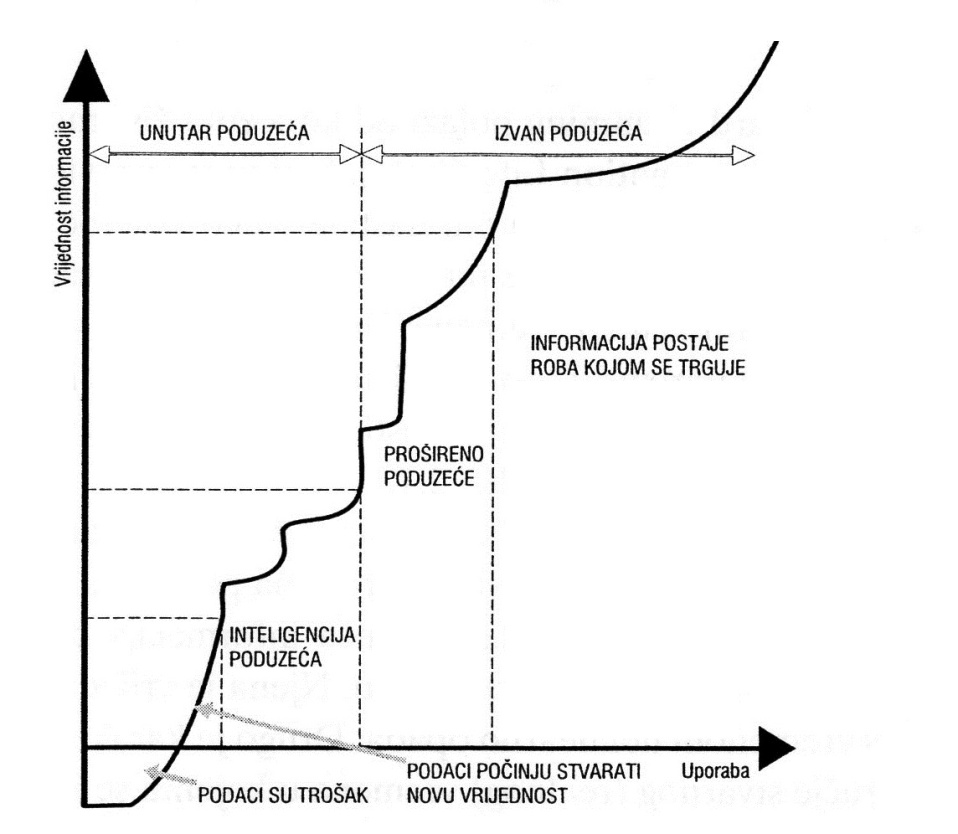
### 2.2.3. Liautaudov poslovno-pragmatički pristup[[5]](#footnote-6)

Bernard Liautaud postavlja polazište za vrednovanje informacija na činjenicu da se vrijednost neke informacije proteže u kontinuumu. Cijelo poduzeće ili veći dio poduzeća koristi istu informaciju za različite odluke, ali isto tako upotreba neke informacije može se širiti i prema klijentima i partnerima. Prema tom polazištu, Liautaud zaključuje da se vrijednost informacija može dovoljno precizno definirati, da bi bilo zadovoljavajuće, kao funkcija broja korisnika te informacije i broja poslovnih područja kojima korisnici pripadaju. Njegov zaključak može se iskazati sljedećim izrazom:

Izraz prikazuje kako vrijednost gledane informacije raste razmjerno kvadratu broja korisnika koji mogu imati pristup informaciji pomnoženim s brojem poslovnih područja u kojima se ti korisnici kreću, to jest rade. Liautaud je inspiraciju za kvadrirani broj korisnika uzeo iz „mrežnog učinka“ jer smatra da je dobro da što više ljudi dijeli istu informaciju jer se lakše razumiju, lakše komuniciraju, bolje surađuju i donose bolje odluke. Također, Liautaud tvrdi da se u kontinuumu vrijednosti određene informacije može uočiti pet zona:

1. Zona u kojoj podaci predstavljaju trošak
2. Zona u kojoj podaci počinju stvarati novu vrijednost
3. Zona inteligencije poduzeća
4. Zona proširenog poduzeća
5. Zona u kojoj informacija postaje roba kojom se trguje

Sljedeća slika, slika 2.2, prikazuje grafički kontinuum vrijednosti informacija, s označenim zonama.



**Slika 2.2. Kontinuum vrijednosti informacije [Panian, Klepac, 2003, str. 45]**

Zona u kojoj podaci predstavljaju trošak odnosi se na podatke koji su samo pohranjeni na računalu, s njima se ništa ne radi, zauzimaju memorijsko mjesto na računalu, a netko se mora i brinuti o tome da podaci ne nestanu ili ih održavati. Za rješavanje takvih situacija, potrebno je čuvati samo informacije koje se budu mogle ponovno koristiti u nekim analizama, ili za koje se zna da budu potrebne u budućnosti.

Zona u kojoj podaci počinju stvarati novu vrijedsnot je upravo korištenje informacija koje poduzeće posjeduje. Najlakše je poduzeće umrežiti i omogućiti onima koji trebaju koristiti informacije lak i jednostavan pristup svim važnim informacijama. Isto tako, nove informacije treba lako moći dijeliti sa svima koji ih trebaju znati.

Zona inteligencije poduzeća odnosi se na dijeljenje informacija unutar poduzeća, tako da svi korisnici informacija tu informaciju mogu razmotriti iz drugačijeg aspekta, vezanog uz svoju funkciju, te time postići sinergiju funkcija i bolje poslovanje.

Zona proširenog područja dozvoljava kontrolirano širenje informacija izvan poduzeća, primjerice s poslovnim partnerom ili klijentom, a time se postiže rast poslovne inteligencije poduzeća.

Zona u kojoj je informacija roba kojom se trguje nadilazi prethodnu zonu, jer se u prethodnoj zoni radi isključivo o poslovnim suradnicima, dok se u ovoj zoni misli na prodaju, to jest dijeljenje informacija koje su u određenom poduzeću već sazrele s konkurentima.

## 2.3. Povijest i rasprostranjenost

Špijunaža ne postoji samo otkad je društvo postalo kapitalistički nastrojeno, ona se spominje još u antičko doba i bila je raširena svuda po svijetu. Adrienne Wilmoth Lerner[[6]](#footnote-7) u svom radu piše kako se u egipatskim hijeroglifima otkrila prisutnost sudskih špijuna, na papirusima su opisane drevne operacije trgovine robljem, također su postojali špijuni koje su unajmljivali faraoni da bi pronalazili neposlušnike, to jest ljude koji nisu odani faraonu, ili plemena koja bi mogla napasti carstvo. Egipatski špijuni su imali zadaću saznati i o Rimu i Grčkoj, kakva je politička situacija i strateška snaga, a bili su prvi koji su masovno koristili zmijske i biljne otrove kako bi sabotirali nekoga ili napravili atentat. Rani Grci su se koristili prevarama. Time su ostvarivali iznenadne napade na svoje protivnike. Grci su bili jako poznati po strategiji prevare protivnika, postoji mnogo književnih djela s tematikom gdje su opisana junačka i prevarantska djela starih Grka. Legendarna je priča kako su Grci ušli u grad Troju, pomoću drvene konstrukcije u obliku konja koju su darovali Troji, a unutra su bili skriveni grčki vojnici koji su potom napali nespremnu Troju. Na taj način su vojnici imali lak i osiguran ulazak u grad Troju. Na Bliskom Istoku je osnovana jedna od prvih obavještajnih službi. Uništavali su informacije koje su dolazile iz drugih država o trgovini i pomorcima. Postoje zapisi iz petog stoljeća koji spominju špijunažu u dolini Inda prije 2.500 godina. Najrazvijeniju špijunažu u starom vijeku su imali Rimljani. Oni su špijunirali susjedne zemlje i plemena, čak su bili uključeni u pripajanje plemena carstvu. Najbolje im je išlo političko špijuniranje. Špijuni su sudjelovali u stranim i domaćim operacijama, procjenjivali su političku klimu u carstvu i okolnim zemljama. Špijunirale su i protivničke strane unutar carstva pa su se počele razvijati i prve protuobavještajne sile.

Lerner također piše kako početkom srednjeg vijeka, kada je Rimsko carstvo propalo, nije bilo toliko potrebe za špijunažom kao prije, barem na tom dijelu svijeta. Uskoro se razvijaju dvije velike države, Francuska i Engleska, ali su ljudi još uvijek bili nepismeni, te je onaj mali broj pismenih radio u diplomaciji, prenosile su poruke usmeno, a prenositelji poruka nazivali su se kuriri, dok su svećenici bili u službi pisara. Špijunaža je uglavnom ostala još uvijek na području ratovanja i napadačkih operacija, ali kako se razvijao feudalni sustav gdje su lordovi obećavali vjernost monarhu, dolazilo je do izdajništva, te su se takve izdaje počele kažnjavati i kazne propisivati zakonima. U tom razdoblju do izražaja dolazi i katolička crkva, kojoj se moć znatno povećala zbog križarskih ratova i inkvizicije, te je time i Crkva postala obavještajna zajednica. Tijekom razdoblja inkvizicije, postojao je velik broj špijuna koji su činili obavještajnu mrežu Crkve, a sve u korist opstanka političke moći Crkve.

Lerner navodi da je razdoblje renesanse je obilježila vladavina Crkve, te se u Europi špijunaža razvila toliko da je svaki narod ili ponegdje i više gradova unutar države imalo obavještajnu službu, a razlog razvoju špijunaže je nadmetanje država za dominaciju u trgovanju. U Velikoj Britaniji, kada je Elizabeta I. preuzela krunu, odlučila je ojačati vojsku kako bi se branila od nelojalnih lordova i njihovih snaga, posebice se zalagala za jačanje i širenje mornarice i obavještajnih službi. Mornarica je uspješno odbila strane prijetnje, pobjedivši španjolsku Armadu, a obavještajne službe su uspješno riješile nekoliko zavjera kojima je bila namjera svrgnuti Elizabetu I. s trona. Tehnološki razvoj u to vrijeme uvelike utječe na špijunažu. Razvilo se malo vatreno oružje, poput pištolja, i česte su bile operacije s bodežima. Kemičari su marljivo radili na nevidljivim tintama, a ponovno proučavanje matematike pomoglo je kod korištenja raznih metoda šifriranja i kodiranja. Razvoj teleskopa, povećala i sličnih pomagala omogućilo je špijuniranje na daljinu, te je razvoj vozila olakšao putovanja.

Ono što možemo nazivati modernom špijunažom počinje se javljati u 18. stoljeću, piše Lerner. Cijelo to razdoblje je obilježeno brojnim ratovima. To je i razdoblje industrijalizacije, ekonomske i teritorijalne ekspanzije, pojave novih političkih poredaka, filozofija i režima, te je potreba za špijunažom sve veća i veća. Velika primjena špijunaže bila je za otkrivanje i traženje izdajica, a ta su se djela kasnije čak smatrala i zloupotrebom obavještajnih snaga. Europski narodi okrenuli su svoju pozornost na kolonizaciju afričkog kontinenta, te su tamošnji vladari bili primorani angažirati tajnu policiju i agente za špijunažu na svojim teritorijima ne bi li ugušili antinacionalne pobune i pokrete. Moderna industrijska špijunaža nastala je nakon revolucije 1848. godine u Europi. Vođe velikih i bogatijih država morali su angažirati špijune koji su ih obavještavali o svim aktivnostima protiv vlasti. Često su se obavještajne jedinice špijunirale međusobno, izvještavale zatim o uvjetima rada, planovima tvornica, rudarskim pronalascima i slično. Mnoge obavještajne službe su sabotirale i uništavale tvornice, rudnike ili neko drugo državno vlasništvo. Dobri špijuni bili su nakon desetogodišnjeg iskustva prebačeni u državne snage kao špijunu protiv stranih ekonomskih interesa. Tijekom industrijalizacije razvile su se naprave za prikrivanje, prepisivanje i analizu podataka. Pronalazak dinamita uvelike je potpomogao u sabotažama, a razvoj fotoaparata u špijuniranju. Kemijsko oružje doživjelo je još veći razvoj. Do pojave elektronske pohrane podataka, fotografija je bila najkorištenije sredstvo kopiranja i prijenosa informacija. Izum telegrafa još je više olakšao špijunske operacije, razvilo se korištenje složenih kodova, te su se razvili odjeli za kriptografiju. Većina obavještajnih službi SAD-a i Europe bila je uključena u komunikacijski nadzor i prisluškivanje telegrafa. Razvojem prometa, željeznice kojima su se često prevozile sirovine, postale su metom sabotaže. Jedan od popularnih načina špijuniranja bili su agenti pod krinkom turista, jer su tako izazivali manje pažnje i sumnje. Današnja špijunaža evoluirala je u tehničkom smislu. Uključuje istraživanja i analizu podataka više nego terenske operacije. Specijalizirane vojne postrojbe i dalje služe u svrhu strateške inteligencije, ali većina zemalja svijeta ima civilne obavještajne zajednice koje provode operacije i u vrijeme mira i u vrijeme rata, uz povećanje tehnološke sofisticiranosti.

# 3. Motivacija i ciljevi, metode, tehnička podrška, zaštita podataka

## 

## 3.1. Motivacija i ciljevi industrijske špijunaže

Većina autora se slaže kako se industrijskom špijunažom, kako je već navedno ranije u radu, bave se poduzeća, to jest poduzetnici. Glavni cilj svakog poduzetnika je profit i prevladavanje na tržištu, a ukoliko je moguće i monopol na tržištu. Kako bi ostvarili svoj konačan cilj, poduzeća se upuštaju u djelatnost industrijske špijunaže ili najam neke obavještajne službe, to jest agencije, koja bude pribavila sve što im je potrebno da steknu prevlast na tržištu i ostvare željeni profit.

Ono što je glavni cilj industrijske špijunaže je dobivanje informacije koju to poduzeće nema, a netko drugi je posjeduje i dobro (ili manje dobro) čuva, a ta informacija ima veliku vrijednost i značaj za poduzeće. Osim toga, motivacija za djelatnost industrijske špijunaže može biti i borba protiv konkurencije, to jest sabotaža konkurenata, također s ciljem ostvarivanja prevlasti na tržištu i profita, ili samo s ciljem uništavanja konkurenata, makar to poduzeće i ne ostvari svoj primarni cilj.

Dakle, smisao industrijske špijunaže je doći do potrebne, a vrijedne informacije, kako bi se tu informaciju moglo što bolje iskoristiti u poslovanju i pregovaranju s ciljem ostvarivanja profita i probijanja na tržištu.

## 3.2. Metode i načini provođenja industrijske špijunaže

Nije lako domoći se informacija u današnjem svijetu, posebice zato što vlada „glad“ za informacijama, i često istu informaciju žele brojna podueća. Zbog takve situacije, često se uopće ne razmišlja o tome kako doći do informacija, to jest koja sredstva koristiti, nego se koristi bilo što samo da se dobiju potrebne informacije. Javorović i Bilandžić[[7]](#footnote-8) navode kako je zbog toga došlo do *rata za informacije*, ali i do *informacijskog rata*, jer je poduzećima koja su svjesna da imaju vrijednu informaciju, cilj tu informaciju zaštiti, te na neki način i sabotirati konkurente. Pod pojmom *rat za informacije*, Javorović i Bilandžić smatraju da je informacija predmet ugrožavanja, to jest pojam označava veliku borbu u nastojanjima da se tu informaciju dobije na vrijeme, dok po pojmom *informacijski rat* smatraju da je informacija sredstvo ugrožavanja, to jest, informacija je glavno oružje kojim se poduzeća koriste.

Jedan primjer rata za informacije među poslovnim subjektima je primjer iz Kalifornije, kada je tamošnja tvornica likera, Saybrex, optužila brokera da je prevarom od jednog zaposlenika tvornice nabavio kopiju telefonskog računa. U ispisu poziva tvornice bili su nabrojani svi pozivi djelatnika tvornice, među kojima su bili brojevi telefona Saybrexovih potrošača. Telefonski račun je broker navodno proslijedio jednom od Saybrexovih konkurenata, koji je kontaktirao brojeve s ispisa, i štupivši u kontakt sa Saybrexovim potrošačima, sklopio višemilijunske poslove s njima. [Javorović, Bilandžić, 2007, str. 185]

Drugi pak primjer je primjer infromacijskog rata iz 1980. godine, kada je jedna tvrtka iz kalifornije dozvolila časopisu „Business Week“ da objavi novi tehnološki postupak proizvodnje šećera, pretvaranje fruktuznog sirupa u kristale šećera. Tim činom su sve informacije o tom postupku dane svima zainteresiranima na uvid, te je time omogućeno zemljama koje proizvode šećer na tradicionalan način (iz šećerne trske) i izvoze ga, da poboljšaju svoju tehnologiju proizvodnje. Svjetska banka je kreditirala mnoge od takvih tradicionalnih proizvođača, te je odlučeno da će napraviti studiju o utjecaju novog zaslađivača na proizvodnju šećera u odnosu na tradicionalan način, a rezultat je pokazao da nova tehnologija donosi brojne pozitivne efekte. Stoga je Svjetska banka odlučila ukinuti kredite za tradicionalan način proizvodnje šećera. [Javorović, Bilandžić, 2007, str. 185-186].

U prethodnim primjerima navedena je jedna od metoda prikupljanja informacija, a to je korištenje *insidera* za odavanje poslovnih tajni, to jest osobe koja je za određenu naknadu spremna iznevjeriti svoje poduzeće i odati poslovne tajne. Insideri najčešće postanu osobe koje nisu zadovoljne svojom plaćom, te pristaju na dodatan izvor zarade, a imaju pristup tim informacijama koje su željene, ali isto tako insideri mogu biti čak i programeri, inženjeri, izvršni menadžeri, i tako dalje, koji imaju neke osobne razloge davanja povjerljivih informacija van poduzeća. Još jedna metoda često korištena metoda dobivanja informacija je hakiranje, to jest provala u informacijski sustav poduzeća, i to je tehnološki napad, izvediv s bilo koje udaljene lokacije. Trećom vrstom napada zbog dobivanja informacije smatra se fizički napad na osobe koje znaju potrebnu informaciju ili pak krađa primjerice računala, papira i slično. [V.K., 2013].

Za hakiranje kao metodu dobivanja informacija, slažu se mnogi autori, a mnogi često spominju i prisluškivanje telefonskih linija, koja je bila korištena i u povijesti, otkad je izumljen telegraf.

Robinson[[8]](#footnote-9) se djelomično slaže s ostalim autorima, a navodi ove metode, teško prevodljive na hrvatski jezik:

1. *Hacking*
2. *Social Engenineering*
3. *Dumpster Diving*
4. *Whacking*
5. *Phone Ease Dropping*

Robinson hakiranje (*hacking*) smatra najpopularnijom metodom, poprilično jednostavnom, i uvrštava je među tri najbolje metode. Hakiranje dijeli u tri kategorije:

1. Hakiranje sustava, kada haker ima pristup određenom računalu, ali nije admin računala,
2. Daljinsko hakiranje, kada haker napada preko Interneta,
3. Fizički napad, kada haker fizički mora ući u prostoriju i ukrasti potrebno.

Ono što haker može napraviti tijekom fizičkog napada je potražiti u poduzeću neke dokumente gdje pišu lozinke korisnika računala, naći potrebne dokumente u arhivi te ubaciti neki lažni dokument unutra kako bi se prikrio, zatim može ući u sobu sa serverima ili telefonskom centralom kako bi saznao više o sustavu koji se koristi, staviti uređaj za analizu protokola u ožičene ormare kako bi snimao podatke, i tako dalje.

Za *social engineering* Robinson kaže kako je to također vrlo popularna metoda za dobivanje korporativnih informacija. Cilj ove metode je dobiti inače neovlašteni pristup do informacija ili sustava, na način da se prevare ljudi. Primjerice, u razgovoru s osobama pokušava se dovesti do situacije da te osobe priznaju svoje lozinke, odaju neke informacije, i to se uglavnom čini manipuliranjem. Često se već i razgovori s rođacima koriste u takve svrhe. Jedan od standardnih trikova kojim se koriste napadači je slanje maila u ime administratora, to jest napadač se pretvara da je administraotr. Napadači u takvim mailovima navode kako je slanje korisničkog imena i lozinke potrebno za rad nekog važnog sustava, primjerice sustava uprave, te je velika vjerojatnost da će dobiti barem dvije ili tri lozinke, to jest par ljudi će nasjesti na ovaj trik. Također, jedan vrlo čest trik je gledanje preko ramena dok netko upisuje lozinku. Ukoliko i ne vidi cijelu, velika vjerojatnost prilikom stvaranja lozinki je da su lako pamtljive, poput datuma rođenja ili godišnjica, imena djece, i slično.

Dumpster diving, ili u slobodnom prijevodu metoda kopanja po smeću, za Robinsona predstavlja najprljaviji način dobavljanja informacija. Poduzeća ili institucije bacaju smeće negdje na ulici, dakle javnom mjestu, i time to prestaje biti privatno vlasništvo, osim ako je kontejner zaključan ili postoji natpis koji zabranjuje ometanje posjeda. Ono što poduzeća bacaju su razni kalendari, imenik tvrtke, razni dopisi, organizacijske sheme, podaci o godišnjim odmorima, razni priručnici, papiri sa zapisanim dodatnim informacijama, poput lozinki, važnih brojeva telefona i slično, a to je upravno ono što treba konkurentu.

Robinson također kao metodu dohvaćanja informacija predstavlja *whacking*, to jest bezično hakiranje. Haker da bi uspio u naumu uhođenja bežičnih mreža, treba samo dvije stvari: imati pravu vrstu radija i biti u dometu bežične mreže. Uz primjenu 802.11b uređaja lako se dohvati mreža i izvan zgrade poduzeća. Kada se haker konačno domogne bežične mreže, može jednostavno i brzo pristupiti i na žičanu mrežu i na bežičnu, jer podaci koji se šalju preko mreže uglavnom nisu kodirani i zaštićeni. Ukoliko poduzeće nema bežičnu mrežu, haker se može opet poslužiti tehnikom social engineeringa, predstaviti kao domar te tako upasti u poduzeće. Nakon što uđe u poduzeće, vraća se na *whacking* tehniku, tako da ubacuje lažni čvor za bežični pristup, te može izaći van. Nakon što se instalira WAP, bežična pristupna točka, haker je opet u mogućnosti dohvaćati informacije koje treba s daljine.

Još jedna metoda koju navodi Robinson je *phone ease dropping* metoda, a odnosi se na prisluškivanje telefonske linije. Osoba uz pomoć digitalnog uređaja za snimanje može pratiti i liniju faksa, te zabilježavati poslane i primljene podatke. Do podataka poslanih i primljenim faksom se dolazi tako da se snimka pušta na modificiranome Group III ili Group IV faks uređaju, a kopija poruke se tada vrlo lako i točno prikazuje, bez da itko išta zna o krađi podataka. Isto tako, postoji mogućnost da se snime tonovi koji predstavljaju nečiji broj računa i lozinku pomoću kazetofona. Na taj način se može dobiti pristup nečijem računu, primjerice.

Svaki špijun zna u čemu je najbolji, to jest koja od ovih metoda mu je najbliža i najlakše izvediva u bitnom trenutku, ovisi o tome koliko resursa ima za rad, te na taj način odlučuje koju metodu će koristiti. Nisu sve metode uvijek uspješne, niti primjenjive u različitim situacijama.

Nekoliko autora slaže se kako su i računalni virusi jedna od metoda špijuniranja, a najpoznatiji primjer toga je virus „Trojanski konj“ ili popularno zvan „trojanac“, koji je ime dobio prema priči iz grčke povijesti. „Trojanski konj“ zlonamjeran je program koji uvijek dolazi u paketu s još nekim programom, koji se osobi kojoj se šalje prikazuje kao neki drugi program, primjerice igrica, neki zabavan sadržaj u e-mail pošti ili na stranciama s kojih ljudi skidaju aplikacije. Kada osoba nasjedne na virus, instalira se dodatan program za praćenje i neke funkcije su krađa lozinki, PIN-ova, brojeva računa i slično. Često ima i nuspojavu da se automatski šalje drugim osobama u ime osobe koja je nasjela, te time usporava rad računala. [Wikipedija]. Primjer iz Sirije kada je korišten program „Dark Comet“, *remote access trojan* (RAT) program, dodatni programi bili su „Skype Encryption“, lažni program za kriptiranje Skype razgovora, kasnije je bio uveden i „AntiHacker“ koji je bio predstavljen kao program za zaštitu od napada hakera i virusa, a ponekad su slao program pod nazivom „MAC Address Changer“ i predstavljen je kao program koji omogućuje anonimnost na Internetu. Mnogo lažnih programa poslano je i preko Facebook chata i Skype chata. Sirijski lažni programi radili su na način da se zaraženo računalo spajalo na IP adresu Sirijskog telekoma. [Nacionalni CERT, 2012, str. 12-13]

## 3.3. Legalnost postupaka u industrijskoj špijunaži

Većina postupaka u industrijskoj špijunaži smatra se ilegalnim, ali ipak postoje neki legalni načini dobivanja informacija.

### 3.3.1. Legalni postupci

Jedna od legalnih metoda industrijske špijunaže je metoda *dumpster diving*. Njena legalnost se očituje u tome da poduzeća smeće izbace u kontejnere i kante na ulici, gdje se smeće ostavlja kako bi ga odvezle i zbrinule firme koje se bave odvozom i zbrinjavanjem otpada, a kada se smeće ostavi na ulici, više se ne smatra privatnim vlasništvom (osim ako postoji znak poput zabranjenog pristupa ili ako je kontejner zaključan). [Robinson, 2003, str. 6]

Još jedna legalna metoda dobivanja podataka je kupnja tvrtke ili proizvoda čije podatke želimo dobiti. Također, legalan način je i prisiljavanje poduzeća na to da se odreknu svojih tehnologija proizvodnje, primjerice. Zapravo, to bi se moglo nazvati i ucjenom. Kako je legalan način kupnje poduzeća, tako je legalno i partnerstvo s konkuretnim poduzećem, iako je sklopljeno i u svrhu dobivanja potrebnih informacija, ali to konkurent ne zna. Open Source Information (OSI) pruža velik izvor informacija jer sadrži razne novinske članke, godišnja izvješća poduzeća, prijave patenata, razne sudske papire i marketinške informacije. Još jedna legalna metoda prikupljanja informacija je zapošljavanje bivšeg radnika konkurenta, koji tada više nije obavezan čuvati poslovnu tajnu ili je čak rado i širi zbog nezadovoljstva starim poduzećem, iako je češći slučaj da takve osobe iz poštovanja ne žele otkriti informacije, ali u novo poduzeće donose svoje znanje i vještine, koje su vjerojatno stekli na starom radnom mjestu. Još jedan od vrlo popularnih načina dobivanja informacija je posjećivanje sajmova poduzeća na kojima netko glumi zainteresiranu osobu za to poduzeće, kupca, istraživača ili slično. Te osobe su većinom vrlo dobro uvježbane da znaju točno što treba reći, i u kojem trenutku, da bi izvukle informacije. Ako se radi o špijuniranju stranog poduzeća, često se kontaktiraju domoroci iz te zemlje koji rade u stranom konkurentskom poduzeću. Zbog privrženosti domovini, vrlo često i otkriju više nego bi smjeli. [Winkler, str. 2]

### 3.3.2. Ilegalni postupci

Ilegalnih postupaka je puno više nego legalnih, a i neki legalni su blizu granice do ilegalnih. Metoda *insidera* zakonom je kažnjiva, to jest krađa informacija i odavanje nekome u zamjenu za novac ili neku drugu uslugu. U velikim poduzećima najčešće se ljude zapošljava dugoročno, što pridonosi pojavi *insidera*, a i veličina tvrke može im olakšati da što manje upadljivo kradu podatke, ako znaju kako se prikriti. Provale u zgradu poduzeća su kažnjivi postupci, makar se radilo i o prolasku kroz otključana vrata zgrade pa tek potom pretraživanja ormara, ladica i krađi nekih dokumenata. Isto vrijedi i za upadanje u računalni sustav*. Dumpster diving* metodu ovaj autor navodi kao ilegalnu, ali to ovisi je li smeće izvan zgrade i ima li znaka privatnog posjeda ukoliko je izvan, te kako je formuliran zakon u određenoj državi. Prisluškivanje, hakiranje i whacking su također ilegalne metode špijuniranja. [Winkler, str. 3-4]

Zakon je drugačiji u svakoj državi, ali uglavnom su suglasni oko legalnosti špijunaže, zbog etičkih pitanja. U Republici Hrvatskoj, kazneni zakon propisuje zatvorske kazne na određeno vrijeme za određene postupke. Kazne su propisane kroz više desetaka članaka, u različitim glavama zakona. Glava dvadeset peta (XXV.) Kaznena djela (pokušaj ili uspješna činidba) protiv računalnih sustava, programa i podataka propisuje kazne primjerice za hakiranje, *whacking*, pristupanje računalima i sustavima za koje se nema ovlaštenje, onemogućavanje rada sustava, krivotvorenje podataka ili brisanje podataka, neovlašteno presretanje računalnih podataka i tako dalje. Također, prema drugima člancima istog zakona, kažnjavaju se djela neovlaštenog zvučnog ili slikovnog snimanja, neovlašteno otkrivanje poslovne tajne, krađa imovine (u ovom slučaju dokumenata s vrijednim infomacijama), prijevare, primanje i davanje mita (primjerice kod *insidera*), zloupotreba ovlaštenih informacija ili odavanje i neovlašteno pribavljanje poslovne tajne. Prema zakonu Republike Hrvatske, svi postupci industrijske špijunaže su kažnjivi, neki u manjoj mjeri, neki u većoj. [Hrvatski Sabor, Kazneni zakon, NN 125/11 i 144/12 ]

## 3.4. Tehnička podrška

Čuljak[[9]](#footnote-10) u svom radu kaže kako sve velike države, ukoliko raspolažu špijunskim satelitima, mogu snimati i pratiti sve telefonske komunikacije, primjerice pozive, faks, čak i e-mail, i to bilo gdje u svijetu, ne samo na teritoriju svoje države. Kabel koji spaja slušalicu telefona s aparatom zrači dovoljno jako da bi se snimio razgovor pomoću satelita. Sve snimke se sortiraju prema brojevima koji zovu ili su bili zvani, prema vremenu razgovora, jeziku na kojem se razgovaralo i po boji glasa govornika, što primjerice pokazuje radi li se o muškoj ili ženskoj osobi. Kada su prikupljene i sortirane sve snimke, daju se dalje analitičarima na provjeru i analizu.

Čuljak također navodi kako se mobilni telefoni mogu prisluškivati i bez skupe i posebne opreme, koja je potrebna za prisluškivanje telefona. Također, mobiteli se mogu lako i prostorno locirati. Veće organizacije si mogu priuštiti da se prisluškivanje obavlja preko mobitela čak i onda kada je aparat isključen, na način da nazovu broj aparata i prije nego stisnu posljednju znamenku broja kojeg zovu, puštaju posebnu šifru koja uključuje mikrofon. Na taj način mobitel postaje sredstvo koje prenosi sve zvukove iz okoline, čak do petnaest metara oko sebe.

Kompjutorske podatke koji se prikazuju preko ekrana moguće je snimiti s nekoliko metara udaljenosti, piše Čuljak.

## Zaštita podataka

Poduzećima bi trebalo biti u interesu podatke za koje znaju da su na meti konkurentima nekako zaštiti. Zbog toga je dobro da se znaju slabosti metoda i tehničke podrške špijunaži. U prethodno navedenom poglavlju, spomenuto je prisluškivanje telefonskih linija pomoću satelita. Od toga se poduzeće može zaštititi tako da se telefonski aparati nalaze u prostoriji koja je Faradejev kavez, te je važno da su električni kablovi i spojevi kroz koje prolaze signali zakopani što dublje po zemljom. Ovakva zaštita jedino ne pomaže ako špijuni imaju dogovor s telefonskim kompanijama da im ustupe sve što treba. Što se tiče mobilne mreže, jedina zaštita je rastaviti mobitel, to je izvaditi mu bateriju ili ga obložiti aluminijskom folijom. Vezano uz zaštitu kompjutora, dobro je paziti kako su uredi složeni, može li netko gledati preko ramena osobi i tako dobiti lozinke, i također, nikakva zaštita ne vrijedi ako špijuni imaju dogovore s proizvođačima operacijskih sustava, jer tada špijuni mogu lako, samo sa spajanjem na Internet, preuzeti sve podatke koji im trebaju. Pomoću posebnog programa mogu i zaobići sve šifre koje i trebaju za pristup računalima. [Čuljak]

Poznati i jaki računalni virusi imali su i svrhu pouke – podigli su računalnu savjest. Mnoge organizacije dobile su uvid u to kako što bolje zaštititi svoje informacijske sustave. Primjetilo se da je glavni razlog nezaštićenosti bio nedostatak osnovnih sigurnosnih principa. Veliki nedostatak našao se i u javnoj objavi programskog koda, jer je velika mogućnost da će se iskoristiti u takve kriminalne svrhe špijunaže i sabotaže. [Nacionalni CERT, 2012, str. 17]

Winkler[[10]](#footnote-11) navodi kako se svako poduzeće može zaštititi na četiri načina, i time čak učini prevenciju špijunaži, a to su:

1. Tehnička zaštita
2. Operativna sigurnost
3. Fizička zaštita
4. Zaštita osoblja

Za postizanje tehničke sigurnosti važno je imati razne protumjere. Zaštita tehničkih alata u poduzeću stvara povjerljivost, integritet i dostupnost računalnih sustava i mreža. Uz malo truda može se postići zaštićenost komunikacijskih kanala, a time i informacija. Operativna sigurnost odnosi se na procese poduzeća, a koji bi mogli ugroziti informacije u netehničkom smislu. Primjerice, poduzeće može postaviti pravila o znanju informacija, odrediti tko smije koliko znati, ili pak se mogu ograničiti korištenja komunikacijskih kanala. Također, operativna sigurnost uključuje i politiku sigurnosti vezanu uz dobavljače ili vanjske suradnike, njih se dodatno provjerava. Važno je i iskomunicirati sa svim zaposlenicima o važnosti informacija i posljedicama ako nekome nešto otkriju, objasniti kako se što bolje zaštiti te raditi na tome da zaštita informacija postane dio kulture poduzeća. Pošto se velik broj krađa informacija događa i zbog fizičkih upada stranih osoba u poduzeće, treba raditi i na fizičkoj sigurnosti poduzeća. Prvenstveno treba postaviti dobar sustav kontroliranja ulaska u zgradu poduzeća i primjerice neke od bitnih proizvodnih pogona i slično, ali treba i zaposlenicima onemogućiti pristup nekim podacima. Savjet je i da zaposlenici nose oznake s imenom i pozicijom u poduzeću na majicama, košuljama ili radnoj odjeći, a isto tako i vanjski suradnici, posjetitelji trebaju dobiti oznaku prilikom ulaska u zgradu. Te oznake imaju smisla kada zaposlenici ponekad i pogledaju na tuđe oznake, pa vide nose li ispravnu, to jest svoju. Često se na takve oznake stavlja i slika osobe kako bi je bilo lakše povezati s imenom. Još jedan način fizičke zaštite je kontrola smeća, to jest trebalo bi važne dokumente ili spaliti ili uništiti na neki drugi način. Tijekom pauza, pametno je računalo zaključati lozinkom, i paziti da se te lozinke ne nalaze na nekom papiriću u blizini računala. Korisno je takve lozinke s vremena na vrijeme i promijeniti. Sve papire koji na sebi imaju povjerljive informacije trebalo bi držati u zaključanim ladicama ili ormarima i negdje dobro sakriti ključ od brave. Zaštita osoblja odnosi se na provjeravanje tko od zaposlenika ima pristup kojim informacijama te postavljanje pravila kojim informacijama i na koji način bi smio pristupiti. Mnoga poduzeća nisu svjesna da podatke mogu krasti domari, zaštitari ili čistačice. Administrativno osoblje moralo bi surađivati s odjelom za ljudske resurse kako bi saznali kada netko od zaspolenika dobije otkaz, da se njegov korisnički račun za korištenje računala odmah pobriše. [Winkler, str. 5-6]

# 4. Povezanost upravljanja znanjem sa industrijskom špijunažom

# Upravljanje znanjem ili *knowledge management* je sastavni dio svakog poduzeća. Kako navode Lee i Rosenbaum, upravljanje znanjem sadrži ključne informacije, ključne igrače, odnose, strateške ciljeve, operativne principe i mehanizme, i tako dalje, te misle kako je upravljanje znanjem zapravo alat kojim poduzeće špijunira samo sebe, u pozitivnom smislu. Može se vidjeti tko je povezan i aktivan, koje su vrijednosti tvrtke, tko doprinosi, tko surađuje, tko ima informacije i slično, a to su sve vrijedna saznanja za tvrtku, ali i za njenog neprijatelja. Upravljanje znanjem tvrtku čini više povezanom, življom i učinkovitijom. Pošto sadrže i podatke o klijentima, planove poduzeća, poslovne tajne, cjenovnike i slično, često se takve platforme nalaze na metama špijuna i hakera. Lee i Rosenbaum također govore kako su *knowledge management* sustavi i *anti knowledge management* sustavi. To objašnjavaju time što se vide praznine i greške u znanju i razumijevanju onih koji ih koriste, a to svakako dodatno koristi špijunima, pogotovo ako imaju informacije i znanja koji mogu nadopuniti te praznine. [Lee, Rosenbaum, 2003.]

Colibasanu spominje pojam *competitive intelligence*, alat za proces donošenja odluka koji pomaže dati odgovore na ključna pitanja. Taj alat je najviše vezan uz strateški menadžment, jer je usredotočen na postavljanje i rješavanje hipoteze, te podržava održivi razvoj tvrtke u promjenjivom i nestabilnom okruženju. *Competitive intelligence* je logičan proces testiranja, provjera valjanosti pretpostavke ili hipoteze, te rješavanja ključnih poslovnih problema. Proces se sastoji od ključnih koraka, a to su identificiranje potreba za informacijama i znanjem u poduzeću, prikupljanje informacija, analiziranje te sinteza prikupljenih podataka, i na kraju objava rezultata. Ovaj alat pomaže poduzeću i time što prati što se događa s konkurentskim poduzećima, što rade i kakva im je pozicija na tržištu, te prati promjene poslovnog okruženja. Autorica špijunažu povezuje s pojmom *competitive intelligence* u jednoj zajedničkoj stvari, a to je stjecanje i zadržavanje ili održavanje konkurentske prednosti. Razlika koju navodi je da *competitive intelligence* alat stvara stabilno okruženje za donešenje poslovnih odluka, dok se špijunažom samo postiže to da se pribave informacije, ali ne da se i od njih napravi znanje potrebno poduzeću. Isto tako, te informacije mogu biti korisne vrlo kratko, ukoliko ih špijunska strana ne obradi brzo i ne iskoristi prije onih kojima su ih uzeli. Može postojati mogućnost da i špijuni koriste *competitive intelligence* sustave. Još jedna velika razlika koju navodi autorica je ta da je korištenje *competitive intelligence* sustava etički ispravno, dok je špijunaža neetično ponašanje, te zakonski kažnjivo. [Colibasanu]

Korištenje *competitive intelligence* sustava, *business inteligence* sustava ili *knowledge managemen*t sustava poduzeće dovodi na metu špijunima, te se poduzeća moraju na neki način zaštititi od mogućih napada. Alstete je u New Yorku 2002. godine proveo istraživanje u kojem je ispitao svijest i percepciju zaposlenika o krađi i zaštiti informacija. Proveo je to na način da ih je ispitivao o sigurnosti imovine znanja, to jest informacija, ne samo u okolnostima promjena nakon napada 11.09.2001., nego u općenitom smislu povećanja sigurnosti u poduzećima u kojima rade. Sudionici su zaposlenici u srednjim i velikim poduzećima. Rezultat koji je dobiven ispitivanjem raspoređuje se u četiri kategorije percepcije zaposlenika:

1. zaposlenici su svjesni vrijednosti upravljanja znanjem,
2. zaposlenici nisu svjesni vrijednosti upravljanja znanjem,
3. nema povećanja sigurnosti,
4. sigurnost je povećana.

Ova studija je pokazala kako su mnogi menadžeri uvjereni da njihova tvrtka ima barem osnovno shvaćanje o vrijednosti upravljanja znanjem te da imaju neke mjere zaštite, ali nedovoljno se bave planiranjem većih mjera zaštite. Kako bi se što učinkovitije zaštitile, tvrtke moraju biti svjesne vrijednosti svojih informacija i znanja, te tek tada mogu planirati što treba štititi i do koje razine sigurnosti treba postaviti zaštitu.

[Alstete, 2003]

# 5. Primjeri industrijskih špijunaža

## 5.1. Renault

## U Renaultu se još prije nekoliko godina počela javljati sumnja za industrijsku špijunažu. Tada su radili na istraživanjima oko električnih vozila, ulagali su u njih, a u isto vrijeme isto to je radio ni japanski Nissan. Počele su stizati anonimne bilješke o tehnologijama električnih automobila. Trojica zaposlenika, sva trojica na visokopozicioniranim direktorskim mjestima, našla su se pod sumnjom da su za velik iznos mita prodali konukrenciji povjerljive informacije koje Renault ima, te su dobili otkaz, ali dana im je mogućnost da se izjasne o optužbama prije nego se išta poduzelo. Odluka o tome da ovi zaposlenici dobiju otkaz, bila je zbog zaštite strateških, intelektualnih i tehnoloških planova koje je Renualt imao. Renault se javno ispričao toj trojici zaposlenika kako bi vratili ugled poduzeća.

Još jedan bitan dio cijele te afere je da je Patric Pelata, glavni operativni direktor Renaulta i često spominjan kao jedan od najboljih stratega proizvodnje, bio dio tima kojeg je predvodio Carlos Ghosn nakon što je Renualt kupio kontrolni udio u japanskom poduzeću. Nakon što je uspio Nissan ponovno vratiti na bolje mjesto na tržištu, vraća se u Pariz kao desna ruka Carlosa Ghosna, zatim vodi marketinšku strategiju probijanja u Renaultu, te nakon toga postaje glavni operativni direktor. Pelata je bio zadužen za dio istrage, ali kaže kako nije imao razloga posumnjati u valjanost optužbi prema trojici zaposlenika.

Francuska vlada, koja je vlasnik dijela dionica Renaulta, shvatila je da su na meti špijunaže, to jest da njihovi menadžeri surađuju s konkurentima, te su pozvali Ghosna da podnese ostavku i bili su ljuti što ih nitko iz Ranaulta nije odmah obavijestio o nastaloj situaciji. Tada je istupio Pelata, rekao je kako je vlada pozvala menadžere na odgovorsnot, te bi ako Ghosn da ostavku moglo propasti udruženje Renault-Nissan. Vlada je odustala od Ghosnove ostavke, ali su i dalje zahtjevali da netko preuzme odgovornost, tada je Pelata dao ostavku na poziciji glavnog operativnog direktora.

U nekim člancima spominje se kako su ova trojica zaposlenika bila krivo optužena, te su im ponudili da se vrate na svoja radna mjesta, ali nisu željeli prihvatiti tu ponudu iz razloga što se nisu htjeli vratiti u neprijateljski nastrojenu radnu okolinu.

Posljedice za Renault u ovom događaju mogle su biti ozbiljne. Osim gubljenja ugleda, imali su skandal vezan uz poduzeće, umiješala se politika, mediji, ostale industrije, obavještajne službe, u igri je bilo puno novca te brojne dezinformacije.

U ovom primjeru korištena je metoda *insidera* te davanje mita kako bi se dobile informacije. Također, došlo je i do širenja dezinformacija.

[Rechtin M, 2013; Schofield, H, 2011; D.Ko., 2011; Nepoznat autor, 2011, republikainfo]

Smatram da je do industrijske špijunaže u ovom primjeru došlo zbog natjecanja poduzeća u inovacijama. Jedno poduzeće ima ideju, istražuje i ulaže novac, a drugom poduzeću najlakše bi bilo uzeti nečije istraživanje i doraditi ga, uzeti si zasluge za inovativan i patentiran proizvod, te tako zaraditi velik novac i imati monopol na tržištu. Špijunažu je teško izbjeći, politika i kultura poduzeća bi trebala biti takva da se ne podliježe špijunaži i mitu, ali i da se zapošljavaju kreativni i kvalitetni radnici, koji će se boriti za položaj i profit svog poduzeća na pošten način.

## 5.2. McLaren protiv Ferrarija

## Poznati primjer vezan uz industrijsku špijunažu dogodio se 2007. godine, prije utrke u Mađarskoj, to jest, tada je i javnost upoznata s time. Uz ovaj događaj dogodilo se i puno spletki povezanih sa špijunažom.

Fernando Alonso bio je vozač formule u Renaultu, a zatim je prešao u tim McLaren, gdje je zbog toga što je bio višestruki prvak Fomrule 1, dobio prvo mjesto u timu, a odmah iza njega nalazio se Lewis Hamilton, koji je postizao sve bolje i bolje rezultate. Do afere je došlo najprije zbog toga što su dva tima, McLaren i Ferrari imali izvanredne vozače, a za Ferrari su vozili Raikkonen i Massa, te je za Ferrari osvojena Velika nagrada Monaka. Nakon osvajanja te nagrade, u Ferrarijevim bolidima nađen je bijeli prah te se posumnjalo na sabotažu.

Ono što je uslijedilo je saznjanje da je glavni projektant McLarena, Mike Coughlan, dobio od Nigela Stepneyja, Ferrarijeva inženjera, kompletan nacrt konstrukcije talijanskog bolida kojeg su talijani planirali napraviti. Dokumentacija konstrukcije imala je oko 780 stranica, a sadržavala je detaljne tehničke nacrte, skice, opise, pojedinosti oko održavanja i pripreme za utrke. Coughlan je poslao svoju suprugu u kopiraonu da umnoži dokumentaciju, a radnik u kopiraoni napravio je dodatnu kopiju kako bi imao dokaz kada to bude prijavio Ferrariju, što je i učinio. Coughlan je policiji priznao da je to dobio od Stepneyja, a vodstvo McLarena se ogradilo od toga pošto nisu znali što Coughlan radi. I Stepney i Coughlan su dobili otkaz, McLaren nije kažnjen jer nije bilo dokaza da su dobivenu dokumentaciju koristili. Međunarodna automobilistička federacija (FIA) također je prihvatila da je krađa dokumentacije bila individualni čin, dok se eventualno ne pokažu nove činjenice. Cijela priča nije se dalje širila niti razbukltavala, te se činilo kako je ova afera gotova, no nije bilo tako.

Tada na red dolazi Alonso, koji je zbog straha za svoju poziciju u McLarenu postupio nekorektno prema timskom kolegi, Hamiltonu. Na kvalifikacijskom treningu, natjecao se s Hamiltonom tko će imati bolje vrijeme, kako bi dobio najbolje mjesto za startnu poziciju na utrci. Hamilton je imao bolje vrijeme i kada je ušao u boks, za njim je ušao i Alonso koji je stao na izlaz iz boksa, te je time Hamiltona spriječio da odvozi još jedan krug. Za taj Alonsov trik doznali su suci koji su ga kaznili tako da nije dobio prvo startno mjesto, nego šesto, a Hamilton je zahvaljujući tom prvom startnom mjestu pobijedio na utrci. Dennis, šef McLarena se razbijesnio na Alonsa i njegovo nekorektno ponašanje te mu je zaprijetio sankcijama ako se to ponovi. Alonso je vratio prijetnjom da će otkriti u javnost kako su i vozači znali za dokument iz Ferrarija i pokazati e-mailove koje je razmjenjivao s talijanskim rezervnim vozačem Pedrom de la Rosom. Dennis ga nije shvatio ozbiljno, ali je u panici otišao do FIA-e, te predsjedniku Mosleyju ispriča što mu je Alonso rekao i kako misli da blefira. Ferrari je cijelo vrijeme bio za to da se McLaren kazni, argumentiravši to time da će javnost shvatiti kako FIA podržava špijuniranje. Iako je dokazano da McLaren nije koristio dokumentaciju, ali nije isključeno da im bude korisna u budućnosti. Kažnjen je samo McLaren, sa 100 milijuna dolara, dok vozači nisu kažnjeni.

U ovom primjeru može se vidjeti kako etika ne postoji ni u sportskim natjecanjima, vjerojatno zato što se u Formuli 1 radi o velikim svotama novca pa svatko gleda samo na sebe i svoj benefit. Posljedice za McLaren bile su velike – osim novca, izgubili su i povjerenje u svog vozača, morali su budno paziti na njega jer je i dalje odbijao timsku suradnju, nisu ga smjeli ni kazniti jer ga je FIA štitila. Ferrari je pak izgubio na tome što je vrijedan dokument podijeljen s McLarenom.

Metoda kojoma su se koristili Coughlan i Nigel je primanje, to jest odavanje poslovnih tajni, to jest Nigel je ovdje imao ulogu *insidera*, koji je dobio veliku novčanu naknadu. Također, mailovi koje su razmjenjivali Alonso i de la Pedro pripadaju u industrijsku špijunažu, a radi se o širenju informacija i dezinformacija, te kasnijoj ucjeni. [Mihovilović, 2007; Collantine, 2007]

Smatram da je do ovog incidenta došlo iz više razloga. Najveći razlozi su osobna pohlepa, pohlepa u ime tima i velik novac koji se vrti u tom sportu. Također, razlog je i ljudska ljubomora i želja za prvim mjestom koja je prekršila i etička pitanja unutar tima. Nekažnjavanje Hamiltona kao člana tima koji sabotira ostale vozače u timu bila je politička odluka, a time su se spriječili veći incidenti u medijima. Ovaj događaj se mogao izbjeći na sličan način kao u prethodnom primjeru, poštenim članovima tima koji rade za boljitak svog tima na pošten način, a ne krađom i podmićivanjem. Drugi dio priče, gdje je Hamilton sabotirao svog timskog kolegu, teško da se mogao spriječiti, jer je ljudsku pohlepu teže kontrolirati u uvjetima gdje se član tima osjeća zakinuto i željno osvete kako bi bio prvi.

## 5.3. Ericson

Još jedan primjer koji je dosegao i pitanje nacionalne sigurnosti je Ericson. Ericson svi znaju po tome što proizvode mobilne uređaje, ali rijetko tko zna da se bave također razvojem i proizvodnjom velo sofisticiranog radara i raketnih sustava za navođenje švedskog borbenog zrakoplova Gripen, glavnog napadačkog zrakoplova. Dvojica zaposlenika su zajedno s jednim bivšim zaposlenikom optuženi da su odali informacije stranoj obavještajnoj službi tako što su dali izvan tvrtke tajne dokumente. Ti zaposlenici čak nisu bili ni na višim menadžerskim pozicijama. Slučaj je postao puno ozbiljniji kada se otkrilo da u tome sudjeluju i dva ruska diplomata, koji su nakon toga dobili izgon iz države. Ericson nije želio veliku medijsku pompu oko ovog događaja, shvatili su da su meta ruske obavještajne službe. Posljedice za Ericson mogle su biti gubitak ugleda i vrijednost ukradenih informacija. U ovom slučaju, metoda je ista kao u prethodna dva primjera, a to je korištenje *insidera* uz primanje mita za davanje poslovnih tajni. [Crane, 2003, str.6-7]

U ovom primjeru do industrijske špijunaže došlo je zbog osobne pohlepe i moguće želje za dokazivanjem samima sebi ili osveti nadređenima, ukoliko se radnici nisu dobro osjećali na radnom mjestu. Ovakav incident mogao se djelomično spriječiti dobrom radnom klimom, poštenim plaćama radnika, eventualno dobrom selekcijom ljudi prilikom zapošljavanja, ali se tada nije moglo znati sa sigurnošću jesu li radnici podložni mitu i korupciji, jer na testiranjima za posao mnogo ljudi zna kako to sakriti, ili su se možda promijenili u međuvremenu, a kako je društvo primorano dobro zarađivati da bi preživjeli, uzimanje mita se ljudima čini kao sasvim pošteno zarađen novac.

## 5.4. Hewlett-Packard špijunirao je sam sebe

Odbor Hewlett-Packarda (HP), poznatog poduzeća u svijetu po proizvodnji osobnih računala i pisača, odlučio je da će špijunirati „sami sebe“ i tako tako da se budu prisluškivale linije i nadgledali mailovi direktora, novinara i zaposlenika, ne bi li se otkrilo šire li možda podatke koje ni bi smjeli izvan poduzeća. Unajmljeni su istražitelji koji su nadzirali cijelo poduzeće. Poduzeće je investiralo tadašnju tehničku opermu i mnogo novca u nabavu nove opreme, i plaćanje istraživateljima. Razlog zašto je to pokrenuto je puštanje informacija iz poduzeća u medije, primjerice interne diskusije. Istraživatelji su koristili metodu „pretexting“, kojom su imali ponovljene pozive na telefone kompanije, i razgovarali su s njima kao s ciljanim individualncem dok nisu uspjeli dobiti informacije o poduzeću. Isto tako, provjeravalo se mail, chat i slično koji su koristili zaposlenici.

Tadašnja predsjednica odbora, Patricia Dunn, koja je odobrila ovu akciju špijuniranja, dobila je otkaz, ali otkaz su dobili još neki dužnosnici, a HP je pristao na novčane izdatke kako bi se istraga završila, za podmirenje troškova tužbi, i slično.

Ova metoda je ilegalna, jer zaposlenici su snimani bez njihova odobrenja, što je kažnjivo i po našem zakonu. [Martin, 2006; Nepoznat autor, 2011, Business Week]

Smatram da je vodstvo HP-a bilo paranoično zbog toga što je u medije poslan dio internih informacija i smatrali su da moraju nekako izaći s tim na kraj tako da špijuniraju svoje radnike. Prekršili su ljudsko pravo da budu obavješteni da su pod nadzorom. Ovo se moglo riješiti na puno drugačiji i manje rigozoran i jeftiniji način. Vodstvo je moglo razgovarati sa svim radnicima iz svih odjela, upozoriti ih na prekršaj davanja internih informacija i reći da se nadalje sve bude snimalo i pratilo, to bi radnike vjerojatno zastrašilo, ako bi to izveli autoritativno. Nikoga ne bi odmah osobno optužili i napali. A onda su nakon toga mogli uvesti snimanje i praćenje, iako bi tada postojala mogućnost da se radnici koji su davali informacije pažljivije ponašaju i nađu način kako da informacije distribuiraju u javnost. Također, smatram da se ovo moglo u potpunosti izbjeći tako da je poduzeće od početka imalo jasna očekivanja od radnika vezano uz davanje informacija, što se smije, a što ne smije, te propisane mjere kažnjavanja takvih radnika. Kultura poduzeća uvelike može utjecati na takva događanja.

## 5.5. Hakerski napad na račune poduzeća u RH

Nakon tri primjera s metodom insidera, slijedi jedan primjer iz Republike Hrvatske, i radi se o hakerskom napadu na bankovne račune poduzeća. Najugroženiji su bili poduzeća i građani koji koriste internet bankarstvo preko USB-a, ali građani nisu bili glavna meta hakera.

Hakeri su birali vrijeme pred kraj radnog vremena tvrtke, jer je tada najmanja vjerojatnost da se provjerava promet računa, i imali su jednu šansu po poduzeću za prebaciti veći iznos novca, ali opet ne prevelik, to jest ne veći od onoga što tvrtke inače isplaćuju, kako ne bi izazvali sumnju. Ovakav način krađe novca najčešće počinje tako što netko u poduzeću pokupi virus koji dohvaća lozinke, PIN-ove i slične podatke potrebne za ulaz u internet bankarstvo, a zatim se vrši prebacivanje novca na neki drugi račun. U ovom slučaju nisu napadnute banke, nego direktno sustavi klijenata banaka, a problem je u tome što USB za internet bankarstvo osoba koja ima ovlaštenja nad njime ostavlja stalno uključenog u računalo, i time daje mogućnost hakerima da napadnu sustav. Transakcije s računa, to jest korištenje aplikacije internet bankarstva uopće nije moguće ako USB nije uključen u računalo, stoga su se poduzeća mogla zaštiti, a vjerojatno su izvukli pouku iz ovog slučaja. S računa poduzeća od početka ove godine ukradeno je ukupno oko dva milijuna kuna, dok su banke oko dvanaest milijuna kuna uspjele vratiti na račune poduzeća. Hakeri znaju da bankama ako otkriju sumnjivu transakciju treba 24 sata da vrate novac na račun s kojeg je poslan novac, a postupak povrata novca nakon tog vremena je dug postupak, te ovisi o kaznenom postupku za čije se rješenje može čekati i više godina, dok se ne otkrije tko je ukrao novac.

U ovom slučaju korišten je hakerski napad, posljedice su financijske prirode za poduzeća s čijih računa je novac otuđen. Mjere zaštite koje poduzeća mogu učiniti je pratiti promet računa u određenim intervalima, te prijaviti banci svaku sumnjivu transakciju, i paziti da kada se internet bankarstvo ne koristi, da se USB i fizički isključi iz računala, jer nije dovoljno samo se odjaviti iz aplikacije. Također, preporuka poduzećima je da ulože u antivirusni program i da ga redovito ažuriraju. [Kavain, 2014]

U ovom primjeru razlog krađe je pohlepa i želja za bogatstvom, te je iskorišteno znanje koje hakeri imaju. Ovo se moglo djelomično spriječiti edukacijom ljudi o tome kako dolazi do hakerskih napada, što sve može biti napadnuto, te kako se zaštititi. Isto tako, poduzeća bi morala na raditi na očekivanjima prema radnicima da budu odgovorni prema poduzeću u kojem rade, te da se USB-ovi, i ostali priključci obavezno isključuju iz računala čim se završi s njihovom upotrebom. Problem je i što u većini poduzeća rade ljudi iznad 40 godina koji se ne teže snalaze s tehnologijom i ne zanima ih pa nisu voljni ni učiti ni o prednostima, a ni nedostacima tehnologije. Također, banke su mogle djelomično to spriječiti, također edukacijama o tome što se najlakše može hakirati, te u skladu s time napraviti tokene ili čitače kartica za internet bankarstvo, koji se uopće ne moraju fizički uključiti u računalo.

## 5.6. Sony PlayStation Network

Velika krađa osobnih informacija koja se dogodila 2011. godine, pogodila je više od 77 milijuna korisnika Sonyevog PlayStation Neworka, točnije pretplatnike i korisnike Qriocity streaming usluge na kojoj korisnici preuzimaju i igraju igrice jedni protiv drugih. Ukradeni su osobni podaci, poput imena, datuma rođenja, adrese, brojeva telefona, mail adresa, i podaci za prijavu na mrežu. Velika je mogućnost da su uzeti i podaci o brojevima kreditnih kartica, te se dogovorila suradnja s bankama da oštećenim korisnicima izdaju nove bankovne kartice. Korisnike se pozvalo na oprez zbog zaštite ostalih društvenih mreža, ili bilo kojih aplikacija za koje su imali iste ili slične lozinke, te da opreznije prate promjene na računima i ako uvide nešto sumnjivo da odmah to prijave banci.

Posljedice ovog hakerskog napada za Sony bile su velik gubitak povjerenja korisnika, koji su i zahtjevali neke usluge kasnije, zatim mreža nije radila oko mjesec dana, te je trebalo nadoknaditi taj gubitak, financijski, a i tvrtka je izgubila na ugledu. Razlog zašto su hakeri napali baš Sony PlayStation Network se samo nagađaju, a pretpostavlja se da su trebali podatke o velikom broju ljudi s jednog mjesta ili da je bila sabotaža Sony-a u pitanju. [Poulter, 2011; Milian, 2011]

Za ovaj primjer teško je reći što bi mogao biti razlog, ja smatram da je razlog bila potreba za velikim brojem informacija o ljudima kako bi im se kasnije mogla slati spam pošta. Ti podaci potrebni su agencijama za anketiranje, marketinškim kućama i tako dalje, pa je moguće da je netko platio hakerima da to učini za njihovo poduzeće. Malo manje vjerojatno, ali isto moguće je da je ljudska dosada u pitanju i samodokazivanje, ili samo mržnja prema Sonyju i želja za sabotiranjem tvrtke. Ne znam je li se ovo moglo spriječiti, vjerujem da Sony ima veliku zaštitu na svojim serverima, ali očito nedovoljnu ili zastarjelu.

## 5.7. Farmaceutske kuće koriste NSA-u da bi dobile podatke

# U Sjedinjenim Američkim Državama nalazi se NSA, to jest National Security Administration, koja je jedna od tehnički najbolje opremljenih obavještajnih službi. Unajmile su je i farmaceutske trvtke, kojima je cilj prodati što više svojih proizvoda za koje ulažu mnogo novca, što u istraživanje, što u razvoj. Jedan od primjera je što je NSA unajmljena kako bi pratila podatke na Internetu oko briga roditelja i nepovjerenja u cjepiva za djecu. Roditelji žele najbolje svojoj djeci, tako i istražuju što više mogu oko bilo kojih stvari koje se tiču djeteta. Tako se može naći podatak kako se u cjepiva stavljaju virusi koji su uzgojeni na bubrezima majmuna, mišjim mozgovima, uzgojeni na fetalnom tkivu pobačenih fetusa, i tako dalje, a nakon takvih informacija, roditelji sigurno ne žele da se tekućina s takvim virusima ubrizga u krvotok djeteta. Mnogi roditelji nisu ni svjesni što cjepiva sadržavaju i kako djeluju. Doktori u ovome ne igraju nikakvu ulogu smirivanja roditelja, jer su potkupljeni od strane farmaceutskih kuća. Na ovom slučaju bila je angažirana i tvrtka Luminoso, koja ima softvere za analizu teksta, te je zajedno s NSA-om tražila ono što roditelji čitaju, objavljuju na forumima i društevnim mrežama, a tiče se zabrinutosti oko cjepiva. Farmaceutske kuće željele su podatke o tome što točno demotivira roditelje kako bi mogle razraditi marketinšku strategiju za poboljšanje prodaje cjepiva, i kako bi roditeljima smanjili brigu.

Ono što je kod ovog slučaja upitno je je li ova metoda snimanja legalna ili nije. Posljedice koje je korištenje ovakvog praćenja moglo izazvati, su to da farmaceuti dobiju željene podatke, a za korisnike interneta taj tren nije bilo opasnosti. Posljedice za roditelje, to jest djecu se mogu vidjeti tek kasnije, kada farmaceuti dovrše svoje marketinške strategije. [Aufderheide, 2013]

U ovom primjeru jasan je razlog, a to je želja za većom prodajom cjepiva i zaradom, a s idejom da se roditelje „educira“ o tome kako cjepiva nisu opasna i smanje im se briga i sumnja u cjepiva i njihove posljedice. Postoje brojne priče o teorijama zavjere farmaceutskih tvrtki i američkih vlasti o želji za vladanjem i kontroliranjem ljudi, a to postižu i cjepivima, pa oni koji vjeruju u te teorije smatraju da je i to razlog za praćenje informacija na internetu. Ova špijunaža se nije mogla spriječiti, roditelje nitko ne može natjerati da povjeruju doktorima, i informacije najčešće traže na internetu, gdje postoje i točne i netočne informacije, a farmaceutske kuće samo iskorištavaju resurse koje mogu.

# 6. Zaključak

# Pojam *industrijska špijunaža* poprilično je teška jasno i jednoznačno definirati. Počevši od toga da jedinstvena definicija ne postoji, tako ne postoje niti jasno pobrojani ciljevi, motivacija, metode i strategije, posljedice ili načini kako koristiti tehnologiju i zaštititi poduzeće od mogućih napada špijuna. Mnogi još smatraju da je obavještajna služba isto što i industrijska špijunaža, ili da je gopodarska špijunaža ili politička špijunaža isti pojam, slični su, ali razlike su male.

# U današnje vrijeme trčanja za profitom i probijanjem na tržište, sasvim je jasno zašto industrijska špijunaža još uvijek postoji. Čovjek je od davnina težio istome – biti najbolji u nečemu, imati najviše, te se koristi svim mogućim sredstvima da bi ostvario svoj cilj i dokazao kao je najbolji. Važno je i pitanje etike industrijske špijunaže, koje je povezano s posljedicama. Posljedice koje čovjek može prouzročiti industrijskom špijunažom su velike. To mogu biti milijunski gubitci za konkurentsko poduzeće, gubitak ugleda poduzeća, isto tako i gubitak novca poduzeća ukoliko ga konkurent tuži te mora platiti kaznu, gubitak novca poduzeću predstavlja i ako ulaže u špijunažu, a uloženo se ne vrati. Gubitak ugleda može značiti i gubitak suradnje i partnerstava s ostalim poduzećima, dok u obrnutom slučaju može značiti i velik napredak i nove suradnje.

# Informacije imaju teško procjenjivu vrijednost, neki su autori pokušali postaviti formulu za izračun, ali sasvim točan izračun nije moguće dobiti pošto se vrijednost informacije gleda iz različitih aspekata i ovisi o situacijama.

# Što se tiče metoda, tu bih zaključila da su metode nastajale u skladu s vremenom i tehnologijama, mnogo ih se promijenilo i nestalo, nove nastaju, i kako tehnologija bude napredovala, čovjek će uvijek naći način da se prilagodi i iskoristi tehnologiju što je moguće više i bolje. Neke metode će vjerojatno teže zastarjeti, primjerice metoda *insidera*, koja je najčešće u korištena u današnje vrijeme, barem po onome što se u javnosti govori i piše. Dok traje financijska kriza u svijetu, ljudi će štošta učiniti ne bi li dobili novac, ali nisu svjesni da oni daju pristup informacijama za malu svotu novca s obzirom koliku vrijednost ta informacija predstavlja onome koji ju treba. Također, digitalne tehnologije učinile su to da se ljudi lakše domognu informacija, a da ne ostave trag jer digitalne dokumente samo trebaju iskopirati, ne moraju ih fizički ukrasti.

# Brojni primjeri postoje za industrijsku špijunažu, to je već svakodnevnica, i smatram da industrijska špijunaža neće nestati, nego će se samo još više razvijati, pogotovo dok je društvo kapitalistički usmejreno. Dok god traje borba za tržištem i novcem, ljudi će tražiti sve načine ne bi li se domogli onog što najviše žele – informacije.

# Literatura

1. Alstete J., (2003), *Trends In Corporate Knowledge Asset Protection*, Journal of Knowledge Management Practice, dostupno na linku <http://www.tlainc.com/articl47.htm>, preuzeto 01.09.2013
2. Aufderheide J.J., 21.08.2013, *This Phamaceutical Company Used NSA-Like tactis to Monitor Parents' Concerns About Vaccines*, Vactruth.com, dostupno na linku <http://vactruth.com/2013/08/21/pharmaceutical-spy-tactics/>, preuzeto 06.07.2014
3. Colibasanu Oana-Antonia, *Between Intelligence and Espionage in the Contemporary Business Environment*, dostupno na linku <http://www.ekonomikaamanagement.cz/getFile.php?fileKey=CEJVB0NUCAdVCEZIU1VHB0MIUUMEBAVDVFVWQ1VUBAVGQ1VCXgQFBERIRENCZA>==, preuzeto 01.09.2014
4. Collantine K., 30.10.2007, *Stories of the season: Hamilton versus Alonso*, F1fanatic, dostupno na linku <http://www.f1fanatic.co.uk/2007/10/30/f1-07-review-hamilton-vs-alonso/>, preuzeto 06.07.2014
5. Crane A., 2003, *In the company of spies: The ethics of industrial espionage*, ICCSR Nottingham University, dostupno na linku <http://195.130.87.21:8080/dspace/bitstream/123456789/1105/1/15-In%20the%20company%20of%20spies%20The%20ethics%20of%20industrial%20espionage.PDF>, preuzeto 05.07.2014
6. Čuljak Tihomir*, Obavještajno sigurnosne službe*, dostupno na linku <http://bs.scribd.com/doc/147948442/obavje%C5%A1tajno-sigurnosne-slu%C5%BEbe>, preuzeto 15.04.2014
7. Ćosić-Dragan, D. (2008), *Poslovnost i izvjesništvo*, dostupno na hrcak.srce.hr/file/33315, preuzeto 25.06.2014
8. D.Ko., 06.01.2011, *Ozbiljna industrijska špijunaža u Renaultu*, dnevno.hr, dostupno na linku <http://www.dnevno.hr/auto-moto/18393-ozbiljna-industrijska-spijunaza-u-renaultu.html>, preuzeto 15.04.2014
9. Hrvatski Sabor, 2011, Osnovni tekst iz NN 125/11 od 07.11.2011, dostupno na linku <http://www.zakon.hr/cms.htm?id=269>, preuzeto 06.07.2014
10. Hrvatski Sabor, 2012, Izmjene iz NN 144/12 od 21.12.2012, dostupno na linku <http://www.zakon.hr/cms.htm?id=270>, preuzeto 06.07.2014
11. Javorović B., Bilandžić M. (2007), *Poslovne informacije i business intelligence*, Zagreb: Golden marketing – Tehnička knjiga
12. Kavain, M., 02.05.2014, *S računa hrvatskih tvrtki hakeri ukrali 2 milijuna kuna: sve je počelo instaliranjem virusa...*, Slobodna Dalmacija, dostupno na linku <http://www.slobodnadalmacija.hr/Crna-kronika/tabid/70/articleType/ArticleView/articleId/243641/Default.aspx>, preuzeto 06.07.2014
13. Lee J., Rosenbaum A., (2003), *Knowledge management: Portal for corporate espionage? Part 1,* dostupno na linku <http://www.kmworld.com/Articles/Editorial/Features/Knowledge-management-Portal-for-corporate-espionage-Part-1--9508.aspx>, preuzeto 01.09.2014
14. Lerner, Adrienne Wilmoth, *Espionage and Intelligence, Early Historical Foundations,* Espionage Encyclopedia (online), dostupno na linku <http://www.faqs.org/espionage/Ep-Fo/Espionage-and-Intelligence-Early-Historical-Foundations.html>, preuzeto 25.06.2014
15. Martin, P., 02.10.2006, *Hewlett-Packard spying scandal sheds new light on US corporate “ethics”*, wsws.org, dostupno na linku <http://www.wsws.org/en/articles/2006/10/hepa-o02.html>, preuzeto 06.07.2014
16. Mihovilović M, 18.09.2007, *Ucjenjivač Alonso upropastio McLaren*, Nacional br. 618, dostupno na linku <http://www.nacional.hr/clanak/37955/ucjenjivac-alonso-upropastio-mclaren>, preuzeto 06.07.2014
17. Milian, M., 27.04.2011, Sony: Hacker stole PlayStation users' personal info, CNN, dostupno na linku <http://edition.cnn.com/2011/TECH/gaming.gadgets/04/26/playstation.network.hack/>, preuzeto 06.07.2014
18. Nacionalni CERT, (2012), *Zlonamjerni programi u službi država*, dostupno na linku <http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2012-10-338.pdf>, preuzeto 05.07.2014
19. Nepoznat autor, 02.03.2011, *Industrijska špijunaža godišnje odnosi milijarde dolara*, republikainfo.com, dostupno na linku <http://republikainfo.com/index.php/vijesti/503-industrijska-spijunaza-godisnje-odnosi-milijarde-dolara>, preuzeto 15.04.2014
20. Nepoznat autor, 20.09.2011, *Famous cases of corporate espionage*, Bloomberg Businessweek, dosupno na linku <http://images.businessweek.com/slideshows/20110919/famous-cases-of-corporate-espionage>, preuzeto 25.06.2014
21. Panian Ž., Klepac G. (2003), *Poslovna inteligencija*, Zagreb: MASMEDIA
22. Poulter, S., 28.04.2011, *Credit card alert as hackers target 77 milions PlayStation users*, dailymail, dostupno na linku <http://www.dailymail.co.uk/sciencetech/article-1381000/Playstation-Network-hacked-Sony-admits-hackers-stolen-77m-users-credit-card-details.html>, preuzeto 06.07.2014
23. Rechtin M., 30.04.2013, *Renault spy scandal: Former COO 'had to leave'*, Automotive News, dostupno na linku <http://www.autoweek.com/article/20130430/CARNEWS/130439995>, preuzeto 15.04.2014
24. Robinson S.W. (2003), *Corporate Espionage 101*, SANS Institute, dostupno na linku <http://faculty.usfsp.edu/gkearns/Articles_Fraud/corporate%20espionage.pdf>, preuzeto 02.07.2014
25. Rouse M., 2012, Industial espionage, WhatIs.com, dostupno na linku <http://whatis.techtarget.com/definition/industrial-espionage>, preuzeto 15.04. 2014
26. Schofield, H., 15.03.2011, *Renault spy scandal risks denting carmaker's reputation*, BBC News, Paris, dostupno na linku <http://www.bbc.co.uk/news/world-europe-12732421>, preuzeto 15.04.2014
27. V.K., (13.06.2013), *Industrijska špijunaža u stalnom je porastu*, MojPosao.net, dostupno na linku <http://www.moj-posao.net/Vijest/61881/Industrijska-spijunaza-u-stalnom-je-porastu/2/>, preuzeto 25.06.2014
28. Wikipedija, (2014), *Trojanski konj (softver),* dostupno na linku <http://hr.wikipedia.org/wiki/Trojanski_konj_(softver)>, preuzeto 06.07.2014
29. Winkler, I., *Case study of industrial espionage through social engineering*, National Computer Security Association, dopstupno na linku <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.36.115&rep=rep1&type=pdf>, preuzeto 06.07.2014

1. Izvor: Javorović, Bilandžić, 2007, str. 32-33 [↑](#footnote-ref-2)
2. Izvor: Panian Ž., Klepac G., 2003, str.39-40 [↑](#footnote-ref-3)
3. Izvor: Panian Ž., Klepac G., 2003, str.40-41 [↑](#footnote-ref-4)
4. Izvor: Panian Ž., Klepac G., 2003, str. 42-43 [↑](#footnote-ref-5)
5. Izvor: Panian Ž., Klepac G., 2003, str. 43-49 [↑](#footnote-ref-6)
6. Izvor: Lerner*,* <http://www.faqs.org/espionage/Ep-Fo/Espionage-and-Intelligence-Early-Historical-Foundations.html> [↑](#footnote-ref-7)
7. Izvor: Javorović, Bilandžić, 2007, str. 184 [↑](#footnote-ref-8)
8. Izvor: Robinson , 2003, <http://faculty.usfsp.edu/gkearns/Articles_Fraud/corporate%20espionage.pdf> [↑](#footnote-ref-9)
9. Izvor: Čuljak, <http://bs.scribd.com/doc/147948442/obavje%C5%A1tajno-sigurnosne-slu%C5%BEbe> [↑](#footnote-ref-10)
10. Izvor: Winkler, <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.36.115&rep=rep1&type=pdf>, str. 4 [↑](#footnote-ref-11)