Negativni učinci industrijske špijunaže na gospodarstva razvijenih zemalja

Vincek, Helena

MEĐIMURSKO VELEUČILIŠTE U ČAKOVCU

PREDDIPLOMSKI STRUČNI STUDIJ MENADŽMENT TURIZMA I SPORTA

Helena Vincek

NEGATIVNI UČINCI INDUSTRIJSKE ŠPIJUNAŽE NA GOSPODARSTVA RAZVIJENIH ZEMALJA

ZAVRŠNI RAD

Čakovec, rujan 2022.

MEĐIMURSKO VELEUČILIŠTE U ČAKOVCU

PREDDIPLOMSKI STRUČNI STUDIJ MENADŽMENT TURIZMA I SPORTA

Helena Vincek

NEGATIVNI UČINCI INDUSTRIJSKE ŠPIJUNAŽE NA GOSPODARSTVA RAZVIJENIH ZEMALJA

NEGATIVE EFFECTS OF INDUSTRIAL ESPIONAGE ON THE ECONOMY OF DEVELOPED COUNTRIES

ZAVRŠNI RAD

Mentor: mr.sc. Miljenko Vrbanec, pred.

Čakovec, rujan 2022.

MEĐIMURSKO VELEUČILIŠTE U ČAKOVCU
ODBOR ZA ZAVRŠNI RAD

Čakovec, 11. siječnja 2022.

država:	**Republika Hrvatska**
Predmet:	**Menadžment poslovne sigurnosti - izborni**
Grana:	**5.01.04 organizacija i menadžment**

ZAVRŠNI ZADATAK br. 19

Pristupnik:	**Helena Vincek (0313023510)**
Studij:	redovni preddiplomski stručni studij Menadžment turizma i sporta
Smjer:	Menadžment turizma

Zadatak: **Negativni učinci industrijske špijunaže na gospodarstva razvijenih zemalja**

Opis zadatka:

U završnom radu biti će objašnjeni pojmovi vezani uz industrijsku špijunažu, rasprostranjenost industrijske špijunaže, ciljevi i planiranje djelovanja industrijske špijunaže, metode provođenja industrijske špijunaže, primjeri industrijske špijunaže te na koji način industrijska špijunaža utječe ne ekonomiju. Na primjerima iz prakse pojedinih razvijenih država objasnit će se fenomen špijuniranja i krađe povjerljivih informacija, poslovnih tajni kao i tehnoloških patenata visoko razvijenih kompanija. Nadalje će se objasniti uloga poslovnih informacija te njihova važnost i zaštita podataka.

Zadatak uručen pristupniku: 11. siječnja 2022.
Rok za predaju rada: 20. rujna 2022.

Mentor:

mr. sc. Miljenko Vrbanec, v. pred.

Predsjednik povjerenstva za završni ispit:

ZAHVALA

Ovim putem želim se zahvaliti dragom mentoru na usmjeravanju i vođenju prilikom pisanja.

Helena Vincek

SAŽETAK

U današnje vrijeme informacija je postala vrlo vrijedna roba. Ekonomija i samo poslovanje koje se odvija unutar ekonomskog procesa, nezamislivo je bez poslovnih informacija. Međunarodna ekonomija usko je povezana s globalizacijom i gospodarskom integracijom. Živimo u svijetu u kojem je tehnologija poduzećima neizbježna. Svaka kompanija mora osigurati potrebnu tehnologiju, a najbitnije je da ju zaštiti. Temelj moderne ekonomije je distribucija informacija unutar poduzeća, ali i cijelog gospodarstva. Nažalost, lažne informacije mogu itekako biti na štetu ekonomiji pa i samom poduzeću. U poduzećima najčešći izvor "curenja informacija" su zaposlenici. Uz izraz "curenje informacija" danas se vežu, odavanje poslovne tajne i napad na informatičku strukturu. Navedena štetna djelovanja spadaju u industrijsku špijunažu koja se danas u najvećem dijelu svodi na *cyber* kriminal. Industrijska špijunaža u stalnom je porastu te se često naziva "najveća pljačka svih vremena." U sklopu istraživanja proveden je intervju u industrijskoj tvrtki "WE-KR" pomoću kojeg se ispitalo kako industrijska špijunaža djeluje na tvrtku. Također, istražilo se kako tvrtka štiti svoje poslovne informacije i podatke. Metodom intervjua, navedeno je da industrijska tvrtka nije bila suočena s industrijskom špijunažom jer se tvrtka ne koristi ne etičkim postupcima kako bi došli do informacija. Svoje podatke tvrtka posluje prema Uredbi o zaštiti osobnih podataka. Upoznata je s pojmom poslovne tajne te je tijekom provođenja intervjua predstavljen primjer izjave o tajnosti informacija prema globalnoj tvrtki Durr, jedna od glavnih partnera tvrtke "WE-KR." Također, predstavljeni su načini uz pomoć kojih sama tvrtka dolazi do bitnih informacija o konkurenciji. "WE-KR" vodeća je hrvatska tvrtka za izradu industrijskih metalnih rješenja. Stalnim unaprjeđenjem tehnologije ovoj tvrtki zajamčen je trajan poduzetnički uspjeh.

Svjetska trgovina u stalnom je porastu, posebno industrijski proizvodi i tehnologija koja dovela do zaštite intelektualnog vlasništva. Briga za zaštitu intelektualnog vlasništva dovela je do sve većeg natjecanja na konkurentnom globalnom tržištu. U tom kontekstu može se govoriti o jednom od najvećih organizacijskih fenomena, a to je industrijska špijunaža. Špijunaža, ima vrlo dugu povijest. Često se naziva korporativnom i ekonomskom špijunažom i industrijskom inteligencijom.

Ključne riječi: *industrijska špijunaža, poslovna tajna, zaštita podataka, poslovne informacije, poslovna inteligencija, patenti, špijuni*

SADRŽAJ

1. UVOD

Problem istraživanja u ovom završnom radu polazi od činjenice da u današnje vrijeme mnoge kompanije nailaze na probleme djelovanja industrijske špijunaže. Ona u pravilu nanosi izravnu štetu tvrtki ili poduzeću koju se špijunira. S druge strane industrijska špijunaža izravno koristi poduzeću koje je provodi. Glavno pitanje je na koji način je ekonomija povezana s industrijskom špijunažom i kako utječe na gospodarstva razvijenih zemalja. Pretpostavka ovog rada je da poduzeća nisu dovoljno upoznata s djelovanjem i metodama špijunaže i koliko negativno može utjecati na samo poduzeće.

U ovom završnom radu predmet istraživanja bit će različite metode i ciljevi kojima se koriste poduzeća tijekom provođenja špijuniranja. Kolika je rasprostranjenost i kako se provodi planiranje djelovanja industrijske špijunaže. Na primjerima iz prakse pojedinih razvijenih država objasnit će se fenomen špijuniranja i krađe povjerljivih informacija, poslovnih tajni kao i tehnoloških patenata visoko razvijenih kompanija, u ovom slučaju na primjeru industrijske tvrtke "WE-KR." Nadalje, će se objasniti uloga poslovnih informacija te njihova važnost i zaštita podataka. Ciljevi istraživanja su istražiti i analizirati svijest tvrtke „WE-KR" o industrijskoj špijunaži. Istražiti da li je tvrtka bila suočena s industrijskom špijunažom, ako jest opisati kako se to odrazilo na samu tvrtku. Istražiti kako tvrtka štiti svoje poslovne informacije i podatke. Na kraju rada nalazi se zaključak u kojem se rezimira tema industrijske špijunaže koja je povezana s važnošću zaštite podataka.

2. TEORIJSKI PREGLED LITERATURE

U ovom poglavlju razrađen je pojam i djelovanje industrijske špijunaže kroz nekoliko potpoglavlja. Glavna tema rada odnosi se na negativne učinke industrijske špijunaže na gospodarstva razvijenih zemalja. Opisane su poslovne informacije i važnost zaštite podataka.

2.1. Nastanak i pojmovno značenje industrijske špijunaže

Pod pojmom špijunaža najčešće se podrazumijeva nešto tajno i prikriveno. Riječ špijunaža potječe od njemačke riječi *Spionage* te u sebi sadržava prikupljanje važnih političkih, gospodarskih ili kao nekada bitnih vojnih podataka. Špijunaža se može promatrati s pravne i političke razine. Politička razina se najčešće odnosi na prikupljanje tajnih podataka, dok se pravna razina odnosi na pravni izraz za kažnjivu obavještajnu djelatnost. Nezakonito djelovanje gospodarskih subjekata kao što su razne tvrtke, ustanove i institucije na prikupljanju podataka gospodarske naravi radi stjecanja nove dodatne vrijednosti nazivamo industrijskom špijunažom. U svom radu(Bazdan,2016) govori o tome da kada je pitanje o industrijskoj špijunaži, iza tog ilegalnog i kažnjivog djela svjesno stoje poslovni subjekti koji pokušavaju doći do poslovnih tajni. Glavni i osnovni objekt špijunaže je državna tajna. (https://www.enciklopedija.hr/natuknica.aspx?id=59838).

Povijesne činjenice razvitka industrijske špijunaže navodi Ćosić(2008) govore da je razvoj industrijske špijunaže zabilježen još u 15.stoljeću. Kineska princeza donijela je na svom šeširu koji je bio ukrašen cvijećem čahure svilene bube u Indiju i tako ih predala svom budućem mužu te je strogo čuvala tajnu o načinu proizvodnje svile. Tada je Indija počela proizvoditi svilu i s vremenom postala jedan od najvećih proizvođača svile u svijetu. Najsnažniji razvoj industrijske špijunaže zabilježen je početkom 20.stoljeća u SAD-u, a prvi europski državnik kojeg je zanimalo značenje industrijske špijunaže bio je Winston Churchill koji je u Velikoj Britaniji, 1919.godine osnovao „Obavještajni centar za proučavanje industrije." Nekoliko godina kasnije, Japanci su osnovali sličan centar te su kao narod najdalje otišli kada je riječ o industrijskoj špijunaži. Danas, u Japanu ovim poslom bave se profesionalni poslovni stručnjaci, a u određenim situacijama i bivši pripadnici obavještajno-sigurnosnog sustava zemlje. Počeci nastanka špijunaže koje spominje Ćosić (2008) vežu se uz potrebe vojne špijunaže. Vojna špijunaža temeljila se na sakupljanju znanja o proizvodnim

kapacitetima oružja i vojne opreme određene zemlje. Također, takva vrsta špijunaže obuhvaćala je špijuniranje tehnologije određene zemlje.

Postoje razne definicije i razni autori koji definiraju industrijsku špijunažu. Najčešća i najjednostavnija definicija koja opisuje industrijsku špijunažu je prikupljanje zaštićenih podataka iz poslovanja neke tvrtke koje proizvode neovlaštene osobe i tvrtke. (http://struna.ihjj.hr/naziv/industrijska-spijunaza/51107/) Osobe koje se bave špijunažom nazivamo špijunima koji se profesionalno bave tim poslom. „Špijun je, zapravo, uhoda, tajni agent koji istražuje i sakuplja važne tajne iz vojne, političke i gospodarske oblasti u jednoj zemlji.“ (Bazdan,2011) Neke od načina i sredstava kojima dolaze do određenih informacija su: praćenje, tajno prikrivanje, dostavljanje podataka, varanje i optuživanje.

Često, uz pojam industrijske špijunaže spominje se gospodarska špijunaža. Prema Ćosiću (2008) takva vrsta špijunaže podrazumijeva djelovanje izvještajnih službi na prikupljanju podataka koji su gospodarske naravi kako bi se stekla nova saznanja, sposobnosti i razne tehnologije. Uspoređujući gospodarsku i industrijsku špijunažu, Ćosić (2008) zagovara da je industrijska špijunaža usmjerenija i koncentriranija u odnosu na gospodarsku. Gospodarsku špijunažu, države najčešće planiraju i provode kroz različite sustave koji su na raspolaganju, od izvještajnih službi pa do drugih državnih tijela i institucija.

Špijunaža nosi sa sobom velike posljedice za gospodarstvo te često djeluje negativno na zemlje. Mnogi stručnjaci naglasili su da se na udaru industrijske špijunaže nalaze tvrtke svih veličina i područja djelovanja. Jedan od primjera je država Njemačka kojoj prijeti rastuća opasnost od industrijske špijunaže zbog koje ima enormno velike novčane gubitke. Najveća posljedica špijunaže u Njemačkoj pa i u ostalim zemljama koje pogađa industrijska špijunaža je ugroženost konkurentnosti na tržištu. Konkurentnost na tržištu bitan je proces kojim se prikazuje interakcija i tzv. borba između raznih poduzeća, odnosno tvrtki. Također, konkurencija je poticaj raznim poduzećima i cijelom gospodarstvu. Industrijska špijunaža donosi velike štete gospodarstvu te samim time i razvitku gospodarstva pojedine zemlje.

2.2. Ciljevi i metode špijunaže

Kada se govori o ciljevima špijunaže, oni su različiti od države do države. Ćosić(2008) ističe najviše o tome ovisi stupanj tehnologije koji određena zemlja posjeduje. Glavni cilj svake vrste špijunaže je prikupljanje podataka novim tehnologijama i tehnikama. Zatim, jedan od ciljeva je prikupljanje podataka poslovnim tajnama konkurentskih gospodarskih subjekata. Prema Ćosiću(2008) velika poduzeća raznim metodama špijuniranja dolaze do novih proizvoda i usluga koje gospodarski subjekti namjeravaju plasirati, također špijuniraju njihove podatke o vremenu i načinu njihova plasmana. Isto tako, špijunirati se mogu i osobe koje su na vodećim pozicijama u tvrtkama te osobe koje vode razvojne i istraživačke dijelove tvrtke jer se na tim dijelovima često nalaze najbitniji podaci za tvrtku. Ćosić(2008) spominje da veće i snažnije tvrtke najčešće prikupljaju podatke strateške važnosti, a manje tvrtke svoje ciljeve postavljaju na nižim razinama koje su vezane uz tehničko-tehnološka znanja i sposobnosti. Prema Ćosiću (2008) pozitivni ciljevi špijunaže su pomoć vlastitim poduzećima protiv strane konkurencije te stjecanje monopola na stranim tržištima. Metode koje se koriste tijekom špijuniranja slične su metodama koje koriste izvještajne službe te ovise o ljudskim i tehnološkim mogućnostima subjekata.

Đorđević (1978:54) govori da se špijunaža može podijeliti na: vojnu, političku, elektronsku i na ekonomsku špijunažu.

1. Vojna špijunaža- smatra se začetnicom špijunaže te je međunarodno pravo priznaje samo u slučaju rata. Ovom vrstom špijunaže prikupljaju se podaci o oružanim snagama drugih zemalja te isto tako prikupljanje podataka o oružanim snagama već postojećih protivnika.

2. Politička špijunaža- u prvi plan stavlja se interes stranih obavještajnih službi te se prati njihova aktivnost u području vođenja politike. Glavnu ulogu imaju razni ministri koji dolaze iz raznih zemalja, predstavnici vlade i druge osobe koje su na višim pozicijama u državi.

3. Elektronska špijunaža- najčešće se koristi u razvijenim zemljama, najviše u investicijskim bankama i raznim velikim korporacijama. Prikupljaju se podaci o konkurentnim elektronskim sistemima i oblika komunikacije u elektroničkom obliku (telefoni, radio, računalo...).

4. Ekonomska špijunaža- sagledava se na dva način. U pravnom smislu često se govori o učincima gospodarstva na određenu zemlju pa se često naziva gospodarskom špijunažom. Visoko razvijene zemlje koriste termin industrijska špijunaža jer se najčešće u takvim zemljama promatraju i špijuniraju velike korporacije i poduzeća. Usmjerena je na tehnološki i tehnički razvoj određenih subjekata.

Bazdan (2016) govori da je industrijska špijunaža postala glavni krivac za novčane gubitke u visokorazvijenim zemljama. Novčani gubici negativno utječu na gospodarstva visokorazvijenih zemalja. Do određenih informacija tijekom industrijske špijunaže dolazi se nelegalnim i neetičnim postupcima. Također, u svom radu Bazdan(2016: 53-54) navodi da su zakonom određene sljedeće nelegalne i neetične aktivnosti: - nelegalni upadi u tuđe informatičke mreže, prisluškivanje telefonskih razgovora, lažno predstavljanje poradi dolaženja u posjed tajnih informacija te nuđenje mita, kompenzacija ili protežiranje neke kompanije u zamjenu za tajne informacije.

U svom radu Bazdan(2016) dijeli metode industrijske špijunaže na klasične i suvremene. Govori da su klasične metode povezane prisluškivanjem i fotografiranjem. Neke od klasičnih metoda su: mikrofon s pneumatskim pričvršćivačem koji se najčešće lijepi na zidove pomoću kojih se mogu slušati razgovori u susjednoj sobi, bešumna minijaturna fotokamera koja je u obliku upaljača za cigarete u kojem se nalazi špijunska kamera s vidnim poljem. Zatim, tzv. tihe kamere koje snimaju kroz rupicu u zidu ili vratima od samo jednog milimetra. Navedene klasične metode koriste se još dan danas, no sve više su zastupljenije one koje se baziraju na informatičkoj tehnologiji. Bazdan(2016) zagovara da se industrijska špijunaža najviše služi kompjuterskim kriminalom ili kompjuterskom špijunažom koja pripada najsuvremenijim oblicima elektroničke špijunaže. Ovakvom vrstom špijunaže koriste se profesionalni špijuni koji su prijenos podataka doveli do samog savršenstva. Oblici kompjutorske špijunaže koje Bazdan(2016) spominje su: otkrivanje poslovne tajne, ilegalni transfer tehnologija i softverska krađa tj. *hacking.* Softverska krađa najzastupljenija je u kompjutorskoj špijunaži te se odnosi na neovlašteno prodiranje kompjutorski sustav kako bi se došlo do bitnih i relevantnih informacija te do određenih dokumenata. Još jedna krađa postaje sve popularnija i zastupljenija. To je krađa laptopa(*Laptop Theft*). Takva krađa pogubna je za korporacije te je najbolje vidljiva u zračnim lukama. Radi se o tome da se špijuniraju ciljane osobe određenih korporacija, najčešće su to direktori kompanija i vrebaju njihovi laptopi u kojima se nalaze bitni programi za rad.

2.3. Utjecaj industrijske špijunaže na gospodarstva

Danas, industrijska špijunaža u velikoj mjeri utječe na ekonomiju. Zauzima značajno mjesto u odnosima među državama i kompanijama. Bazdan (2016) zagovara da su glavne odlike suvremenog razdoblja međunarodne ekonomije: globalizacija, informatička revolucija i gospodarske integracije. Najčešće, industrijsku špijunaže provode gospodarski najmoćnije države koje pomoću svojih špijuna pokušavaju doći do povjerljivih podataka. Mnoge zemlje pokušavaju doći do bitnih podataka na različite načine. SAD u tome najviše odskače, naime ima na raspolaganju najmoćniji obavještajni i kontraobavještajni aparat na svijetu. Japanci su izgradili sofisticiranu obavještajnu infrastrukturu u zemlji i inozemstvu.(Bazdan,2016). Najbrojnijom obavještajnom mrežom na svijetu može se pohvaliti Kina, koja je još u dalekoj prošlosti prva koristila obavještajnu službu. Francuska, također još od rane prošlosti za vrijeme vladavine Luja XIV. koristi mehanizam obavještajne službe i danas je lider za gospodarsku diplomaciju. (Bazdan,2016). U svom radu Bazdan(2016) zagovara da u današnje vrijeme, države koje raspolažu s najmoćnijim globalnim špijunskim sustavom su SAD, Velika Britanija, Australija, Kanada i Novi Zeland. Ruska Federacija je zemlja koja po tom pitanju vrlo agresivno postupa prema SAD-u i drugim zemljama s visokim stupnjem tehnologije kao što su Kina i Japan. U skupinu agresivnih zemalja još spada i Sjeverna Koreja i Irak. Svim navedenim zemljama glavni je cilj pomoću tajnih podataka doći do superiornog položaja na tržištu. Da bi svaka zemlja uspjela u svom naumu treba imati itekako snažnu ekonomsku bazu. Kada se govori o utjecaju špijunaže na ekonomiju, često se pojavljuje izraz „poslovna špijunaža." Poslovna špijunaža predstavlja kombinaciju podataka i znanja u odnosu na poslovno okruženje u kojem poduzeće djeluje i posluje. Prikupljeni podaci omogućuju stjecanje konkurentske prednosti i donošenje važnih poslovnih odluka. Podaci koji utječu na pravilno donošenje odluka vrlo su važne jer poboljšavaju konkurentsku poziciju domaćih industrijskih i pogonskih kapaciteta na drugim tržištima. Čovjek, tj.osoba može imati vrlo važnu ulogu u poslovnoj špijunaži. Direktne informacije koje dolaze od pojedine osobe smatraju se najvrjednijom „robom" i bolju osnovu za donošenje kvalitetnih odluka. Za prikupljanje takvih informacija koriste se trenutno zaposlene osobe u određenom poduzeću i bivši zaposlenici gospodarskih subjekata i institucija koje predstavljaju predmet interesa obavještajnih agencija. Tu spadaju nezadovoljne osobe koje su zaposlene u tim poduzećima ili osobe koje su ucijenjene surađivati. Prenošenje znanja može biti materijalni interes kao i utjecaj samog poslodavca radi ostvarivanja osobnih interesa.

Industrijska špijunaža najviše se fokusira na tehnološki i tehnički razvoj te ostvarivanje interesa poslovnih subjekata tj. raznih poduzeća koja žele doći do bitnih informacija koja bi im bila korisna da dosegnu visok položaj na tržištu. Industrijskom špijunažom obuhvaća se samo jedno područje ekonomske špijunaže jer je po svojim zadacima i normama fokusirana samo na određenu specifičnu stručnu djelatnost u ekonomiji. (Bazdan,2016)

Neizostavno je spomenuti globalizaciju i njezin utjecaj na ekonomiju. Globalizacija se rezultira iz tehnološkog razvoja i napretka. Tehnološki razvoj na području komunikacija, prijevoza, upravljanja i dizajniranja proizvodom, itd. Špijunaža je jedan od glavnih razloga zašto u pojedinim zemljama dolazi do pada tehnologije. Padom tehnologije uništavaju se nacionalna gospodarstva.

2.3.1. Utjecaj špijunaže na gospodarstva razvijenih i nerazvijenih zemalja

Danas, ekonomija i ekonomski učinci imaju vrlo važnu ulogu za pojedinu zemlju. Najčešća podjela, ako govorimo o ekonomskoj razvijenosti je podjela na razvijene zemlje koje se često nazivaju ekonomskim liderima i nerazvijene zemlje koje su uglavnom siromašne. Zemlje u razvoju sve više i više gube svoj značaj, zbog toga što se razvijene zemlje koje su najčešće bogate i imaju visok BDP sve više bogate, a one koje su nerazvijene se sve više osiromašuju. Taj proces bogaćenja razvijenih zemalja Leko i Požega(2016) u svom radu nazivaju „grude snijega“ , što bi jednostavno značilo da zemlje s većim kapitalom stvaraju i veći kapital, dok siromašne zemlje s malim kapitalom stvaraju manji kapital. Također, Leko i Požega(2016) ističu da se kapital može odnositi na materijalno i nematerijalno. Materijalni kapital predstavlja novac ili sirovine, a nematerijalni kapital se odnosi na znanje, vještine i sposobnosti.

Ekonomske vođe ili tzv. ekonomski lideri su najviše svojih postignuća postigli materijalnim kapitalom i to prvenstveno novcem i sirovinama. Što je zemlja bogatija sirovinama, gospodarski će se i bolje razvijati. Razvijenim zemljama „vladaju ekonomski lideri“ koji se u današnje vrijeme najviše koriste ekonomijom znanja. Prema Bazdanu(2016) osnovne stavke ekonomije znanja su: ljudsko znanje i ljudska kreativnost, povezanost motivacije i razvoj mrežne industrije. Nerazvijene zemlje puno teže dostižu razvijene zemlje, no ako određena zemlja ima čimbenike koje zna na pravilan način iskoristiti i kojim bi mogla poboljšati svoj gospodarski razvoj, kao npr. Afrika koja ima puno ruda ili Hrvatska koja najviše zarađuje od turizma, mogu poboljšati svoje ekonomsko stanje.

Industrijska špijunaža jedan je od razloga zbog kojeg razvijene zemlje često nastradaju te sa sobom nose velike gubitke. Uništava se cjelokupno gospodarstvo pojedine zemlje. Špijunažom se, kako ističe Bazdan(2016) dolazi do informacija o intelektualnom vlasništvu konkurenata što se odnosi na patente, poslovne tajne, autorska prava, tehnologiju, inovacije i razne postupke. Većina zemalja najviše je osjetljiva na kompjutorsku špijunažu koja je odgovor na razvoj i primjenu softverskih i hardverskih rješenja.

2.3.2. Hrvatska i negativni učinci na gospodarstvo

Kada se govori o Hrvatskoj i problemima s kojima se ona najviše susreće misli se sve više i više na gospodarski kriminalitet koji je u velikoj mjeri prisutan te se često naziva i hrvatskim fenomenom. Gospodarski kriminalitet najjednostavnije je opisati kao izravno ugrožavanje gospodarstva određene zemlje koje za sobom nosi kobne posljedice i velike financijske štete. U Hrvatskoj, gospodarski kriminalitet najviše pogađa infrastrukturu.

Ono sa čime se Hrvatska, također bori su kibernetički napadi. Hrvatska je zauzela 10. mjesto sa 4,55 posto rizika za kibernetičke prijetnje. (https://www.itpro.co.uk/security/cyber-security/354818/uk-among-countries-most-likely-to-encounter-cloud-attacks) Najnoviji napadi dolazili su iz Rusije te su glavne mete bili: Mistarstvo obrane i Ministarstvo vanjskih poslova.(https://zimo.dnevnik.hr/clanak/cyber-napadi-sve-cesci-na-hrvatsku---717678.html) Takvim napadima uništava se prvenstveno tehnologija, a postupno i cijelo gospodarstvo.

Jedan od najpoznatijih kibernetičkih napada u Hrvatskoj dogodio se 2020.godine na naftnu kompaniju INA. Hakeri su zlućudnim programom zvanim „malware“ ušli u računalnu mrežu kompanije te su time prouzrokovali probleme s plaćanjem računa te izdavanju bonova. Nakon napada, slučaj je prijavljen nadležnim institucijama. Srećom, napad nije ugrozio cjelokupno poslovanje kompanije te su plaćanja(gotovina, bankovne ili INA kartice) osigurana. (https://www.bug.hr/sigurnost/ina-sanirala-korisnicima-vidljive-posljedice-kibernetickog-napada-14269)

„Ransomware“ je virus koji je Hrvatima stvarao najviše komplikacija i problema. Sastoji se od više zlonamjernih programa koji korisniku računala onemogućuje ponovni pristup računalu. Da bi korisnik ponovno pristupio, treba platiti određenu otkupninu u zamjenu za daljnje korištenje. (https://www.cert.hr/19795-2/ransomware/)

Hrvatska je također, imala problem s internet bankarstvom. Hrvatske banke koje nude internetske usluge napadnute su od raznih hakera koji ispituju lozinke . 2014. godine nepoznati su hakeri ulazili i ubacivali softver i Trojance na računala Hrvata i tako dolazili do bitnih podataka pomoću kojih su ljudi pristupali internet bankarstvu. (https://www.poslovni.hr/sci-tech/hakeri-provaljuju-stranice-internetskog-bankarstva-kako-bi-vam-ukrali-novac-356166)

2.3.3. Statistički podaci o nedozvoljenim radnjama u Hrvatskoj

Prema podacima Ministarstva unutarnjih poslova za 2021. godinu evidentirano je 4.627 kaznenih djela iz područja gospodarskog kriminaliteta, što je za 2,1 posto više, nego u 2020.godini. U podacima iz Ministarstva unutarnjih poslova, zabilježeno je sljedeće: „ Za kaznena djela gospodarskog kriminaliteta osumnjičeno je 1.226 osoba, što je 18,3 posto više u odnosu na 2020. godinu. Krivotvorenje službene ili poslovne isprave najbrojnije je kazneno djelo iz dijela gospodarskog kriminaliteta u 2021. godini.“ Što se tiče, kibernetičkog kriminaliteta zabilježeno je ukupno 1.563 kaznenih djela u 2021.godini. Najbrojnije kazneno djelo koje spada u kibernetički kriminalitet je računalna prijevara s udjelom od 73,1 posto. Problem s kojim se Hrvatska, već godinama susreće je korupcija. Zabilježeno je ukupno 912 korupcijskih djela u 2021. godini, što je za 69,5 posto više, nego u 2020.godini. (https://mup.gov.hr/UserDocsImages/statistika/2022/Statisticki_pregled_2021_Web.pdf)

2.4. Ilegalne sastavnice globalne ekonomije

Globalna ekonomija sadrži u sebi dvije razine, to su ilegalna i legalna razina. U sivo gospodarstvo ili tzv. podzemno gospodarstvo spadaju: patološko poduzetništvo i prihodi od trgovine ljudima, droge, alkohola, oružja, nezaštićena autorska prava, novac koji se „pere“ ,crnog tržišta benzina i nafte. Neki od ilegalnih segmenata globalne ekonomije smatraju se: korupcija, nelojalna konkurencija u koju spada krađa patenata te pranje novca.

Staro shvaćanje pojma korupcija je prvenstveno kvarenje moralnih vrijednosti. „Etimološki termin korupcija dolazi od latinske riječi rumpere što doslovce znači razbijanje, lomljenje, kidanje, sugerira se da je nešto prekinuto.“ (Aras, 2007). Najčešće do korupcije dolazi zbog socijalne solidarnosti i nepovjerenje građana u zakone i vlast. Korupcijom se ugrožava tržišna utakmica i resursi koje određena država ima. Kako bi korupcije bilo što manje u svijetu, globalna ekonomija inzistira na vrednotama i solidarnosti među ljudima te samim time i poboljšanju životnog standarda.

Nelojalna konkurencija se najčešće odnosi na krađu patenata. Bazdan(2011) u svom radu definira nelojalnu konkurenciju na sljedeći način: „Prema definiciji nelojalna konkurencija su načini i postupci koji su protivni dobrim poslovnim običajima, a kojima se nanosi ili se može nanijeti šteta drugom poslovnom subjektu, potrošačima jer su dovedeni u zabludu, ali i

državi.“ U nelojalnu konkurenciju spadaju razne nelojalne reklame koje iznose neistine o konkurentu. Također u nelojalnost konkurencije spada i krađa gospodarskih patenata, grbova, zaštićenih znakova i žigova. Korištenje tuđe poslovne tajne, vrbovanje djelatnika konkurencije i manipuliranje cijenama, također spada u nelojalnu konkurenciju. Neke zemlje kao što su Tajland, Singapur, Hong Kong, Kina, Ruska Federacija toleriraju i prihvaćaju krađu gospodarskih patenata i zaštićenih znakova. Tu se najčešće misli na znakove svjetskih poznatih marka kao što su Adidas, Nike, Prada, Gucci, itd. Posljedice toga su veliki novčani gubici poznatih svjetskih kompanija.

Pranje novca je radnja koja je sve više globalno prisutna. Ovom radnjom podrazumijeva se tzv. čišćenje novca stečenog kriminalnim aktivnostima. Pranje novca najviše prijeti financijskim ustanovama, zbog čega dolazi do toga da se slobodni kapital nepromišljeno ulaže te se time narušavaju postojeći ekonomski tokovi. Pojam pranje novca Bazdan(2011) u svom radu navodi na sljedeći način: „Danas se pod pranjem novca podrazumijeva svaka financijska transakcija kojoj je cilj stvaranje vrijednosti koja je rezultat nezakonitog postupka. A takvi mogu biti utaja poreza i lažna financijska izvješća.“ Pranjem novca uništava se tržišno gospodarstvo čime se narušava politička struktura i stabilnost zemlje.

2.5. Primjeri najpoznatijih svjetskih špijuna

Razne misterije, opasnost, adrenalin, tajanstvenost i fizička spremnost samo su neki od opisa špijuna. Među pet najpoznatijih špijuna u svijetu spadaju: Klaus Fuchs, Giacomo Casanova, Mata Hari, Richard Sorge i Ian Fleming.

Klaus Fuchs bio je njemački fizičar koji je radio na projektu razvoja atomske bombe u Engleskoj. Surađivao je sa Sovjetskim Savezom te im je davao informacije o britanskim i američkim projektima. Nakon završetka Drugog svjetskog rata Amerikanci su ga otkrili kao špijuna te je u Velikoj Britaniji optužen na 14 godina zatvora.

Talijanski avanturist i pisac Giacomo Casanova također se smatra jednim od poznatijih špijuna. Bio je svestrana ličnost. Umjetnik, pisac, odvjetnik i strastveni kockar. U špijunskim poslovima, špijunirao je mletačke inkvizitore. Također, bio je na glasu kao veliki ljubavnik sa ženama iz visokih klasa te mu je to pomoglo da postane vrlo moćna ličnost koji traga za važnim informacijama.

Mata Hari predstavlja simbol žene koja koristi „ženske čari“ kako bi doznala skrivene tajne. Rođena je u Nizozemskoj te s 18 godina postaje žrtva trgovanja. Nakon par godina pobjegla je u Pariz te tamo postala poznata plesačica. Njemačka tajna služba plaćala joj je velike svote novaca za špijunske uloge. Tada je dobila i tajno ime H-21. Izabrali su je za špijunku jer je navodno lako dolazila do visokih ljudi iz vojske i politike. Bila je u izvrsnoj poziciji za prikupljanje raznih podataka. Njezin glamurozan život svrstan je na samom vrhu najpoznatijih špijuna svih vremena.

Sovjetski agent, Richard Sorge dobrovoljno je služio tijekom Drugog svjetskog rata. Bio je novinar u Japanu i Njemačkoj. Zanimljivost koja se veže za njega je ta da on bio prvi koji je Staljinu rekao da Japan neće napasti Sovjetski Savez te se Staljin povukao sa svojom vojskom na zapad, spašavajući Moskvu. Uhićen je u Tokiju 1941. godine, no nakon što je pušten nikada nije priznao da je imao veze sa Sovjetskim Savezom. Prema mnogima, Sorge se smatra najuspješnijim špijunom ikad te je jedan od likova koji su bili inspiracija za lik James Bonda. Ian Fleming, britanski pisac i novinar koji je najpoznatiji kao tvorac serije romana o James Bondu. Mnogi govore da je bilo loš špijun i još gori novinar, no unatoč tome zaslužan je za globalno proširenje tajnih agenata te je pridonio golem entuzijazam za špijunski život.

(https://dnevnik.hr/vijesti/svijet/najpoznatiji-spijuni-u-povijesti.html)

2.6. Poslovne informacije i poslovna inteligencija

Riječ informacija potječe od lat. *Informare* što bi u prijevodu značilo obavještavanje. (https://www.enciklopedija.hr/natuknica.aspx?id=27405). Bazdan (2009) objašnjava da su poslovne informacije sve one informacije koje prikupljamo sa svrhom stjecanja što boljih znanja i dobivanja što jasnije slike o nekoj stvari koja nam je u fokusu interesa. Takve su informacije od krucijalne važnosti jer na temelju njih može se stječi povoljna situacija i prednost na tržištu te imati što jasniji i kvalitetniji pogled na situaciju/stvar koja nam je bitna. Poslovne su informacije zapravo podaci koje poslovna inteligencija pretvara iz podataka u konačne informacije. Svrha je informacije pružiti što bolji i jasniji uvid u trenutačno stanje stvari. U današnje vrijeme u velikim kompanijama najvažnije su istinite i dobro provjerene informacije. Živimo u svijetu u kojem imamo na raspolaganju moderno opremljenu tehnologiju. U toj gomili informacija, često se nalaze i one koje su neupotrebljive ili su zastarjele te dovode do gubitka utrke s konkurentima na tržištu. Ponekad, informacije treba što brže diferencirati jer one često označuju i opstanak na tržištu.

Uz poslovne informacije često se veže pojam „Bussines Intelligence“ što znači poslovna inteligencija. Pojam „Business Intelligence-a” u svijetu je u uporabi 20-ak godina. Stoga ni u svjetskim relacijama nije postignuta suglasnost o njegovu generičkom određenju. Pojam kada je uveden odnosio se na industrijsku špijunažu. Javorović i Bilandžić (2007:167-168) navode da je poslovna inteligencija pristup obradi podataka koji transformira podatke u informacije, a te informacije onda transformira u znanja kojima se doprinosi poslovnom odlučivanju i ponašanju poduzeća. Poslovna se inteligencija ostvaruje u organiziranom integriranom informacijskom sustavu s usklađenim analitičkim i transakcijskim vrstama obrade podataka kao što su rudarenje podataka, obrada polustrukturiranih sadržaja, pohranjivanje podataka, itd. Glavni i osnovni cilj poslovne inteligencije jest uočiti povoljne poslovne prilike prije konkurenata. U smislu toga, Javorović i Bilandžić(2007:167) navode sljedeće: „Poslovna inteligencija usko povezana s time da si niti jedno ozbiljno poduzeće u današnjim uvjetima koji vladaju na tržištu ako se u obzir uzme žestoka konkurencija, sve zahtjevniji kupci, ubrzan tempo života i svijet koji se mijenja nevjerojatnom brzinom, ne može priuštiti donositi poslovne odluke na temelju osjećaja, na temelju subjektivnih procjena menadžera, intuitivnih spoznaja i sl . Poslovne su odluke raznolike i nose sa sobom visok rizik te se poslovni ljudi svakodnevno susreću s odlukama koje ozbiljno utječu na poslovanje, kako sadašnje tako i ono buduće.“

S obzirom na to da je na tržištu velik broj prikupljenih informacija te iste informacije treba i obraditi. Prikupljene informacije najčešće se obrađuju kroz rudarenje i skladištenje podataka. Prema Javoroviću i Bilandžiću(2007:171) Rudarenje predstavlja sortiranje po velikim količinama podataka i odabir najrelevantnijih podataka. Ovaj proces koriste svakodnevno sve velike kompanije kako bi pridonijele poboljšanju kvalitete odluka menadžera. Skladištenje podataka se još naziva i spremište podataka. Pripada bazama s više dimenzija koje su izrađene na osnovama dimenzijskog modela. Skladištenje ima četiri važna obilježja: integriranost, vremenska određenost, sadržajna nepromjenjivost i usmjerenost predmetima.

2.7. Povjerljivi podaci i zaštita podataka

Bazdan(2009) u svome radu navodi Zakon o gospodarskoj špijunaži SAD iz 1996. Koji je ujedno i prvi samostalni zakon protiv industrijske špijunaže , kojim je posebno je definiran institut poslovne tajne. Članak koji se odnosi na to glasi: : „Poslovna tajna je svaki oblik i svaka vrsta financijskih, poslovnih, znanstvenih, tehničkih, gospodarskih ili tehnoloških informacija, uključujući obrasce, planove, procedure, programe, ili kodove, vidljive ili nevidljive, bez obzira kako su spremljeni, organizirani ili sačuvani, elektronički, grafički, na fotografijama ili napisani-ako je: vlasnik poduzeo odgovarajuće mjere za očuvanje njihove tajnosti i ako informacije predstavljaju neovisnu ekonomsku vrijednost, aktualnu ili potencijalnu, odnosno ako nisu opće poznate i nisu bile prisutne u javnosti na bilo koji način.“ Članak 19. Zakona o zaštiti tajnosti podataka NN 79/07, NN 86/12 u daljnjem tekstu (ZZTP) definira poslovnu tajnu na sljedeći način: „Poslovnu tajnu predstavljaju podaci koji su kao poslovna tajna određeni zakonom, drugim propisom ili općim aktom trgovačkog društva, ustanove ili druge pravne osobe, a koji predstavljaju proizvodnu tajnu, rezultate istraživačkog ili konstrukcijskog rada te druge podatke zbog čijeg bi priopćavanja neovlaštenoj osobi mogle nastupiti štetne posljedice za njezine gospodarske interese.“ Člankom 19. (ZZTP) propisano je sljedeće: „Općim aktom se ne može odrediti da se svi podaci koji se odnose na poslovanje pravne osobe smatraju poslovnom tajnom niti se poslovnom tajnom mogu odrediti podaci čije priopćavanje nije razložno protivno interesima te pravne osobe.“ Također, člankom 19. (ZZTP) propisuje se sljedeće: „Poslovnom tajnom ne mogu se odrediti podaci koji su od značenja za poslovno povezivanje pravnih osoba niti podaci koji se odnose na zaštićeno tehničko unapređenje, otkriće ili pronalazak.“ Poslovna tajna ima veliku važnost za poduzeće. Predstavlja alat koji jača konkurentnost te upravlja

istraživačkim i razvojnim inovacijama samog poduzeća. Time se i povećava ukupna vrijednost poduzeća. Poslovna tajna, također predstavlja i poslovnu praksu ili određenu informaciju koja pomaže poslovnim subjektima da se natječu s konkurencijom. U poslovnim odnosima, poslodavac će posebnim općim aktom urediti pitanje poslovne tajne. Pojmovi vezani uz klasifikaciju podataka navedeni su i uređeni u Zakonu o tajnosti podataka. Članak 2. Zakona o tajnosti podataka NN 1108/96, propisuje klasificirani podatak na sljedeći način: „Klasificirani podatak je onaj koji je nadležno tijelo, u propisanom postupku, takvim označilo i za koji je utvrđen stupanj tajnosti, kao i podatak kojeg je Republici Hrvatskoj tako označenog predala druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje“ , dok članak 2. Zakona o tajnosti podataka, neklasificirani podataka propisuje na sljedeći način: „Neklasificirani podatak je podatak bez utvrđenog stupnja tajnosti, koji se koristi u službene svrhe, kao i podatak koji je Republici Hrvatskoj tako označenog predala druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje.“

Osobni podaci su najvrjednija roba koju čovjek posjeduje. Najvažnije je da se osobni podaci dobro zaštite i da se ne zloupotrebljavaju. Opća uredba o zaštitu osobnih podataka (GDPR) usvojena je od strane parlamenta 14.travnja 2016.godine. Počinje se primjenjivati 25.svibnja 2018.godine. Glavni ciljevi ove uredbe su: usklađivanje zakona o zaštiti podataka u cijeloj Europi, zaštita i osnaživanje osobnih podataka svih građana EU te pružiti kontrolu građanima nad njihovim osobnim podacima. Osim toga, Opća uredba olakšava poduzećima poslovanje na tržištu te pojednostavljuje prekogranični protok podataka. Načela obrade osobnih podataka su: zakonitost, poštenost i transparentnost, ograničavanje svrhe, smanjenje količine podataka, točnost, cjelovitost i povjerljivost, točnost i pouzdanost. Neka od prava ispitanika su: pravo na informiranje, pravo na ispravak, pravo na brisanje, pravo pristupa, pravo na prigovor, pravo na prijenos podataka... Ne primjenjuje se na: nacionalnu sigurnost, zajedničku vanjsku i sigurnosnu politiku EU, u svrhu istrage, otkrivanja ili progona kaznenih djela te na aktivnosti fizičke osobe za vlastite potrebe. Važnost GDPR-a danas je od velikog značaja i brojni su propisi koje za sobom nosi navedena uredba. Složen zakon koji donosi mnoge novosti i mijenja način rada. Propise unutar zakona treba poštivati kako bi zaštita osobnih podataka bila najvišoj razini i kako ne bi došlo do određenih sankcija koje mogu biti na štetu raznim poduzećima. (https://gov.hr/hr/sto-je-opca-uredba-o-zastiti-podataka-eng-general-data-protection-regulation-gdpr/1868)

2.7.1. Zaštita patenata

Državni zavod za intelektualno vlasništvo definira patent na sljedeći način: Patent je isključivo pravo priznato za izum koji nudi novo rješenje nekog tehničkog problema. Patent se priznaje za izume koji se odnose na proizvod, postupak ili primjenu.“ (https://www.dziv.hr/hr/intelektualno-vlasnistvo/patenti/regionalna-zastita/)

Priznanje patenata provodi Europski patentni ured koji pruža zaštitu na regionalnoj razini za zemlje članice Europske patentne organizacije. Članice patentne organizacije ne moraju biti članice Europske unije te je danas, zaštita omogućena u 38 europskih zemalja. Unatoč pandemije, broj podnesenih prijava Europskih patenata nije se znatno smanjio, samo za 0,7 posto. Zemlje koje imaju zaprimljen najveći broj patentnih prijava su: Njemačka, Japan, Francuska, Kina i SAD. Vodeći prijavitelji na svjetskoj razini su Samsung i Huawei. U Hrvatskoj postupak zaštite patenata započinje podnošenjem prijave patenata Državnom zavodu za intelektualno vlasništvo, koja mora biti u skladu sa Zakonom i Pravilnikom o patentu. Postupak se sastoji od dvije bitne faze. Prva je ispitivanje sadržaja prijave patenata do objave prijave u službenom glasilu Zavoda, a druga je ispitivanje nakon objave. Nakon toga, podnositelj je dužan podnijeti zahtjev za potpuno ispitivanje, kojim se onda odlučuje o priznanju ili odbijanju zahtjeva za priznanje patenata. Trajanje zaštite patenta može trajati najviše 20 godina od datuma podnošenja prijave patenta uz obavezno plaćanje propisane godišnje naknade. (https://www.dziv.hr/hr/intelektualno-vlasnistvo/patenti/postupak-zastite-patenta/) „Prema broju prijava, Hrvatska je zabilježila porast od 15.8%, što ju svrstava na 27. mjesto od 27 zemalja članica Europske Unije. Po broju Europskih prijava Hrvatska je na 34. mjestu između 38 članica EPO-a. U odnosu na broj prijava na milijun stanovnika Hrvatska je na 43. mjestu među „top 50“ zemalja iz kojih je EPO u 2020. godini zaprimio prijave.“ (https://www.dziv.hr/hr/novosti/objavljeno-epo-statisticko-izvjesce-za-2020,5841.html)

2.8. Hibridne prijetnje kao način ugrožavanja gospodarstva

Hibridne prijetnje najčešće se odnose na slabosti određene države, odnosno njenog gospodarstva. Takvim prijetnjama nastoje se ugroziti i temeljna demokratska prava i slobode. Hibridnim prijetnjama dolazi se do ozbiljnih društvenih i gospodarskih problema unutar određene zemlje. Veliku ulogu u suzbijanju hibridnih prijetnji ima Europska unija koja koristeći se svojim instrumentima i politikama podiže svijest o sigurnosnom okruženju.

Postoje razne definicije koje opisuju hibridne prijetnje. Najčešće se opisuju kao prijetnje koje su promjenjive prirode te zbog toga moraju biti i fleksibilne. U ovakvu vrstu prijetnji spadaju prisilne aktivnosti te razne vojne, gospodarske, tehnološke i diplomatske metode koje državni sudionici upotrebljavaju kako bi postigli određene ciljeve, a da pritom službeno ne objavljuju rat. Glavni cilj hibridnih prijetnji je destabilizirati određenu zemlju ili regiju. Ovakvim pristupom najčešće stradava prvenstveno infrastruktura koju je vrlo važno zaštiti. Tu su posebno ranjive energetske mreže, sigurnost prometa, obrambeni kapaciteti, zaštita zdravlja(javno zdravstvo) i sigurnost hrane te kibernetička sigurnost.

Danas, u petu dimenziju ratovanja spada tzv. *cyber* ratovanje koje se vodi u kibernetičkom prostoru, a koriste se razna tehnologija kao što su računala i internet. *Cyber* ratovanje je ratovanje koje vode mnogobrojne zemlje, kompanije i organizacije. Kako vojnici rabe oružja tijekom ratovanja tako cyber napadači rabe računalne mreže, internet i telekomunikacijske sustave preko kojih vrlo lako i brzo mogu naštetiti gospodarstvu te sustavima određene zemlje kao što su politički i vojni sustavi. (https://hrvatski-vojnik.hr/odgovor-na-cyber-prijetnje/)

Hibridne prijetnje itekako predstavljaju veliki izazov kako za Europsku uniju, tako i za Ujedinjene narode. Glavni zadatak navedenih dviju organizacija je brza i učinkovita reakcija svake države članice na hibridne prijetnje. Zbog toga, države članice trebaju razvijati suradnju s međunarodnim organizacijom, među kojima glavnu ulogu ima NATO.

Republika Hrvatska je 29. lipnja 2021. postala članica Europskog centra izvrsnosti za suzbijanje hibridnih prijetnji. Europski centar izvrsnosti za suzbijanje hibridnih prijetnji predstavlja instituciju u kojoj se razvijaju sredstva koja pomažu od hibridnih prijetnji. Centar jača savezničke i europske sigurnosti. Također, centar služi i kao središte stručnog znanja za podršku sudionicima koji žele unaprijediti svoje vojne i civilne sposobnosti. Aktivnim sudjelovanjem u centru, Hrvatska će biti otpornija na hibridne prijetnje te steći iskustvo za

Republika Hrvatska je 29. lipnja 2021. postala članica Europskog centra izvrsnosti za suzbijanje hibridnih prijetnji. Europski centar izvrsnosti za suzbijanje hibridnih prijetnji predstavlja instituciju u kojoj se razvijaju sredstva koja pomažu od hibridnih prijetnji. Centar jača savezničke i europske sigurnosti. Također, centar služi i kao središte stručnog znanja za podršku sudionicima koji žele unaprijediti svoje vojne i civilne sposobnosti. Aktivnim sudjelovanjem u centru, Hrvatska će biti otpornija na hibridne prijetnje te steći iskustvo za unaprjeđenje nacionalnog sustava suzbijanja hibridnih prijetnji. (https://mvep.gov.hr/press/224897)

3. ISTRAŽIVANJE

U ovom poglavlju prikazano je istraživanje metodom dubinskog intervjua koje je provedeno u industrijskom poduzeću „WE KR.“ Kroz poglavlja opisana je metodologija i rezultati istraživanja. Na kraju se nalazi kratak rezime provedenog istraživanja.

3.1. Metodologija istraživanja

U ovom istraživačkom radu prikupljeni su primarni podaci kroz jednokratno kvalitativno istraživanje na namjernom uzorku. Empirijsko istraživanje provedeno je putem metode dubinskog intervjua. Istraživanje je provedeno metodom intervjua kako bi se dobila što jasnija i opsežnija slika problema istraživanja. Za potrebe istraživanja sastavljena su pitanja otvorenog tipa. Istraživanje na temu “Negativni učinci industrijske špijunaže na gospodarstva razvijenih zemalja” provedeno je na jednom ispitaniku, točnije na zaposleniku poduzeća “WE-KR.” koji je ujedno i direktor navedenog poduzeća. Glavni ciljevi istraživanja su istražiti i analizirati svijest tvrtke „WE-KR“ o industrijskoj špijunaži. Istražiti da li je tvrtka bila suočena s industrijskom špijunažom, ako jest opisati kako se to odrazilo na samu tvrtku. Istražiti kako tvrtka štiti svoje poslovne informacije i podatke.

3.2. Rezultati istraživanja

Intervju se odvijao u prostorima industrijskog poduzeća „WE-KR“ te je ukupno trajao 45 minuta. Na prvo pitanje je li tvrtka upoznata s industrijskom špijunažom, odgovor je glasio da je jest, no poduzeće nikada nije bilo sklono industrijskoj špijunaži jer se poduzeće ne koristi neetičkim nelegalnim postupcima kako bi došli do bitnih informacija i podataka. Navedeno je da se smatra da je glavni razlog kojim se može izbjeći ovakva vrsta špijunaže stalno unaprjeđenje tehnologije i praćenje promjena koje se odvijaju na tržištu. Iduće pitanje odnosilo se na odnos sa zaposlenicima. Ispitanik je odgovorio da poduzeće trenutno zapošljava 160 visokomotiviranih djelatnika u što se ubrajaju 16 naučnika. Pomoću raznih programa za školovanje i usavršavanje kontinuirano proširuju i unapređuju kompetencije djelatnika. S redovitim investicijama u djelatnike i moderna postrojenja, kao i inovacije i nove tehnologije godinama dokazuju svoj poduzetnički uspjeh. Također je rečeno da je zadovoljstvo djelatnika i kupaca unutar poduzeća uvijek na prvom mjestu. Osobni podaci zaposlenika u poduzeću čuvaju se u propisanim normama, u elektroničkom ili pisanom

obliku, gdje pristup imaju samo ovlaštene osobe. Za elektroničke mape potrebni su pristupni kodovi dok su papirnati dokumenti u prostorijama koje se zaključavaju. Poduzeće je upoznato s Uredbom o zaštiti osobnih podataka te istu primjenjuje kako je zakonski propisano u Republici Hrvatskoj od 2018. godine. Ispitanik je naveo da smatra da je jedna od najgorih stvari koja se može dogoditi direktoru da doživi povredu podataka. Naveo je da smatra da se u tom trenutku ne smije umanjivati važnost ili najgore negiranje postojanja povrede. Iskreno objasniti što se dogodilo jer samim time stvara se i povjerenje. Zbog toga direktor ovog poduzeća, nastoji uvijek pružati točne i aktualne informacije svim djelatnicima i javnosti. Na primjeru izjave o tajnosti informacija ispitanik je objasnio pojam poslovne tajne. U toj izjavi sudjeluje Dürr, globalna tvrtka za strojarstva i postrojenja. Informacije u smislu ove obveze povjerljivosti su sve tehničke i komercijalne informacije, posebice crteži, planovi, specifikacije, metode, formule, uzorci, dokumentacija, izračuni, podaci o tržištu i kupcima, kao i materijali i drugi predmeti koji su izravno ili neizravno povezani do pokretanja ili izvršenja poslovnog odnosa opisanog od strane Dürra, bilo u usmenom, vizualnom, pisanom obliku ili putem nosača podataka ili na bilo koji drugi način. Podatke koje je Dürr otkrio primatelj će tretirati kao strogo povjerljive i neće ih prosljeđivati trećim stranama niti ih koristiti u vlastite komercijalne svrhe ili drugi klijenti bez prethodnog pismenog pristanka Dürra. Osobito se primatelj također mora suzdržati od oponašanja putem takozvanog "obrnutog inženjeringa". Primatelj će podatke koristiti samo u svrhu koju je odredio ili dopustio Dürr. Osim toga, primatelj se obvezuje osigurati odgovarajuće mjere povjerljivosti. Primatelj će informacije primljene od Dürra učiniti dostupnim odabranim zaposlenicima samo u mjeri koja je apsolutno neophodna u svrhu koju je Dürr odredio ili dopustio. U mjeri u kojoj je to dopušteno zakonom, primatelj će te zaposlenike obvezati na čuvanje tajnosti za vrijeme trajanja radnog odnosa, kao i vrijeme nakon njegovog prestanka u skladu s uvjetima ove obveze neotkrivanja podataka. Za svaki slučaj kršenja jedne od obveza preuzetih ovom obvezom povjerljivosti, primatelj će Dürru platiti ugovornu kaznu do 50.000 eura, koju će Dürr odrediti prema razumnom nahođenju i čiji iznos može preispitati nadležni sud prema ovaj sporazum. Dürr zadržava pravo na daljnje zahtjeve za naknadu štete i zabranu; oduzeta ugovorna kazna se prebija sa zahtjevom za naknadu štete.

Tijekom intervjua ispitanik je naveo da ponekad primaju neželjenu poštu, poput raznih reklama na koje ne bi trebalo nasjedati. Kada se govori o konkurenciji, „WE-KR“ do bitnih poslovnih informacija o konkurenciji dolazi putem javno dostupnih načina orijentiranih za prikupljanje podataka tj. istraživanje tržišta kao što su javna dokumentacija poduzeća,

financijske institucije, Eurostat ili Hrvatski državni zavod za statistiku, Hrvatska gospodarska komora, sudski registar, baze poslovnih podataka i slično.

3.3. Ograničenja istraživanja

Provedeno istraživanje bilo je djelomično ograničeno jer se na određena pitanja u vezi samog poduzeća ne smiju otkrivati. Prije samog provođenja intervjua, potrebna je najava preko elektroničke pošte uz konkretan razlog provođenja kako bi se intervju mogao prihvatiti i održati.

3.4. Osvrt na istraživanje

Nakon provedenog ispitivanja može se zaključiti da industrijska tvrtka „WE KR“ nije bila sklona industrijskoj špijunaži te posluje na pravilan način, poštujući zakonske regulative što se može zaključiti po opisu poslovne tajne s glavnim partnerom „WE-KR“-a, Dürrom . Usredotočena je na osobni rast i razvitak što je i najvažnije za poslovanje svakog poduzeća. Povjerljivi podaci su zaštićeni te se poštuju ljudska i radnička prava.

4. ZAKLJUČAK

Ovim završnim radom prikazuje se najveći fenomen svih vremena, a to je industrijska špijunaža i njezino djelovanje na nacionalna gospodarstva. Špijunaža se javlja, već u ranoj prošlosti te se špijuni u to vrijeme koriste za vojne svrhe. Poznata imena špijuna poput Fleminga i Casanove još se uvijek često pojavljuju i spominju u raznim medijima i knjigama. Danas se u potpunosti može prihvatiti izreka „vrijeme je novac.“ što bi značilo da se prava informacija treba iskoristiti u pravo vrijeme. To je vrlo važno za daljnji opstanak na tržištu. U tome svemu vrlo važnu ulogu ima proces Bussines Intelligence koji pomaže da u najkraćem mogućem vremenu dođemo do bitne informacije.

Glavni cilj rada bio je istražiti kako industrijska špijunaža utječe na ekonomiju i kako se to odražava na velike kompanije ili poduzeća. Također, koliko negativno može djelovati na gospodarstva i koje su najčešće metode industrijske špijunaže kojima se narušavaju nacionalna gospodarstva. Provedeno je istraživanje u industrijskom poduzeću „WE-KR“ pomoću kojeg se prikazalo na konkretnom primjeru pojam poslovne tajne koja je jedna od glavnih objekata industrijske špijunaže. Naglašena je zaštita osobnih podataka te važnost Uredbe o zaštiti osobnih podataka. Važno je da se svaka pravna i fizička osoba koja obrađuje podatke u komercijalne svrhe drži zakona i propisa koji reguliraju određeno područje. Neki od bitnih zakona koji reguliraju zaštitu podataka su: Zakon o zaštiti tajnosti podataka, Zakon o informacijskoj sigurnosti, Zakon o tajnosti podataka. Najvažniji zakon koji regulira špijunažu u Republici Hrvatskoj je Kazneni zakon.

Danas, svaka država mora biti spremna na špijunaže, koje će sve više biti prisutne tijekom 21. stoljeća. Za uspješno poslovanje najvažnije je stalno praćenje promjena na tržištu te unaprjeđenje i zaštita tehnologije i podataka. Za zaključak ovog rada može se izdvojiti poznata izreka Petera Druckera, koja glasi: „Kada vidiš uspješno poduzeće, znaj da je jednom netko donio hrabru odluku.“

LITERATURA

1. Aras, S. (2007). „Korupcija“ , Pravnik, 41 (84), 25-59

2. Bazdan, Z. (2009.). „ POSLOVNA OBAVJEŠTAJNA DJELATNOST – KLJUČAN ČIMBENIK POSLOVNE IZVRSNOSTI CASE STUDY: INDUSTRIJSKA ŠPIJUNAŽA“, Poslovna izvrsnost, Vol.3(1), 57-75.

3. Bazdan Z. (2011.). „Gospodarska diplomacija i patološki trendovi globalne ekonomije“ ,Poslovna izvrsnost, Vol.5, 103-124.

4. Bazdan, Z. (2016.). „POSLOVNO-OBAVJEŠTAJNE SLUŽBE, INDUSTRIJSKA I GOSPODARSKA ŠPIJUNAŽA U MEĐUNARODNOJ EKONOMIJI“ , Zbornik Sveučilišta u Dubrovniku, Vol.3, 49-72.

5. Bug-dostupno 23.08.2022. na https://www.bug.hr/sigurnost/ina-sanirala-korisnicima-vidljive-posljedice-kibernetickog-napada-14269

6. Cert.hr.-dostupno 23.08.2022. na https://www.cert.hr/19795-2/ransomware/

7. Ćosić,D. (2008.): „ Poslovnost i izvjesništvo“ , National security and the future, Vol.9(1-2), 53-76.

8. Državni zavod za intelektualno vlasništvo-dostupno 3.09.2022. na https://www.dziv.hr/hr/intelektualno-vlasnistvo/patenti/sto-je-patent/

9. Državni zavod za inelektualno vlasništvo- dostupno 3.09.2022. na https://www.dziv.hr/hr/novosti/objavljeno-epo-statisticko-izvjesce-za-2020,5841.html

10. Đorđević, O. (1978). Šta je špijunaža. Beograd: Politika.

11. Economic Espionage Act (1996), 18 U. S. C., paragraphs: 1831–1839. , Washington.

12. Hrvatski vojnik- dostupno 23.08.2022. na https://hrvatski-vojnik.hr/odgovor-na-cyber-prijetnje/.

13. Informacija, Hrvatska enciklopedija, Leksikografski zavod Miroslav Krleža- dostupno 1.06.2022. na https://www.enciklopedija.hr/natuknica.aspx?id=27405.

14. Industrijska špijunaža u stalnom je porastu, MojPosao- dostupno 1.06.2022. na https://www.moj-posao.net/Vijest/61881/Industrijska-spijunaza-u-stalnom-je-porastu/ .

15. Industrijska špijunaža, Struna, Hrvatsko strukovno nazivlje- dostupno 1.06.2022.na http://struna.ihjj.hr/naziv/industrijska-spijunaza/51107/.

16. ITPro-dostupno 23.08.2022. na https://www.itpro.co.uk/security/cyber-security/354818/uk-among-countries-most-likely-to-encounter-cloud-attacks

17. Javorović, B., Bilandžić, M(2007.). :Poslovne informacije i business inteligence, Golden marketing, Zagreb, str. 166-175.

18. Leko,V., Požega, Ž.(2016.). : „UTJECAJ LJUDSKOG FAKTORA NA RAZVIJENOST ZEMALJA“ , Tranzicija, Vol.18, 67-88

19. Ministarstvo vanjskih i europskih poslova RH- dostupno 23.08.2022. na https://mvep.gov.hr/press/224897 .

20. Ministarstvo unutarnjih poslova Republike Hrvatske-dostupno 5.09.2022. na https://mup.gov.hr/UserDocsImages/statistika/2022/Statisticki_pregled_2021_Web.pdf.

21. Najpoznatiji špijuni u svijetu, Dnevnik.hr. – dostupno 1.06.2022. na https://dnevnik.hr/vijesti/svijet/najpoznatiji-spijuni-u-povijesti.html.

22. Špijunaža, Hrvatska enciklopedija, Leksikografski zavod Miroslav Krleža- dostupno 1.06.2022. na https://www.enciklopedija.hr/natuknica.aspx?id=59838.

23. Što je opća uredba o zaštiti podataka (eng. General Data Protection Regulation - GDPR) E-građani- dostupno 1.06.2022. na https://gov.hr/hr/sto-je-opca-uredba-o-zastiti-podataka-eng-general-data-protection-regulation-gdpr/1868
.

24. Zakon o tajnosti podataka. NN 79/07, NN 86/12.

25. Zakon o zaštiti tajnosti podataka. NN 1108/96.

26. Zimo- dostupno 23.08.2022. na https://zimo.dnevnik.hr/clanak/cyber-napadi-sve-cesci-na-hrvatsku---717678.html

PRILOZI

Intervju se sastoji od sljedećih pitanja:

1. Je li poduzeću "WE-KR" poznat pojam industrijska špijunaža?

2. Je li poduzeće u kojem radite bilo sklono industrijskoj špijunaži?

3. Ako jest, kako se to odrazilo na samo poduzeće?

4. Kakav je Vaš odnos sa zaposlenicima?

5. Jeste li upoznati s Uredbom o zaštiti osobnih podataka (General Data Protection Regulation?

6. Na koji način se čuvaju osobni podaci zaposlenika u poduzeću?

7. Jeste li upoznati s pojmom "poslovne tajne?"

8. Primate li neželjenu poštu, poput reklama?

9. Na koje načine dolazite do bitnih poslovnih informacija o konkurenciji?

10. Koliko često unaprjeđujete tehnologiju s kojom radite (računala, računalni programi, aplikacije…)?

IZJAVA O AUTORSTVU ZAVRŠNOG RADA

Ovime potvrđujem da sam osobno napisala završni rad pod naslovom „Negativni učinci industrijske špijunaže na gospodarstva razvijenih zemalja.“ Svi dijelovi rada, nalazi ili ideje koje su u radu citirane ili se temelje na drugim izvorima su označeni te takvi navedeni u popisu literature.

Helena Vincek