УДК: 343.534(510)(73)
DOI: https://doi.org/10.22182/pnb.1922020.10
Прегледни рад

Политика националне безбедности
Година XI, vol. 19
број 2/2020.
стр. 219-240

Синиша Домазет*

Факултет за студије безбедности, Универзитет Едуконс

Здравко Скакавац

Факултет за правне и пословне студије
др Лазар Вркатић, Нови Сад

ИНДУСТРИЈСКА ШПИЈУНАЖА НА ПРИМЕРУ КИНЕ И САД

Сажетак

У раду је анализиран појам и основне карактеристике индустријске шпијунаже на примеру САД и Народне Републике Кине. Циљ рада је да се укаже на опасност од овог облика нелегалних активности и на велике економске штете које се проузрокују. Пример представља афера у вези са компанијом *Huawei*. Поменута компанија је постала „камен спотицања" између две суперсиле, с обзиром на бројне оптужбе које стижу са америчке стране да се *Huawei*, поред основне делатности, бави и индустријском шпијунажом у корист кинеске владе. Установљено је да се кинеска индустријска шпијунажа односила и на наводне крађе технологије за ловац најновије генерације Ф-35, корпорацијских тајни више компанија као што су Моторола, Форд, Џенерал моторс, Дипон, укључујући и познате америчке компаније у области пољопривреде, затим у области сателитског програма, као и крађе интелектуалне својине уз помоћ такозваних „спавача", односно кинеских студената у САД. Утврђено је да индустријска шпијунажа обухвата практично све делове привреде, као и да наноси енормне економске штете. Уз помоћ агресивне индустријске

* Контакт: sdomazetns@gmail.com

шпијунаже стиче се конкурентска предност на тржишту, прибављају осетљиве пословне информације, али и нарушавају политички односи. Стога је неопходно повећати контраобавештајну заштиту, али и развијати ефикасне системе одбране од сајбер напада и откривања пословних тајни. У истраживању су коришћени нормативни метод и правно-логички методи индукције и дедукције.

Кључне речи: *право, политика, безбедност, Кина, САД, индустријска шпијунажа, Huawei*

ПОЈАМ (ИНДУСТРИЈСКЕ) ШПИЈУНАЖЕ

Шпијунажа представља прибављање и одавање података који представљају неку тајну (Бошковић 2017). Неки аутори шпијунажу дефинишу као тајно, потајно, прикривено и на преваран начин прикупљање економских, политичких, војних и техничких података, које држава и покрети означавају као тајне (Тепавац 2019, 164), а поједини аутори шпијунажу одређују као прикупљање поверљивих информација без неопходне дозволе њиховог власника (Androulidakis and Fragkiskos-Kioupakis 2016).

У ужем значењу, шпијунажа представља деликт угрожавања националне безбедности, одавања политичке, војне, економске или службене тајне страној држави, организацији или лицу које им служи. Кривично дело шпијунаже има један основни, три посебна и један квалификован (тежи) облик. Основни облик шпијунаже састоји се у саопштавању, предаји или чињењу доступним тајних података или докумената војног, економског или службеног карактера страној држави, страној организацији или лицу које им служи. Радња овог дела састоји се у саопштавању, предаји или чињењу доступним наведених података поменутим субјектима. Посебни облици шпијунаже су стварање обавештајне службе или руковођење том службом за потребе стране државе. Квалификовани облик шпијунаже јавља се у случају када су из основног дела настале тешке последице за безбедност, економску или војну моћ. Учинилац кривичног дела шпијунаже може да буде свако лице, али с

обзиром на природу тајних података и докумената који су објект кривичног дела, најчешће су то лица која службено располажу таквим подацима и документима (Бошковић 2017).

Постоје различити облици шпијунаже, при чему се истичу политичка, војна, економска (привредна, пословна, индустријска шпијунажа).[1] Индустријска шпијунажа је типична карактеристика савремене шпијунаже, јер је индустрија производ и карактеристика савременог друштва. Уско је упућена на ону делатност чија је позадина чисто комерцијалне природе. Индустријска шпијунажа се може посматрати као скупни појам који обухвата конгломерат деликата којем припадају крађа, утаја, превара, нелојална конкуренција, подмићивање, фалсификовање докумената и слично. Индустријска шпијунажа, као најужи појам, подразумева такву врсту делатности која се односи на технички и технолошки развој и уже професионалне интересе одређених пословних субјеката. Дакле, индустријска шпијунажа представља само једно подручје и део економске шпијунаже, јер је она по својим задацима усмерена само на одређену специфичну стручну делатност у области економије (Тепавац 2019, 167; Petković 2009).

Економска шпијунажа добија посебан значај након завршетка Другог светског рата и поделе света на два блока, на земље које су приступиле НАТО савезу и земље потписнице Варшавског уговора. Између два супротстављена блока наступа време хладног рата у којем обавештајне и контраобавештајне службе имају водећу улогу у заузимању примата у светској политици. Економска шпијунажа у то време није представљала посебан сегмент већ је била део војно–политичке шпијунаже, с тим да су се прикупљени подаци користили у циљу побољшања привредних капацитета сопствене националне државе. Распадом Варшавског блока и окончањем биполарне поделе света, економска шпијунажа заузима централно место у стратегијама савремених држава. Значај економског развоја заузима важно место и у развоју осталих области као што је одбрана, индустрија, квалитет и степен међународне сарадње. Америчка служба ФБИ прави

1 С обзиром да се у развијеним земљама чешће користи израз индустријска шпијунажа, определићемо се за овај назив.

разлику између економске и индустријске шпијунаже, на тај начин што првом управља држава, а спроводе је обавештајне институције које, применом легалних и нелегалних метода, прикупљају тајне податке од значаја за конкурентску државу и користе их за јачање сопственог државног и приватног сектора, док индустријском шпијунажом управљају приватни пословни субјекти у циљу постизања пословне предности у односу на конкуренцију (Тепавац 2019, 168).

Дакле, индустријска шпијунажа представља корпорацијски облик шпијунаже одређен предметом-облашћу деликта. То је, заправо, тајно прикупљање података који су пословна, то јест, индустријска или технолошка тајна. Практикује се у организацији мултинационалних компанија или обавештајних служби земаља које нису потписнице међународних конвенција о патентима и лиценцама. Тако се прибављају подаци о проналасцима и иновацијама савремених техничких уређаја и направа, технолошких процеса и рецептура нових производа, такозваних брендова (Бошковић 2017).

Не треба да чуди што су све иоле снажније обавештајне службе прибављале научно-техничке информације велике вредности, с обзиром на велике економске добитке.[2] Ниједна влада, а тиме ниједна држава, не може себи допустити ту лагодност да се економске и друге активности одвијају мимо ње. Теоретичари безбедности су давно утврдили да су економске полуге којима располаже власт јаче и значајније од полуга силе (војске и полиције). Тиме долазимо до тезе да је напад или урушавање економске безбедности и економског система некада опасније и перфидније од напада на друге системе државе. Осим тога, држава на себе преузима мноштво задатака у сфери економије, како би успоставила неопходну хармонију у свим сферама друштвене делатности. Држава,

2 Тако, поједини припадници обавештајне службе тврде да је (некадашњи) КГБ коаутор огромног броја совјетских научних открића и изума. С тим у вези, некадашњи припадници службе безбедности тадашњег СССР-а наводе: „Ми смо добијали задатке из научних центара и усмеравали своје агенте н задобијање те или неке друге научно-техничке информације. И тако један агент донесе један податак из неке земље, други-из друге, трећи из треће и тако даље. А онда гледаш-и научно откриће и технички пробој совјетских научника! Ето тако су код нас настале напредне технологије. Довучене су мало по мало из читавог света. И иначе, у том правцу раде све обавештајне службе света. Због тога што стотине милиона морају да се уложе у неке пројекте, а они могу скоро бесплатно да се украду готови. У име државних интереса“ (Север 2017, 109).

за то захтева од јавног и приватног сектора, од појединаца и колективитета, да поштују законе и друге норме и да остварују своју улогу према држави у складу са правима и дужностима, управо ради заштите националне безбедности, иако то на први поглед није одмах видљиво (Стајић и Милошевић 2017, 176).

Штете од индустријске шпијунаже су велике и крећу се у милијардама америчких долара годишње. Треба истаћи да све велике силе шпијунирају једне друге и воле да се докопају осетљивих података (економског карактера) конкурентских земаља. Пракса показује да индустријска шпијунажа у највећој могућој мери „поткопава" политичке односе између државе која је украла неку индустријску тајну и државе која је била жртва таквих активности. Историја је пуна примера индустријске шпијунаже, при чему ће на овом месту бити обрађени примери индустријске шпијунаже у односима између САД и Кине.

Русија и Кина прилагодиле су се техникама ратовања информационог доба, усвојиле асиметричне стратегије, модернизовале своје војске и научиле лекције о значају „меке моћи", те је јаз у погледу моћи између њих и САД ужи него раније. Објективна процена стања упућује на закључак да је амерички поредак достигао своје максималне границе и да се не може више ширити без угрожавања унутрашње стабилности. Уместо либералног „бизниса промоције демократије", најреалнија опција коју и један број америчких аутора саветује јесте „укопавање" ("*re-entrenchment*") тј. консолидација добијеног која ће значити да Вашингтон треба да се спреми на дуг период компетитивне коегзистенције са либералним великим силама (Jennifer Lind, William Wohlforth 2019, 71 цитирано у: Цветићанин и Благојевић 2019, 54).

МЕЂУНАРОДНО-ПРАВНО РЕГУЛИСАЊЕ ШПИЈУНАЖЕ

Кад је реч о индустријској шпијунажи, треба истаћи да државе углавном прибегавају примени домаћих прописа, посебно из домена кривичног права, како би заштитиле националну безбедност. Међутим, проблем настаје због ограничене територијалне важности националне легислативе на

лица која су напустила њену територију и вратила се у матичне државе. То посебно долази до изражаја код индустријске (сајбер) шпијунаже, јер извршилац кривичног дела шпијунаже не борави физички на територији погођене државе. Треба истаћи да на међународном плану не постоји велики број релевантних аката који би се односили на индустријску шпијунажу, због тога што државе сматрају да су одредбе међународног привредног права, махом, неприменљиве на индустријску шпијунажу.

Ипак, могла би се, макар посредно, пронаћи одређена интеракција између индустријске шпијунаже и правила међународног привредног права. С тим у вези, од значаја је Париска конвенција о заштити индустријске својине (УПКЗИС 1986), али и важећа правила у оквиру Светске трговинске организације. Према члану 10. bis ове Конвенције, земље Уније за заштиту индустријске својине обавезују се да осигурају припадницима Уније једну стварну заштиту против нелојалне конкуренције. Акт нелојалне конкуренције представља сваки акт конкуренције, који је противан поштеним обичајима у индустрији или трговини. У складу са Конвенцијом, треба забранити нарочито:

> 1) било каква дела која по својој природи могу створити забуну, ма којим средством, са предузећем, производима или индустријском односно трговинском делатношћу једног конкурента;
>
> 2) лажне примедбе, при вођењу трговине, такве природе да дискредитују предузеће, производе или индустријску односно трговинску делатност једног конкурента;
>
> 3) ознаке или наводе чија употреба у трговини може довести јавност у заблуду о пореклу, начину производње, особинама, погодностима за употребу или количини робе.

С обзиром на наведену одредбу, може се констатовати да индустријска шпијунажа представља *акт (нелојалне) конкуренције*, с обзиром да се тако нарушава конкурентска способност компаније која је жртва тих активности, односно непоштовања поштених обичаја у индустрији или трговини.

Друго, индустријска шпијунажа често подразумева да се од погођене компаније прибављају поверљиве пословне информације у вези са запосленим лицима, купцима или добављачима, набавним ценама и слично. Због тога се индустријска шпијунажа може такође окарактерисати као акт нелојалне (нефер) конкуренције. Треће, државе чланице Светске трговинске организације, у случају да су њихове компаније погођене активностима индустријске шпијунаже од стране других држава, могу интересе својих компанија да заштите пред телом за решавање спорова, Панелом. Панел ће препоручити држави нападачу да прекине са спровођењем недозвољених активности (индустријске шпијунаже). У случају да се и даље настави са тим активностима, Тело за решавање спорова при Светској трговинској организацији ће дозволити погођеној држави да суспендује примену обавеза или уступака у складу са закљученим споразумима. У складу са чланом 22.4 Споразума о решавању спорова, санкција за кршење споразума ће бити еквивалентна нивоу поништења или оштећења претрпљеног од стране погођене државе (услед индустријске шпијунаже) и мора утицати на државу прекршиоца да се убудуће придржава одговарајућих прописа. Дакле, на основу реченог, може се закључити да правила међународног трговинског права и правила Светске трговинске организације екстензивним тумачењем могу да се примене и на акте индустријске шпијунаже.

Други значајан међународно-правни акт представља Бечка конвенција о дипломатским односима, која је ступила на снагу 1964. године (БКДО 1964). У складу са поменутом Конвенцијом, једна од функција дипломатске мисије је да обавештавају, свим дозвољеним средствима, о условима и развоју догађаја у држави код које се акредитује и подношењу извештаја о томе влади државе која акредитује (БКДО 1964, чл. 3). Даље, сва лица која уживају привилегије и имунитете према овој Конвенцији дужна су да поштују законе и прописе државе код које се акредитује. Она су такође дужна да се не мешају у унутрашње ствари те државе. Истовремено, сви службени послови са државом код које се акредитује, а које држава која акредитује поверава мисији, морају се водити са министарством иностраних послова државе код

које се акредитује или његовим посредством, или са неким министарством о коме буде договорено. Просторије мисије не смеју се употребљавати за циљеве који нису у складу са функцијама мисије онако како су одређене овом конвенцијом или другим правилима општег међународног права или посебним споразумима на снази између државе која акредитује и државе код које се акредитује (БКДО 1964, чл. 41). Дакле, дипломата мора да познаје позитивно-правне прописе државе домаћина, нарочито оних који се односе на шпијунажу.[3] У супротном, постоји ризик избијања озбиљног међународног инцидента који се, неретко, завршава проглашењем одговорног лица за *persona non grata*, односно његовим протеривањем из земље домаћина.

Такође, овом Конвенцијом се гарантује да је личност дипломатског агента неприкосновена. Он не може бити подвргнут никаквој врсти хапшења или притвора. Држава код које се акредитује третира га с дужним поштовањем и предузима све разумне мере да би спречила наношење увреда његовој личности, његовој слободи или његовом достојанству (БКДО 1964, чл. 29). Важна је и одредба Конвенције по којој дипломатски агент ужива имунитет од кривичног судства државе код које се акредитује (БКДО 1964, чл. 31). Бечка конвенција о дипломатским односима предвиђа и неповредивост просторија мисија, а органима државе је дозвољено да у њих уђу само уз пристанак шефа мисије. Држава код које се акредитује има специјалну обавезу да предузме све потребне мере да би спречила насилан улазак у просторије мисије или њихово оштећење, нарушавање мира мисије или повреду њеног достојанства. Просторије мисије, намештај и други предмети који се у њима налазе, као ни превозна средства мисије не могу бити предмет никаквог претреса, реквизиције, заплене или мере извршења. Под резервом закона и прописа који се односе на зоне у које је улаз забрањен или посебно регулисан из разлога националне безбедности, држава код које се акредитује обезбеђује свим члановима мисије слободу путовања и кретања на својој територији (БКДО 1964, чл. 22,24,26).

3 У нашој земљи кривично дело шпијунажа је уређено чланом 315. Кривичног законика Републике Србије (КЗРС 2019).

НЕКИ СЛУЧАЈЕВИ КОЈИ СЕ ПОВЕЗУЈУ СА ИНДУСТРИЈСКОМ ШПИЈУНАЖОМ

У пракси је било доста примера индустријске шпијунаже међу великим силама, а случај који је нарочито интересантан за односе између САД и Кине, прерастављи у праву међународну аферу, односи се на компанију *Huawei*. Поменута компанија је постала предмет спора између две суперсиле у последње време, с обзиром на бројне оптужбе које стижу са америчке стране да се *Huawei*, поред основне делатности, бави и индустријском шпијунажом у корист кинеске владе. Афера око компаније *Huawei* попримила је и политичке димензије, нарочито у светлу актуелног трговинског рата између две државе, који се све више заоштрава и прети да остави озбиљне последице по целокупну светску економију.

Иначе, кинеска компанија *Huawei Technologies Co*, једна од највећих у свету, све више „жуља" америчку владу и то баш у тренутку када та кинеска компанија заузима водећу улогу у новој бежичној технологији познатој као 5G, пише „Блумберг". *Huawei* се тако недавно суочио са разним вишеструким искушењима, попут хапшења свог главног финансијског директора у Канади, кривичне пријаве у САД, могућег прекида сарадње са свим америчким компанијама и онемогућавања увођења своје нове инфраструктуре широм света. Американци оптужују компанију из Кине да своју опрему користи за шпијунирање америчких интереса, као и да крши америчке санкције Ираку. Сједињене Америчке Државе су још током 2018. године практично забраниле продају *Huawei* телефона кроз понуду оператора, па чак и кроз канале слободне продаје. Досадашња истраживања нису довела у везу компанију *Huawei* са могућностима шпијунирања, као ни са кршењем досадашњих протокола безбедности ни у једној земљи, док су нова испитивања у току. Сједињене Америчке Државе су чак тужиле *Huawei* за шпијунажу. Амерички званичници већ неко време претпостављају, оправдано или не, да компанија *Huawei* ради за интересе кинеске владе. У извештају америчких обавештајних служби из 2014. године, компаније *Huawei* и *ZTE Corp*, означене су као потенцијалне „претње по безбедност". У том извештају се наводи да је *Hua-*

wei одбио да пружи информације о „војној позадини" оснивача *Huawei* -ја Рена Женгфеија (*Ren Zhengfei*), бившег инжењера Народноослободилачке војске. Под изговором „претњи по безбедност", америчка влада страхује да би напретком развоја технологије произвођачи из других земаља могли да, помоћу својих компоненти, омогуће њиховим обавештајним агенцијама приступ поверљивим информацијама, пише „Блумберг". Током 2011. и 2012. године компанија Водафон (*Vodafone*) је на *Huawei* рутерима и другој опреми, уочио тзв. *backdoors* у софтверу, која су кинеској компанији могли да омогуће недозвољени приступ Водафоновој фиксној интернет мрежи у Италији, чиме су се могле прикупљати разне информације. Није утврђено да ли је та грешка била намерна или случајна, али су наводи италијанске компаније прилично наштетили *Huawei* репутацији. Поготово што је Водафон тражио да се исправи грешка, а *Huawei* је тврдио да је све исправљено. Да би се потом утврдило да проблем и даље постоји. Тек накнадно је решен. Амерички државни секретар Мајкл Помпео (*Michael Pompeo*) изјавио је да би САД могле да стопирају размену обавештајних података са савезницима НАТО-а ако оне наставе да користе *Huawei* опрему. Компанија *Huawei* у више наврата је негирала да помаже Пекингу при шпијунажи других земаља и истакла да нико до сада није пружио никакав уверљив доказ који би ишли у прилог таквим оптужбама. И поменути Рен Женгфеи је у јануару рекао да је поносан на своју каријеру и чланство у Комунистичкој партији Кине, али је одбацио тврдње да је компанија *Huawei* давала властима у Пекингу информације о клијентима (Čavić 2019).

Поједине америчке компаније су до сада већ оптуживале *Huawei* за крађу интелектуалне својине. Моторола (*Motorola*) је, рецимо, 2010. године, поднела тужбу против кинеске компаније у којој је изнела тврдњу да се „уротила са бившим запосленима како би дошла до пословних тајни Мотороле". Пре две године, амерички суд је утврдио како је *Huawei* одговоран за крађу роботске технологије компаније *T-Mobile US Inc*, а крајем јануара је Министарство правосуђа САД подигло оптужницу против кинеске компаније *Huawei* због крађе пословних тајни, а то је повезано са случајем из 2017. године. Догодио се и случај хапшења радника *Huawei* у Пољској, који је осумњичен

да је шпијунирао за кинеску владу. Тај радник је отпуштен, а *Huawei* је одбацио оптужбе. „Кинеска економска шпијунажа" је појам који се све чешће користи у САД, а наведени примери, као и оптужбе на рачун кинеске државне фирме „*Fujian Jinhua Integrated Circuit Co*", њеног тајванског сарадника и још три особе за крађу пословних тајни компаније „*Micron Technology Inc*", показују да САД немају намеру да дозволе Кинезима да превладају у овој области (Čavić 2019).

Huawei је оптужен и за индустријску шпијунажу, због чега ФБИ, ЦИА и друге државне агенције позивају да се *Huawei* опрема и телефони не користе. Наводно, *Huawei* инжењери су украли делове робота „*Tappy*" и његове функције, приликом посете Т-Мобиле центру (*T-Mobile Center*), због чега је у оптужбу умешан и директор тог националног оператора у САД. Према овим оптужбама *Huawei* је на овај начин успео да унапреди и направи свог робота, који се, као и „*Tappy*", користи за симулацију смартфон употребе (Mondo Portal 2019s).

Huawei је потом у марту 2019. године кренуо у противнапад, па је америчком Савезном суду поднео тужбу против статута којим се спречава агенцијама САД да користе његову опрему.

Председник САД, Доналд Трамп, потписао је директиву (President of the United States 2020) којом се америчким фирмама забрањује коришћење телекомуникационе опреме из извора који се сматрају претњом по националну сигурност. Иако у почетку није било прецизирано који се то извори сматрају за несигурне, свима је било јасно да одлука обухвата и кинеског гиганта *Huawei*. Убрзо је дошла и формална потврда од стране америчког министра трговине, који је додао *Huawei* на списак забрањених компанија. Ово представља врло конкретан потез Вашингтона који долази после дугог периода у којима је *Huawei* оптуживан за шпијунажу. Кинеска компанија је оптуживана и да је уско повезана с владајућом Комунистичком партијом Кине. Званичници ову директиву представљају као доказ да је Трамп предан томе да очува националне мреже од страних противника. Обавештајне службе упозоравају да би кинеска компанија могла да контролише мреже и сумњају да би могла да пресреће и преусмерава сигурне поруке у

Кину. Најгори сценарио, по њима, јесте да би кинеске власти могле да нареде *Huawei*-ју да блокира мреже у случају неког сукоба и да тако онемогући функционисање читаве америчке инфраструктуре, укључујући гасоводе и телекомуникацију. Ова одлука долази усред ескалације економског рата између Кине и САД. Сједињене Државе су више него дупло повећале таксе на неке кинеске производе, а друга страна је најавила да ће узвратити истом мером. Осим очигледних проблема које ово може да створи за *Huawei* на америчком тржишту, постоји и питање компоненти које купују од Интел-а и *Qualcomm*-а, а које користе за производњу паметних телефона (*smartphone*) и лаптопова. По новим правилима, америчке компаније морају да добију специјалну дозволу да би продавале технологију *Huawei*-ју. Штавише, ова директива се односи и на већ купљену телекомуникациону опрему из несигурних извора. Ипак, званичници се не изјашњавају поводом тога да ли ће влада финансијски помоћи у уклањању старе опреме, нити какве казне ће бити за оне који прекрше нову политику (Marković 2019).

Предвођени америчким државним секретаром Мајком Помпеом, амерички званичници су месецима упозоравали своје савезнике да ће престати да деле обавештајне податке ако они наставе да користе *Huawei* и друге кинеске технологије за развијање 5G мрежа. Осим САД, за сада су и Аустралија и Нови Зеланд увели сличне забране које се односе на *Huawei*. Дебате су започете у многим другим државама. Вероватно је највећи тас на ваги чињеница да *Huawei* представља лидера у развоју 5G технологије. Пошто се ова технологија сматра за срж економије у будућности, не чуди изражена подела у европским земљама. Недавно је бивша британска премијерка Тереза Меј отпустила министра одбране Гевина Вилијамсона (*Gavin Williamson*). Он је оптужен да је процурео вест како се Велика Британија спрема да *Huawei*-ју дозволи приступ неким деловима националне 5G мреже. Док се они најближи Терези Меј залажу за ограничено учествовање *Huawei*-ја у британским мрежама, али не и пуну забрану, други су ближи одлуци Трампове администрације. Представник кинеског Министарства трговине, Гао Фенг (*Gao Feng*), изјавио је како ограничавање пословања компаније *Huawei* у САД-у неће ту

државу учинити сигурнијом или јачом. Фенг их упозорава да ће се САД само ограничити на инфериорне, али и скупље, алтернативе, које ће их оставити у заостатку приликом ширења 5G мреже. Упркос бројним критикама и скепси, *Huawei* веома успешно послује. Њихови представници износе како су потписали већ 40 уговора за изградњу 5G мреже, с тим да је више од пола у Европи. Испоручили су чак 70.000 базних станица, кључних компоненти за изградњу мрежа, у местима која се не налазе у Кини (Marković 2019).

Huawei, који прави паметне телефоне, као и опрему за умрежавање повезивање, укључујући и надолазеће супербрзе 5G мреже, већ дуже време је под забраном пословања у Сједињеним Државама, делом због сумњи да би могао изградити „стражња врата" за своју опрему за шпијунирање или злоупотребе мреже, написао је Вашингтон пост. У једном случају описаном у оптужници, коју је објавило америчко Министарство правде, *Huawei* је упутио своје запослене у Сједињеним Државама да украду дизајн робота за тестирање мобилних телефона који је развио амерички *T-Mobile*. Тако је, 29. маја 2013. године, инжењер *Huawei*-а, који је био у посети *T- Mobile*-у, у своју торбу увукао роботску руку и изашао из лабораторије. Преко ноћи је фотографисао уређај и извршио критична мерења пре него што га је сутрадан вратио, извињавајући се да је то урадио „грешком", преноси Вашингтон Пост и истиче како је *Huawei* имао и бонус програм за раднике који су крали информације од конкурената Водеће кинеске компаније често су блиско повезане с државом и од њих се тражи да буду подређене држави, написао је Вашингтон Пост додајући како, према оптужници, *Huawei*-ев приступ подсећа на кинеску државу: Невезан је за међународно уређење засновано на правилима и закону, и одлучан је да успе користећи крађу и дволичност (Slobodna Evropa 2019).

Најновији случај односи се на наводну крађу технологије за ловац најновије генерације Ф-35, када је помоћник председника САД за националну безбедност Џон Болтон (*John Bolton*) оптужио Кину за крађу технологије летелице Ф-35 приликом производње ловца пете генерације. Изразио је забринутост због преноса војне технологије у Кину, истакавши да је кинески ловац пете генерације веома сличан америчком

Ф-35 и да су га Кинези украли. Раније је саопштено да је Болтон у Кијеву разговарао са секретаром Савета за националну безбедност и одбрану Украјине Александром Данилуком о подршци евроатлантским интеграцијама Украјине и начинима да се заштити индустрија земље од „неморалног понашања Кине". Амерички лист Вол стрит журнал (*The Wall Street Journal*) је пре тога саопштио да Болтон тежи да спречи кинеску компанију „*Skajrizon erkraft*" да купи више од 50 одсто акција великог украјинског предузећа за авио-производњу „*Motor sič*" (B92 2019).

Бивши кинески радници у холандској корпорацији ASML Holding N.V. (*ASML*) украли су мноштво корпоративних тајни, наносећи корпорацији штету од неколико стотина милиона евра. То пише холандски финансијски лист „*Het Financieele Dagblad* (ФД)", на основу сопствене истраге. Компанија *ASML* је један од водећих светских произвођача опреме за конструисање чипова. Кинески радници, запослени на високим позицијама, а са везама у кинеском Министарству за науку и технологију, годинама су имали приступ интерној мрежи података у америчкој подружници холандског гиганта у Сан Хозеу, одакле су крали изворне кодове, софтвер, стратегије пласмана и цена и тајна упутства за употребу опреме. Крађу је организовала конкурентска компанија XTAL Incorporated (*XTAL*), коју је 2004. године основао бивши кинески радник *ASML* -а, а током времена још неколико кинеских радника прешло је из холандске у конкурентску компанију, која је у веома кратком времену успела да искористи украдено знање и за свега годину дана преотме Холанђанима велике купце, између осталих и електрогиганта Самсунг (*Samsung*). Калифорнијски суд изрекао је крајем 2018. године пресуду, која до сада прошла готово неопажено у медијима, а по којој је конкурентска фирма *XTAL* холандској корпорацији дужна да исплати 223 милиона евра на име одштете. Према писању холандског финансијског листа ФД, кинеска влада је индиректно умешана у индустријску шпијунажу, иако *ASML* за то нема чврсте доказе. Један од извештаја којима лист располаже, међутим, показује да је матична кућа фирме основане 2014. године уживала финансијску подршку Кине у циљу освајања што јаче позиције на светском тржишту чипова.

Штета од неколико стотина милиона евра нанета холандској компанији *ASML*, са седиштем у Фелдховену, на југу Холандије, чини ову крађу највећом индустријском шпијунажом икад (Mondo, 2019n).

Још један случај индустријске шпијунаже догодио се када су амерички цариници и граничари у августу 2017. године отворили пртљаг кинеске пољопривредне делегације, нашли су коверте које садрже посебно генетски модификован пиринач и друге врсте семена, за које тврде да су украдени од једне компаније у Арканзасу. Према кривичној пријави поднетој у Канзасу, то семе, генетски измењено за фармацеутску употребу уз утрошак више милиона долара, набављено је на нелегалан начин уз помоћ двојице кинеских емигранта-биљног генетичара у истраживачком центру у Арканзасу (који је основало министарство пољопривреде) и биотехнолога, који је дипломирао на Државном универзитету Луизијане, а ради у компанији из Колорада, која је поменуто семе и произвела (Jašarević 2018).

О активностима кинеске индустријске шпијунаже се све више говори и пише у САД. Тако, Мишел ван Клив (*Michelle Van Cleavei*), бивша председница Националне службе за контрашпијунажу САД, тим поводом за Њузвик (*Newsweek*) је истакла да је истина да Кина доживљава запањујући привредни раст, али већина људи не зна да је део тога заснован на систематском програму чисте крађе који њихова држава спроводи. Компаније као што су Моторола (*Motorola*), Форд (*Ford*), Ценерал моторс (*General Motors*), Дипон (*Du Pont*) и друге-приватни покретачи иновација и профита-све су на мети Кинеза. Ван Кливова и званичници контраобавештајне службе кажу да су Кинези необично интелигентни и стрпљиви. „Они потајно ангажују комерцијална предузећа да сакупљају стране технологије", објашњава она. „Убацују „скупљаче" у америчке компаније како би себи олакшали прибављање нових технологија. Пекинг у САД има неформалну организацију која помаже да се ти стручњаци прате како би могли да планирају њихов следећи потез – што значи да ће у том погледу ствари постати још горе. Број пословних људи, научника, инжењера, свршених студената и комерцијалних предузећа из Кине који раде у САД наставља да расте и далеко превазилази наше

могућности да контролишемо њихове потенцијалне илегалне активности“ (Jašarević 2018).

Још један од метода којима се врши индустријска шпијунажа у пракси представљају такозвани ‘’спавачи’’. Наиме, много је студената које Кина шаље у САД и који годинама мирују пре него што их позову у акцију, обично након што се запосле у некој фирми која користи високу технологију. Ту је још једна додатна корист: кинеско улагање у обавештајну службу је „практично никакво и све врло уверљиво могу да порекну. Ако погледамо суђења кинеским ‘шпијунима’ додаје он, „готово увек су у питању Кинези који су прва генерација емиграната у САД-они који и даље гаје етничке, културне и емоционалне везе са мајком Кином”, а умешани су и Американци који немају кинеско порекло. „У принципу, претпостављам да већина њих сарађује са Кинезима напросто као плаћеници-због новца. А Кинези умеју добро да искористе све што те људе чини погодним за сарадњу” (Jašarević 2018).

Сматра се и да САД немају свеобухватну стратегију за супротстављање кинеској шпијунажи, иако се Бела кућа и администрација с тим не слажу. Бела кућа је издала и брошуру под називом: ‘’Стратегија за сузбијање крађе пословних тајни САД’’ (*Administration Strategy on mitigating the theft of U.S. Trade Secrets*), која је навела пет области деловања: дипломатско ангажовање, добру праксу заштите на иницијативу самих индустријских предузећа, интензивирање домаћих законских истрага, ревизију законодавства, помоћ акционара и кампању за информисање јавности. Америчка обавештајна агенција ЦИА и ФБИ имају тај задатак, али то ни најмање није смањило кинеску шпијунажу, бар судећи по случајевима који се гомилају у америчким федералним судовима. Од 2008. до 2010. Министарство правосуђа водило је 26 истрага, које су за резултат имале више од 40 Кинеза осуђених по оптужбама за шпијунажу, крађу индустријских и државних тајни САД и илегални извоз проблематичних материјала у Кину. Истраживање које је спровео Ројтерс (*Reuters*) утврдило је да се у последњих осам година од 280 кривичних гоњења због нелегалног извоза оружје 66 односило на Кинезе (Jašarević 2018).

Трампова администрација је 2018. године чак разматрала и меру којом би се забранило кинеским студентима да студирају у САД, као део „пакета“ мера за борбу против индустријске шпијунаже. Ипак, након многих расправа, ова идеја је одбачена јер се сматрало да би то могло да нанесе више штете него користи америчким интересима (O'Malley 2018).

Познати је и случај бившег инжењера компаније Боинг Донгфан „Грег" Цхунг-а (*Dongfn Grege Chung*), кинеског порекла, осуђеног на 16 година затвора због крађе пословних тајни у вези са сателитским програмом САД-а. Задуго ће остати запамћен у историји, јер је чак 30 година снабдевао Кину украденим информацијама, достављајући најмногољуднијој земљи на планети више од 350.000 докумената из једне од најважнијих и најзаштићенијих сфера за САД (Mujanović 2012).

Из свега наведеног, може се закључити да индустријска шпијунажа, нарочито у виду крађе интелектуалне својине, доноси милијарде долара добити, па услед тога расте њен значај у савременом свету. Афера у вези са компанијом *Huawei* показала је сву комплексност овог питања. Показало се да индустријска шпијунажа поприма различите форме и да се методологија рада обавештајних служби развија из дана у дан. Посебно опасан облик индустријске шпијунаже представља крађа интелектуалне својине уз помоћ савремених информационо - комуникационих технологија. Сајбер простор представља ново бојно поље између великих сила, где се применом модерних технологија могу остварити много бољи резултати, него што би се догодило стварањем агентуре у страној држави. Утврђено је да су акти индустријске шпијунаже вршени у осетљивим секторима привреде погођене државе (САД у овом случају), или према критичној инфраструктури, а кинеска индустријска шпијунажа односила се на (наводне) крађе технологије за ловац најновије генерације Ф-35, крађе корпорацијских тајни више компанија као што су Моторола, Форд, Џенерал Моторс, Дипон, укључујући и познате америчке компаније у области пољопривреде, затим акте индустријске шпијунаже у области сателитског програма, као и крађе интелектуалне својине уз помоћ такозваних „спавача“, односно кинеских студената у САД.

Мада је у овом раду акценат стављен на индустријску шпијунажу извршену од стране Кине у односу на САД, *то не значи да из супротног смера нема сличних напада*. Може се без устручавања констатовати да ниједна велика сила не преза од вршења аката индустријске шпијунаже, без обзира на то да ли је циљ тих активности политичког, одбрамбеног или економског карактера. Због тога је одбрана од индустријске шпијунаже изузетно комплексно питање, које захтева ангажовање целокупног безбедносног апарата погођене државе. Не треба занемарити ни чињеницу да је безбедносни апарат савремених држава, неретко, оптерећен и другим изазовима, као што је тероризам, организовани криминал, корупција и слично, па се намеће дилема да ли су постојећи ресурси (кадровски и материјално-технички) довољни за борбу против индустријске шпијунаже. Потребно је да и потенцијалне жртве индустријске шпијунаже поведу више рачуна о заштити властитих истраживања и пословних тајни, као и да предузму адекватне мере у области безбедности информација. Све у свему, индустријска шпијунажа (посебно у светлу афере око компаније *Huawei*) представљаће озбиљан политички проблем у односима Кине и САД, што може довести до даље ескалације сукоба између супер - сила у наредном периоду.

ЛИТЕРАТУРА

Androulidakis Iosif, and Emmanouil Fragkiskos-Kioupakis. 2016. *Industrial Espionage and Technical Surveillance Counter Measurers*, New York: Springer.

B92. 2019. „Alarm u Vašingtonu: „Kina nam je ukrala tehnologiju za F-35“. 28. avgust 2019. https://www.b92.net/biz/vesti/svet.php?yyyy=2019&mm=08&dd=28&nav_id=1583590

Бечка конвенција о дипломатским односима [БКДО], *Службени лист СФРЈ-додатак*, бр. 2/64).

Бошковић, Мило. 2017. *Лексикон безбедности*, Београд-Нови Сад: Службени гласник.

Кривични законик Републике Србије, *Службени гласник Републике Србије*, бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019.

Marković, Marko. 2019. „Amerika je zabranila *Huawei*: Kreće bitka za digitalno nadziranje sveta". *Startit*. 17. maj 2019. https://startit.rs/amerika-je-zabranila-huawei-krece-bitka-za-digitalno-nadziranje-sveta/.

Mondo Portal. 2019s. „SAD tužile Huawei za prevare, špijunažu, krađu patenata". 28. januar 2019. https://mondo.rs/MobIT/Tech-Vesti/a1162564/SAD-Huawei-tuzba-SAD-tuzile-Huawei-SAD-tuzi-Huawei-SAD-tuzba-Huawei-Kina.html.

Mondo. 2019n. „Najveća industrijska špijunaža ikada!" 11. april 2019. https://mondo.rs/Info/Svet/a1178973/Industrijska-spijunaza-kineski-radnici-ukrali-tajne-ASML-a.html.

Mujanović, Erol. 2012. „Industrijska špijunaža: krađe u milionima". *Aljazeera Balkans*. 14. maj 2012. http://balkans.aljazeera.net/vijesti/industrijska-spijunaza-krade-u-milionima.

O'Malley, Brendan. 2018. „White House discussed unilateral ban on Chinese students", *University World News*. 04 October 2018. https://www.universityworldnews.com/post.php?story=20181004180117952.

Petković, Todor. 2009. *Poslovna špijunaža i ekonomsko ratovanje*. Novi Sad: Protexi Group System.

President of the United States. 2020. Executive Order on Securing the Information and Communications Technology and Services Supply Chain, May 15, 2019, https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/ , last accessed 31 March 2020.

Север, Александар. 2017. *Историја КГБ*. Београд: Логос.

Slobodna Evropa. 2019. „Slučaj Huawei kao triler o aferama, špijunaži i politici". 31 januar 2019. https://www.slobodnaevropa.org/a/slu%c4%8daj-huawei-kao-triler-o-aferama-%c5%a1pijuna%c5%bei-i-politici/29742427.html.

Стајић, Љубомир, и Горан Милошевић. 2017. „Финансијска делатност државе као фактор економске безбедности-осврт на Републику Србију.“ *Српска политичка мисао* 55(1): 175-195.

Тепавац, Дејан. 2019. „Шпијунажа као облик угрожавања пословних информација.“, *Војно дело* 71(3): 163-173.

Уредба о ратификацији Париске конвенције за заштиту индустријске својине од 20. марта 1883. године, ревидирана у Брислу 14. децембра 1900. године, у Вашингтону 2. јуна 1911. године, у Хагу 6. новембра 1925. године, у Лондону 2. јуна 1934. године, у Лисабону 31. октобра 1958. године и у Стокхолму 14. јула 1967. године [УПКЗИС], *Сл. лист СФРЈ - Међународни уговори и други споразуми*-бр. 5/74 и *Сл. лист СФРЈ - Међународни уговори*, бр. 7/86 - др. уредба).

Цветићанин, Невен, и Милан Благојевић. 2019. „Унутрашњи конфликти и спољна политика САД између интервенционизма и изолационизма“, *Српска политичка мисао* 65(3): 43-62.

Čavić, Marko. 2019. „Zašto su se SAD „okomile“ na Huawei?“. *Mondo*. 20. maj 2019. https://mondo.rs/MobIT/Tech-Vesti/a1187590/Huawei-i-SAD-sta-je-problem-optuzbe-za-spijunazu.html.

Siniša Domazet

Faculty for security studies, Educons University

Zdravko Skakavac

Faculty for legal and business studies Lazar Vrkatić, Novi Sad

INDUSTRIAL ESPIONAGE IN CASE OF CHINA AND USA

Resume

Industrial espionage, especially in the form of intellectual property theft, generates billions of dollars profit, and thereby its importance in the modern world is increasing. The scandal regarding the company *Huawei* has showed the complexity of the issue. The company concerned has become a "stumbling block" between the two superpowers, given the numerous accusations that are coming from the US side that Huawei, in general sense, engaged in industrial espionage on behalf of the Chinese government. It was found that the Chinese industrial espionage related to the alleged theft of technology for fighter of the latest generation F-35, corporate secrets of many companies, such as Motorola, Ford, General Motors, DuPont, well-known US companies in the field of agriculture, and in the field of satellite program, as well as theft of intellectual property with the help of so-called "sleepers'' in form of Chinese students in the United States. It turned out that industrial espionage takes many forms and that the methodology of intelligence agencies is developing day by day. A particularly dangerous form of industrial espionage represents the theft of intellectual property with the help of modern information and communication technologies. Numerous detected activities in the field of industrial espionage shows that no superpowers does not shy away from committing acts of industrial espionage, regardless of whether the objective of the activities has political, defense or economic character. Although in this paper emphasis is placed on industrial espionage conducted by China against the US, it does not mean that from the opposite direction has similar attacks. Therefore, defense against industrial espionage is very complex issue that requires the

involvement of the entire security apparatus of the affected country. We should not neglect the fact that the security apparatus of modern states, often, burdened with other challenges, such as terrorism, organized crime, corruption which, however, imposes a dilemma whether existing resources (personnel and material-technical) are sufficient to fight against industrial espionage. It is necessary that the potential victims of industrial espionage pay greater attention to the protection of its own research and trade secrets, as well as to take appropriate measures in the field of information security. It is necessary to increase the counter-intelligence protection, but also to develop effective systems of defense against cyber attacks and disclosure of business secrets. Industrial espionage (particularly in light of the scandal around the company Huawei) will be a serious political problem in the relations between China and the US, which may lead to further escalation of the conflict between these states in the future.

Keywords: *law, politics, security, China, USA, industrial espionage, Huawei*

* Овај рад је примљен 7. априла 2020. године, а прихваћен за штампу на телефонском састанку Редакције, 1. октобра 2020. године.