GOSPODARSKA ŠPIJUNAŽA – PARADIGMA MODERNOG SVIJETA

Tomislav Đozić*

Sažetak: *Gospodarska špijunaža u rudimentarnim oblicima egzistira još od vremena najstarijih civilizacija. Razvojem društava i gospodarstava razvijale su se i njezine metode koje su postajale sve sofisticiranije. Danas u svijetu egzistiraju brojni pojmovi koji se izravno ili neizravno vežu s područjem koje obuhvaća pojam gospodarske špijunaže. Temeljna podjela, odnosno razdjelnica među njima ogleda se u tome primjenjuju li njihovi nositelji legalne i/ili nezakonite metode djelovanja. U praksi čest je slučaj da se kombiniraju različite metode radi lakšeg prikrivanja. Nositelji mogu biti različiti, od obavještajnih struktura, poslovnih kompanija iza kojih stoje državne ili političke elite, pa sve do tvrtki koje se bave legalnim business intelligenceom. Postoje i brojni primjeri suradnje između gospodarskih/poslovnih kompanija te obavještajnih službi na području prikupljanja informacija gospodarske naravi. Upravo zbog toga u praksi je teško odrediti stvarne nositelje gospodarske špijunaže. U tim aktivnostima nema prijatelja ili saveznika, to je „rat" koji vode svi protiv svih. Metode koje se pritom rabe obuhvaćaju širok spektar djelovanja, od onih banalnih (upiti, slanje e-mailova, stručna usavršavanja itd.) do onih sofisticiranijih koji uključuje elektronsko presretanje različitih oblika komunikacija.*

* Stavovi izneseni u ovom članku osobni su stavovi autora i ne mogu se ni pod kojima uvjetima smatrati službenim stavovima tvrtke u kojoj je autor članka zaposlen.

Ciljana područja gospodarske špijunaže su različita te vrlo često ovise o stupnju tehnološkog razvoja pojedine zemlje. Dok se slabije i srednjerazvijene zemlje zadovoljavaju i s pribavljanjem starijih tehnologija do kojih je ujedno i lakše doći zbog niže razine njihove zaštite, razvijene zemlje Zapada se nastoje domoći najsuvremenije tehnologije posljednje generacije. Posebno zanimljive mete su osim dual-use tehnologija, područje energetike, komunikacija, ekologije, farmacije, informatike, kemijske industrije te laserske i nuklearne tehnologije.Štetni učinci gospodarske špijunaže mjere se u milijardama USD-a i eura, a u konačnici slabljenjem pojedinih gospodarskih grana te nacionalnih gospodarstava i smanjenjem konkurentnosti na globalnom tržištu.

Ključne riječi: gospodarska špijunaža, pojmovne razlike, metode djelovanja, realizatori gospodarske špijunaže, ciljevi gospodarske špijunaže, obavještajne službe, poslovne kompanije, gospodarske interesi, štetni učinci.

Summary

Economic espionage in primary forms existed since the time of ancient civilizations. Development of societes and economies have developed and method that are becoming increasingly sophisticated. In the world today exist numerous terms that are directly or indirectly associated with the area encompasses the notion of economic espionage. The fundamental division, that division between the two is reflected in whether their holders apply legal and/or illegal methods for easy concealment. Holders can be different from the intelligent structures, business companies backed by the state or political elite, to companies engaged in lawful business intelligence. There are numerous examples of cooperation between economic/business company and intelligence services in the field of information gathering economic nature. That is why it is difficult to determine the actual holders of economic espionage. In these activities from trivial ones (questions, send e-mails, specialization training etc.) to those involving sophisticated electronic surveillance and interceptions of various forms communications. Target areas of economic espionage are different and often depend on the level of technological development of a country. While weaker

and middle-developed countries meet with older technolgy by obtaining them is also easier to get because of their lower level protection, the developed countries of the West are trying to get hold of the latest generation of leading-edge technologv. Especially interesting are the targets: dual-use technology, the fielsd of energy, communications, environmental, pharmaceutical, IT, chemical industry, and laser and nuclear technology. Adverse effects of economic espionage are measured in billions of U.S. dollars and euros and ultimately weaking of certain industries and national economies and reducing competitiveness in the global market.

Keywords: economic espionage, conceptual diferences, method of operations, organizers of economic espionage, the objectives of economic espionage, intelligence agencies, commercial companies, economic interests adverse effects.

Uvod

Gospodarska špijunaža egzistirala je još od najstarijih civilizacija, doduše u vrlo pojednostavljenim oblicima. Poznat je primjer iz državnog ustroja starog Egipta gdje su pojedini svećenici koji su odlazili u strane zemlje sustavno obučavani za zadaće prikupljanja podataka o njihovoj gospodarskoj snazi. Također, oko 1200 godina prije Krista, a tijekom izraelskog pohoda na Palestinu, Jošua je uputio dvojicu svojih uhoda da „tajno izvide da li je zemlja plodna“. Ovakvih, relativno pojednostavljenih primjera gospodarske špijunaže te primjera koji su obuhvaćali sustavniji pristup navedenoj problematici tijekom povijesti bilo je bezbroj.

Razvoj država, društva, društvenih odnosa i gospodarstva doprinio je značajnijem razvoju gospodarske špijunaže, a njezine metode su postale sve sofisticiranije. Danas, gospodarska špijunaža egzistira kao sustavna i visokorazvijena djelatnost poticana i usmjeravana od brojnih zemalja kako onih nerazvijenih i srednjerazvijenih tako i onih visoko razvijenih. Njezini štetni učinci mjere se u milijardama dolara i/ili eura, a njezine posljedice često puta snažno, negativno, utječu na cjelokupno nacionalno gospodarstvo pojedinih država.

Pojmovna distinkcija

U svjetskoj stručnoj i znanstvenoj javnosti (pa tako i hrvatskoj) danas ne postoji potpuno suglasje o pojmovima kao što su industrijska špijunaža, gospodarska špijunaža, intelligence, business intelligence (BI), špijunaža općenito i drugo. Temeljna podjela odnosi se na podjelu između business intelligencea koji je legalna metoda djelovanja poslovnih kompanija u svom poslovnom okružju, odnosno na tržištu te gospodarske špijunaže koja predstavlja nedopustivo prikupljanje osjetljivih poslovnih/gospodarskih informacija na nezakonit način.

Nadalje, potrebno je uočiti distinkciju pojmova business intelligence i industrijske/gospodarske špijunaže. Vjerojatno najprecizniju definiciju ovih pojmova, koja je ujedno prihvaćena u javnosti, daje John F. Quinn[1] koji smatra kako je BI legalna, a industrijska ili gospodarska špijunaža to nije. Tako je tijekom jednog svog predavanja na konferenciji[2] o business intelligenceu u svibnju 1994. u Mc Leanu u Virginiji (SAD), Quinn iznio kako proces BI-a vidi kao proces prikupljanja poslovnih ili konkurentskih informacija putem legalnih i etičkih metoda uključujući novine, časopise Internet te posebne baze podataka, dok industrijska ili gospodarska špijunaža predstavlja „potajno prikupljanje osjetljivih, restriktivnih ili posebno klasificiranih informacija“, s time da industrijska špijunaža obuhvaća i krađu informacija od svojih izravnih poslovnih konkurenata.

Kanadski stručnjak za međunarodne odnose, jedan od utemeljitelja časopisa Canadian Foreign Policy i dugogodišnji voditelj studija „Menadžment konflikta i pregovaranje“ na Sveučilištu u Torontu, Evan Potter, radi jasnu podjelu pojmova kao što su economic espionage, industrial espionage i economic espionage. Prema Potteru, gospodarska špijunaža (economic espionage) obuhvaća „potajna i nedopuštena nastojanja inozemnih zemalja koja u korist vlastitih gospodarskih interesa i pritom se mogu služiti i sabotažama ili nekim drugim nedopuštenim sredstvima,

1 John F. Quinn je rođen u Massachusetsu, u SAD-u. Znatan dio radnog vijeka proveo je u Japanu gdje je i tečno naučio japanski jezik. Bio je dugogodišnji dužnosnik CIA-e. U svom djelokrugu bavio se poslovnim i tehnološkim razvojem Japana i drugim razvijenim zemljama Dalekog Istoka. Niz godina predaje predmet business intelligence (BI) na sveučilištima u Sofiji i Tokiju. Osim toga, John B. Quinn je stručni savjetnik u različitim kompanijama koje se bave BI i primjenom suvremenih informacijskih i drugih tehnologija. Također se zauzima za strateške poslovne saveze japanskih i američkih kompanija u nastupu prema trećim tržištima.

2 www.nsi.org/Library/Intel/japanesp.html

zadiru u gospodarsku sigurnost drugih zemalja“[3]. Potter definira pojam industrijske špijunaže kao uporabu ilegalnih, potajnih i prinudnih ili prijevarnih načina ili metoda da se dođe do određenih spoznaja unutar dva subjekta u privatnom sektoru[4].

Nadalje, Potter smatra kako pojam economic intelligencea obuhvaća politiku ili komercijalno relevantne gospodarske informacije, uključujući financijske, trgovinske i informacije pojedine vlade koje pomažući vlastitim nacionalnim interesima (državnim interesima ili interesima gospodarskih subjekata) izravno ili neizravno pomažu u podizanju relativne učinkovitosti i produktivnosti ili pomažu konkurentnosti vlastitog gospodarstva u svijetu (za što imamo više primjera u svijetu: možda najeklatantniji su Kina, Južna Koreja i među prvima Japan). Također, Potter smatra kako economic intelligence može snažno pomoći jednoj državi nauštrb druge, što će se posebno ogledati u različitim poslovima gospodarske prirode, investicijama, produktivnosti, konkurentnosti ili gospodarskom rastu.[5]

Kanadski stručnjak klasificira i raščlanjuje tipove gospodarske špijunaže:

1. Primarna i sekundarna gospodarska špijunaža – „zelena“ i „žuta“ zona:

Prikuplja informacije iz otvorenih izvora kao što su istraživački centri, sveučilišne baze podataka, knjižnice, trgovačka društva ili udruge, javni mediji, Internet, specijalizirane publikacije, različiti think – tankovi. Često puta obuhvaća i prikupljanje podataka o različitim makroekonomskim analizama ili trendovima. Osnovna razlika između dvije razine tj. zelene i žute onosi se na stupanj težine/lakoće kojom se prikupljaju javni podaci i informacije.

2. Taktička gospodarska špijunaža – „crvena“ zona

Informacije se prikupljaju na relativno osjetljiv način i putem privilegiranih izvora kao što su: osobni kontakti između menadžera pojedinih kompanija tijekom poslovnih susreta, sudjelovanje na usko specijaliziranim simpozijima za strogo određeni krug korisnika, uporaba internih baza podataka u pojedinim kompanijama uključujući analize pojedinih tržišta, interna izvješća o kvaliteti i znanstvenim potencijalima

3 E: Potter, Economic Intelligence & National Security, Carlton University Press & The Center for Trade Policy and Law, Canada, 1998., predgovor

4 Ibid.

5 Ibid.

u pojedinim tvrtkama, informacije o budućim projektima određene tvrtke. U obavještajnim krugovima zapadnih zemalja ovaj tip informacija se često označava kao „sakrivena“ informacija. Samo u određenim okolnostima ovakva vrsta špijunaže može se okarakterizirati kao neetička. U ovom slučaju prikupljaju „se sirovi“, odnosno neobrađeni, podaci na nižim razinama. Uz pomoć analitičkih alata kasnije nastaju nove taktike i strategije koje kompanije rabe u svojim aktivnostima na svjetskom tržištu.

3. Tajna gospodarska špijunaža – „crna“ zona

Prikupljanje informacija na nedopuštene i ilegalne načine svim mogućim metodama i sredstvima (tehnička sredstva, ljudski resursi). Ovakve informacije prikupljaju se pomoću specijaliziranih i visokoprofesionalnih skupina kao što su pravnici, stručni i financijski savjetnici, agenti obavještajnih službi itd. Prikupljanjem ovakvih, najčešće strateških informacija, gaze se svi etički standardi, a dolaženje u posjed istih znači za pojedinu tvrtku ili državu komparativnu prednost pred političkim protivnicima ili gospodarskim konkurentima.

U kontekstu različitih tumačenja špijunaže, potrebno je navesti kako pojedini analitičari i stručnjaci pod „industrijskom ili konkurencijskom špijunažom“ podrazumijavaju djelovanje konkurentske kompanije, dok drugi pod tim pojmom podrazumijavaju obavještajnu djelatnost koja se provodi od strane različitih čimbenika. Zanimljiv je primjer Njemačke gdje se zbog boljeg razumijevanja te zakonskih okvira u kojima djeluje tamošnja Savezna služba za zaštitu Ustava (BfV) nastoje što konkretnije razlučiti razni oblici špijunaže što je uostalom i sve češći slučaj u razvijenim zapadnim zemljama koje su najčešće na udaru gospodarske špijunaže.

Kao temeljna razdjelnica u pojmovima egzistira slijedeća podjela:

-„Industrijska ili konkurencijska špijunaža“ u pravilu cilja na određene proizvode i znanstvene ili poslovne projekte te je najčešće kratkoročne naravi;

-„Gospodarska špijunaža“ dugoročno je koncipirana i teži prikupljanju što je moguće opsežnijih informacija iz gospodarskih sfera i gotovo uvijek iza nje stoji vlada neke strane zemlje.

Dosadašnja praksa pokazala je da je u većini slučajeva vrlo teško odrediti granicu između prikupljanja informacija koje provode državne institucije u skladu s državnim interesima i privatnog prikupljanja informacija od strane

pojedinih kompanija iza kojih stoje interesi privatnog kapitala, odnosno njegovih vlasnika. Ovakvi, često puta komplementarni interesi gospodarskih subjekata i obavještajnih službi već su duže vrijeme realnost u današnjem svijetu.

Različiti aspekti redefiniranih gospodarskih i obavještajnih sfera i njihova međusobna interakcija

Za razliku od hladnoratovskog razdoblja kada je protivnik bio jasno označen kroz političku i ideološku sferu, nove, izmijenjene, okolnosti u međunarodnim političkim i gospodarskim odnosima donose i izmijenjene prioritete u djelovanju službi, odnosno zadaća dobivenih od strane političkih elita. Vojna problematika prestaje biti jedan od važnijih prioriteta u aktivnostima službi već to, između ostalog, postaju: globalno gospodarsko nadmetanje, komercijalni patenti i pronalasci, znanstvena istraživanja, načini poslovanja i pregovaračka strategija svjetskih kompanija itd.

Obavještajne službe slabije i srednjerazvijenih zemalja, poglavito Kine, Rusije te nekih drugih azijskih i južnoamaeričkih zemalja, intenziviraju svoje aktivnosti na prikupljanju strateških gospodarskih informacija. Njihov cilj je ovladavanje suvremenim sofisticiranim tehnologijama kako bi smanjili zaostajanje svojih zemalja za razvijenim zemljama Zapada. Karakteristično je da su u jednakoj mjeri značajno intenzivirane i obavještajne aktivnosti zapadnoeuropskih zemalja i SAD-a, čije obavještajne službe, usko povezane s privatnim sektorom u okviru nacionalnih gospodarstava, sve više zadiru u gospodarske sfere i strateške gospodarske interese svojih „saveznika i prijatelja“.

U tom kontekstu možemo promatrati i izjavu tadašnjeg čelnika CIA-e Williama Webstera koju je iznio u rujnu 1989. tijekom stručnog savjetovanja u Los Angelesu: „Gospodarska pitanja koja sam spomenuo – trgovinska neravnoteža i tehnološki razvitak, ilustriraju pitanje koje postaje sve jasnije: naši politički i vojni saveznici ujedno su i naši gospodarski suparnici.“[6] Pritom ne treba zaboraviti da je ova izjava dana još tijekom Hladnog rata dok je ideološki protivnik/suparnički blok još uvijek postojao. Tako je npr. nedvojbenu potvrdu o ciljevima ruskog obavještajnog

6 William Engdahl, Stoljeće rata: Anglo – američka naftna politika i novi svjetski poredak, AGM, Zagreb, 2000., str. 337

aparata dao bivši zamjenik KGB-a Vladimir Kirpečenko: „Težište djelovanja ruskih obavještajnih službi odnosi se na industrijsku i tehnološku špijunažu.“[7]

Nadalje, u dokumentu pod nazivom „Angažman i proširene obveze u strategiji nacionalne sigurnosti“ što ga je Bijela kuća donijela 1994., znakovita je izjava tadašnjeg američkog predsjednika Billa Clintona: „Suprotstavljajući se vanjskim opasnostima po američku demokraciju i gospodarstvo blagostanja, obavještajna zajednica mora utirati put političkom, gospodarskom i socijalnom i vojnom razvoju u onim dijelovima svijeta gdje američki interesi ne mogu biti zadovoljeni samo javnim prikupljanjem informacija iz otvorenih koji nisu dovoljno adekvatni. Gospodarska špijunaža imat će najvažniju ulogu u pružanju pomoći političkim donositeljima odluka u razumijevanju svjetskih gospodarskih trendova. Gospodarska špijunaža mora podržati američke pregovarače u različitim poslovnim pregovorima i pomoći gospodarstvu na svim razinama u identificiranju prijetnji američkim poslovnim kompanijama koje mogu uslijediti od inozemnih obavještajnih službi ili neetičkih poslovnih trikova“.[8]

Ove izjave potvrđuju važnost gospodarskih pitanja, odnosno fokusiranost obavještajnih struktura upravo na to područje za razliku od hladnoratovskog razdoblja kada su glavni interesi službi bile informacije vojne i političke naravi.

U uvjetima promijenjenih međunarodnih odnosa (političkih i gospodarskih) „problem predstavlja i nedovoljno precizno definirana nadležnost obavještajnih i sigurnosnih službi na području gospodarskih aktivnosti.“[9] Osim toga, kod jednog dijela privatnih poslovnih kompanija i korporacija prisutan je strah od uplitanja obavještajno – sigurnosnih struktura u njihove poslovne aktivnosti što prema mišljenju stručnjaka može dovesti do slabljenja kompanija na regionalnim i svjetskim tržištima.[10]

Svojevremeno je John Hayden, jedan od vodećih menadžera u američkom Boeingu, odbijajući bilo kakvu obavještajnu pomoć američkih službi u poslovanju kompanije izjavio: „Od američkih tajnih službi ne želimo dobivati nikakve tehnološke, tržišno – strateške ili gospodarske informacije o našim konkurentima. Mi sami možemo poduzeti djelotvorne korake kako stvorili prednost u

7 Intervju Vladimira Kirpečenka u The Europeanu, 23. – 29.11.1995.

8 E. Potter, Economic Intelligence & National Security, op. cit., str. 81

9 Francesco Cossiga, Gospodarske izvještajne službe, Zbornik – Nacionalna sigurnost i budućnost, Svezak 1, Udruga Sv. Jurja, Zagreb 2001., str. 13

10 Ibid.

tržišnoj utakmici."[11] Primjer Boeinga je indikativan jer pokazuje kako se pojedine kompanije pribojavaju gubitka vlastite neovisnosti o političkim centrima moći, a u slučaju otkrivanja potpore (involviranosti) obavještajnih struktura njihovim poslovima, postoji velika vjerojatnost da bi im zbog podozrenja i sumnjičavosti potencijalni poslovni partneri mogli okrenuti leđa. Poslovne kompanije izražavaju sve veću zabrinutost zbog bojazni da bi obavještajne službe mogle reducirati njihovu poslovnu sposobnost te im dokinuti samostalnost u donošenju poslovnih strateških odluka.

Međutim, primjeri različitih oblika uspješne suradnje gospodarskih subjekata i obavještajnih struktura daleko su brojniji. Mnoštvo poslovnih kompanija rabi usluge bivših pripadnika službi ili čak imaju svojevrsne poslovne aranžmane s nacionalnim obavještajnim službama. Najuočljivija tendencija kod gospodarski najrazvijenijih zemalja je da u stvaranju i očuvanju gospodarske strategije, uključujući i gospodarsku sigurnost, osim obavještajnih i sigurnosnih struktura, u velikoj mjeri sudjeluju i poslovne kompanije i korporacije. Zabilježeni su i različiti specifični slučajevi gdje obavještajne službe zbog svojih operativnih interesa te uslijed izražene potrebe za praćenjem suvremenih tehnologija žele rabiti rezultate najnovijih znanstvenih istraživanja. Tako je npr. krajem 1999. američka CIA osnovala vlastitu informatičku tvrtku In-Q-Tel sa sjedištem u Silicijskoj dolini u Kaliforniji.[12] Glavnu zadaću tvrtke predstavlja investiranje u nove visokotehnološke projekte koji bi CIA-i trebali pripomoći da ponovno ostvari superiornost nad privatnim kompanijama u novim i naprednim tehnologijama kakvu je imala tijekom hladnoratovskog razdoblja sedamdesetih i osamdesetih godina prošlog stoljeća.

Također, potrebno je spomenuti specifičnu pojavu kod brojnih kompanija iz razvijenih zemalja Zapada koje kopiraju ustroj obavještajnih službi te često puta funkcioniraju na sličan način. Kao posebno pozitivan primjer Herbert Mayer, stručnjak za pitanja business intelligencea, navodi američku elektronsku kompaniju Motorola koja je svojevremeno bila organizirana poput američkog Nacionalnog protuobavještajnog centra NACIC-a.[13] Općenito promatrano, velike svjetske kompanije da bi bile uspješne, provode

11 Unclassified, listopad/studeni 1993., iz A. Förster, Maulwürfe in Nadelstreifen, Henschel Verlag, Berlin, 1997., str. 95

12 K. Breslau, „Intelligence – Snooping around the Valley. CIA sets up a high-tech investment fund", Newsweek, 10.4.2000.

13 H. Mayer, Real World Intelligence, Storm King Press, Friday Harbor, Washington, 1987., 1991., str. 59

različite aktivnosti koje su po načinu vođenja i ciljevima gotovo podjednake načinu prikupljanja i analiziranja informacija od strane obavještajnih službi. Također, odjeli nekih kompanija vjerna su kopija organizacijske strukture obavještajnih službi, a njihove aktivnosti obuhvaćaju: istraživanja tržišta, gospodarska predviđanja, dubinsku analizu političkog rizika pojedinog tržišta (nacionalnog ili regionalnog), stupnjevanje tehnoloških aktivnosti konkurentskih kompanija i drugo.

Realizatori i nositelji suvremene gospodarske špijunaže

Kada je riječ o nositeljima obavještajnih aktivnosti potrebno je voditi računa o tome je li riječ o industrijskoj špijunaži ili je pak riječ o gospodarskoj špijunaži.

Nositelji obavještajnih aktivnosti, kada je riječ o industrijskoj špijunaži najčešće su tvrtke ili kompanije. Kada govorimo o gospodarskoj špijunaži nositelji su, u pravilu, ali ne i nužno, političke i/ili gospodarske elite pojedinih zemalja koje na ovaj način žele premostiti tehnološki jaz i osigurati gospodarski napredak svojih zemalja, odnosno konkurentnost nacionalnog gospodarstva u globalnoj tržišnoj utakmici ili pak ostvariti veći profit u poslovanju vlastite kompanije. U pravilu, nositelji gospodarske špijunaže su nacionalne obavještajne službe koje rade u skladu sa zadaćama dobivenim od svojih vlada. Međutim, stvari nisu uvijek jednoznačne. Postoje brojni slučajevi u suvremenom svijetu gdje je teško odrediti glavnog nositelja obavještajnih aktivnosti, ponekad je to poslovna kompanija, a ponekad je riječ o obavještajnoj službi. Naime, u globaliziranom svijetu postoje slučajevi gdje obavještajne službe djeluju u korist nacionalnih kompanija ili korporacija. Također postoje primjeri gdje su poslovne kompanije provodile klasične obavještajne aktivnosti u korist nacionalnih obavještajnih službi, tj. nacionalne političke i državne elite što je još jedan dokaz u prilog tezi o komplementarnosti obavještajnih i gospodarskih interesa.

Zanimljiva je činjenica da su Njemačka i SAD sastavile „crnu listu“ tvrtki iz jedne prijateljske i „savezničke“ zemlje koje usko surađuju, odnosno stoje na usluzi nacionalnim obavještajnim službama. Riječ je o Francuskoj, a spomenuta usluga sastoji se u pružanju logističke potpore. Često puta te iste tvrtke služe kao paravan za špijunske operacije koje provode domicilne službe. Međutim, tvrtkama se to obilato isplati, budući da zauzvrat dobivaju rezultate elektronskog

izviđanja što ga francuske službe provode protiv inozemnih kompanija koje su im ujedno i glavna konkurencija.

Kao svojevrsni kuriozitet te potvrda koliku važnost Francuska pridaje području gospodarska špijunaže je činjenica da je u listopadu 1997. u Parizu utemeljena institucija pod nazivom „Škola za gospodarski rat" (Ecole de Guerre Economique). Službeno stajalište je da je riječ o „borbi protiv nedopuštene konkurencije", te i jedan kolegij nosi taj naziv. Međutim, riječ je o teorijskoj i praktičnoj obuci obavještajnih aktivnosti u skladu s najnovijim obavještajnim tehnikama. Osnivač škole je francusko Ministarstvo obrane posredno preko jedne tvrtke u njezinom vlasništvu, a prema kategorizaciji Ministarstva obrazovanja škola se svrstava u kategoriju poslovnih škola. Moto ove škole glasi: „znati, predvidjeti, djelovati reagirati", prema maksimi generala Charlesa de Gaullea.

Kada se govori o realizatorima gospodarske špijunaže, tu značajnu ulogu, osim obavještajnih službi, imaju i različite tvrtke koje bave business intelligenceom (BI) te pitanjima poslovne sigurnosti. Trend osnivanja BI tvrtki[14] je u SAD-u započeo još sredinom osamdesetih godina, dok je Europi on započeo nešto kasnije, tijekom devedesetih godina prošlog stoljeća. BI tvrtke u SAD-u su tijekom 1994. ostvarile prihod od 3,3 milijarde USD-a, da bi 2001. taj prihod narastao na 4,6 milijardi USD-a.

Iako je poslovanje takvih tvrtki legalno, učestali su primjeri u svijetu gdje one zalaze u „sivu" pa čak i „crnu" zonu nadopuštenog prikupljanja informacija ili transfera zabranjene tehnologije. Vodeći menadžeri BI tvrtki u svijetu vole naglašavati kako se njihove kompanije ne bave gospodarskom špijunažom, koja je protuzakonita, već informacije crpe iz otvorenih izvora. Međutim, brojni poslovni ljudi iz poslovnih krugova sumnjaju u njihove tvrdnje jer smatraju da, budući da su u tim tvrtkama zaposleni brojni bivši obavještajci, zadržane stare veze s kolegama iz obavještajno – sigurnosnih struktuta te da ipak jedan dio informacija prikupljaju na nezakonit način. Osim toga, zabilježeni su brojni slučajevi vrbovanja obavještajaca od strane svojih dojučerašnjih kolega u business intelligence tvrtkama.

Znakovit je slučaj najveće kineske telekomunikacijske kompanije Huawei15 koja se bavi proizvodnjom elektroničke opreme. Naime, ona se našla pod istragom u Kanadi i

14 U SAD-u se često za ove tvrtke rabi naziv front companies.

15 Huawei ima 140 000 zaposlenih, drugi je najveći proizvođač telekomunikacijske opreme na svijetu te je jedan od najvećih investitora u zapadnoj Europi.

Australiji zbog sumnje da se bavi određenim oblicima špijunaže. Dapače, američki Kongres ih je nedavno proglasio sigurnosnom prijetnjom.16 U ožujku ove godine Odbor za obavještajne službe Kongresa je upozorio američke kompanije da izbjegavaju poslovanje s Huaweijem zbog mogućnosti da njihova oprema može poslužiti za cyber napad iz Kine. Zbog istovjetne prijetnje, australska vlada je kineskoj kompanija zabranila da sudjeuje u izgradnji brze internetske mreže. Jedan od razloga za takvu zabrinutost je činjenica da je utemeljitelj Huaweija Ben Zhengfei bivši inžinjer kineske vojske. Iako, Kinezi tvrde da je riječ o pokušajima suzbijanja konkurencije i miješanja u tržišno natjecanje, kod dijela vladajućih političkih elita na Zapadu, postoji bojazan da je kompanija zapravo produžena poluga kineske vlade u pokušaju prikupljanja povjerljivih informacija gospodarske naravi.

Ciljana područja gospodarske špijunaže

Gospodarska špijunaža danas se u svijetu usmjerava ka prikupljanju osjetljivih informacija s područja: financija, businessa, znanosti i tehnike. Osnovni cilj ogleda se u stvaranju određenih prednosti za vladu vlastite zemlje i nacionalno gospodarstvo, odnosno pojedine gospodarske grane. Podaci do kojih se nastoji doći usko su povezani s najsuvremnijim znanstvenim i tehničkim dostignućima i sofisticiranim tehnologijama. Stoga je sasvim razumljivo da su udaru gospodarske špijunaže najizloženije najrazvijenije zemlje Zapada. Inozemnoj gospodarskoj špijunaži, osim tehnološke razvijenosti, dodatnu pogodnost za djelovanje daje činjenica da je riječ o zemljama s visokim stupnjem otvorenosti njihovih društava te u velikoj mjeri slobodnom kolanju ljudi, dobara i kapitala.

Ciljana područja gospodarske špijunaže nisu ista kod svih zemelja. Dok zapadnoeuropske i američke kompanije i obavještajne službe nastoje prikupiti podatke o posljednjim generacijama tehnologija svojih konkurenata, zemlje u razvoju (među najaktivnijima su Rusija, Kina i Indija) nastoje se domoći softwarea i hardwarea nešto starije generacije koji im još uvijek pomaže u jačanju vlastitih tehnoloških baza za daljnji razvoj industrijskih potencijala. Do takve tehnologije se zbog njezine relativne zastarjelosti lakše može doći na „crnom tržištu“ i to iz dva razloga. Prvi je niža i povoljnija cijena. Osim toga za tehnologiju starije generacije

16 Jutarnji list od 11.10.2012.

primjenjuju se niži standardi sigurnosne zaštite. Posebno interesantno područje za gospodarsku špijunažu predstavljaju dual – use tehnologije: zrakoplovna industrija, kemijska industrija, biomedicina, razvoj i usavršavanje kinetičkih energija, radarski i navigacijski sustavi, senzorska i laserska tehnologija, svemirski programi i tehnologije istraživanja svemira, elektronički i informatički sustavi, sustavi vezani uz pomorsku tehnologiju, nuklearni sustavi i proizvodnja poluvodiča i specijalnih materijala. Osim toga na udaru gospodarske špijunaže nalaze se i energetske tehnologije i tehnologija zaštite okoliša, biotehnologija i primijenjena molekularna biologija, farmacija itd.

Metode i sredstva gospodarske špijunaže

Sredstva i metode gospodarske špijunaže nikad nisu jednoznačna i unificirana. Najčešće ovise o mogućnostima onih koji je provode ali i ciljevima. Iako na prvi pogled djeluje iznenađujuće, jedno od od najbitnijih državnih tijela u SAD koje se bavi analizama djelovanja inozemne obavještajne djelatnosti, uključujući i onu gospodarsku NCIX (National Counterintelligence Executive) u jednom od svojih izvješća koje je upućeno Kongresu navodi kako je jedna od čestih i najjednostavnijih metoda, postavljanje upita od strane inozemnih „poslvnih“ ljudi koji se (fax-om ili e-mailom itd.) zanimaju kod američkih kompanija koji se bave sofisticiranim tehnologijama za pojedine projekte ili neke druge osjetljive podatke do kojih ne mogu doći posredstvom otvorenih izvora.[17] Nedovoljno sigurnosno – educirani službenici u svojim odgovorima šalju podatke od gospodarskog značaja za svoju tvrtku te ustvari otkrivaju poslovne tajne tvrtke.

Dosadašnje iskustvo zapadnoeuropskih zemalja te SAD-a u suprotstavljanju gospodarskoj špijunaži ukazuje kako se ista najčešće provodi na nekoliko osnovnih načina:

- Krađom informatičkih baza podataka (ili nekih njezinih dijelova) uz pomoć unajmljenih hackera;
- Slanjem službenika, poslovnih ljudi ili studenata na specijalizaciju, odnosno školovanje;
- Formiranjem joint-venture tvrtki gdje većinski udio pripada inozemnim vlasnicima;
- Vrbovanjem znanstvenika i stručnjaka koji se bave sofisticiranim tehnologijama ili rade na nekim osjetljivim znanstvenim projektima;
- Sitnim krađama po laboratorijima i institutima;

17 Godišnje izvješće NCIX-a za 2003. godinu

- Klasičnim obavještajnim metodama uključujući i metode elektronskog izviđanja različitih oblika komunikacija;
- Širenjem glasina i dezinformacija s najčešćim temama o:
  - navodnoj „nekvaliteti i nepouzdanosti“ proizvoda čijom proizvodnjom se bavi suparnička tvrtka i
  - izmišljanjem korupcionaških afera u ciljanoj tvrtki ne bi li se srušio njezin ugled i status na tržištu.

Bitno je napomenuti kako se u većini slučajeva gospodarska špijunaža provodi u kombinaciji s legalnim metodama (business intelligence i slično). To se čini zbog više razloga. Mnogo teže ju je detektirati nego što je to slučaj s klasičnim oblicima obavještajne djelatnosti, a čak i u slučajevima kada se otkrije daleko teže ju je, upravo zbog gore nevedenih razloga, pravno sankcionirati budući da se često puta jednim dijelom zadržava u zakonskim okvirima.

Zaključak

Gospodarska špijunaža ne poznaje saveznike. To je rat svih protiv svih u koji su uključene od onih slabije i srednjerazvijenih pa sve do najrazvijenijih zemalja svijeta. Razvijenim zemljama EU posebno teško padaju različiti oblici gospodarsko – obavještajnih aktivnosti koje protiv njih provode njihovi „prijatelji i saveznici“ na što one još uvijek ne pronalaze adekvatan odgovor i kvalitetne načine suprotstavljanja. Ovakve aktivnosti izazivaju štete koje se mjere u milijardskim iznosima zbog čega dolazi do ozbiljnog ugrožavanja gospodarske odnosno nacionalne sigurnosti dotičnih zemalja. Temelji sigurnosti postaju: gospodarski prosperitet koji uključuje zaštitu vlastitih gospodarskih interesa i resursa te primjenu modernih tehnologija uz odgovarajuću valorizaciju znanstvenih potencijala.

Nadalje, gospodarska špijunaža iza koje stoje obavještajne strukture pojedinih zemalja znači određen oblik intervencije političkih elita u principe slobodnog tržišta i može značiti preferiranje točno određenih kompanija, odnosno određenog oblika privatnog kapitala. Osim što ulaze u gospodarska nadmetanja, obavještajne službe svoje aktivnosti u gospodarskoj sferi provode i zbog trgovanja informacijama. Naime, povjerljivi podaci gospodarske prirode koje uspijevaju prikupiti obavještajne strukture, u slučajevima kada ne predstavljaju nacionalni interes, odnosno nisu predmet interesa državnih institucija, rabe se za razmjenu s privatnim kompanijama i korporacijama,

Uz sve brži razvoj znanosti i rastući nesrazmjer gospodarskog stupnja razvoja različitih zemalja u svijetu sve više će se i širiti gospodarska špijunaža. Osim slabije razvijenih zemalja koje će ju rabiti za smanjivanje tehnološke ovisnosti te će im biti najlakši put za ovladavanjem suvremenih tehnologija, njome će se podjednako koristiti i razvijene zapadne zemlje radi očuvanja i jačanja svoje uloge na globaliziranom svjetskom tržištu.

Literatura:

Adams, J. *The New Spies*, Hutchinson, London, 1994.;

Potter, E. *Economic Intelligence & National Security*, Carlton University Press & The Center for Trade Policy and Law, Canada, 1998.;

Endgal, W. *Stoljeće rata: Anglo – američka naftna politika i novi svjetski poredak*, AGM, Zagreb, 2000.;

Förster, A. *Maulwürfe in Nadelstreifen*, Henschel Verlag, Berlin, 1997.;

Mayer, H. *Real World Intelligence*, Storm King Press, Friday Harbor, Washington, 1987., 1991.;

Cossiga, F. *Službe za gospodarsku špijunažu*, Nacionalna sigurnost i budućnost, Zbornik, svezak 1, Udruga Sv. Jurja, Zagreb, 2001.;

Godišnje izvješće američkog NCIX-a za 2003. godinu;

Newsweek od 10.04.2000.;

The European, 23. – 29.11.1995.;

Jutarnji list od 11.10. 2012..

www.nsi.org/Library/Intel/japanesp.html