VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, O. P. S., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

PRŮMYSLOVÁ ŠPIONÁŽ A EKONOMICKÉ SOUPEŘENÍ FIREM

Autor práce: Radek Stejskal

Studijní obor: Bezpečnostně právní činnost ve veřejné správě

Forma studia: Kombinovaná

Vedoucí práce: Ing. Jiří Dušek, Ph.D.

Katedra: Katedra právních oborů a bezpečnostních studií

2012

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v této práci.

Souhlasím, aby práce byla uložena v knihovně Vysoké školy evropských a regionálních studií v Českých Budějovicích a zpřístupněna v souladu s § 47b zákona č. 111/1998 Sb. v platném znění.

……

Děkuji vedoucímu bakalářské práce Ing. Jiřímu Duškovi, Ph.D. za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

STEJSKAL, R. *Průmyslová špionáž a ekonomické soupeření firem : bakalářská práce.* České Budějovice : Vysoká škola evropských a regionálních studií, o. p. s., 2012. 92 s. Vedoucí bakalářské práce : Ing. Jiří Dušek, Ph.D.

Klíčová slova: ekonomické soupeření firem, konkurence, konkurenční výhoda, průmyslová špionáž

Bakalářská práce řeší, jaký vliv má ekonomické soupeření firem a snaha o získání konkurenční výhody na průmyslovou špionáž. Hlavním cílem je analýza historie průmyslové špionáže, metod získávání a sdílení informací, ekonomického soupeření firem, dopadů průmyslové špionáže na postižené subjekty a úlohy tajných služeb. Práce analyzuje případy průmyslové špionáže globálního konkurenčního prostředí a předkládá možnosti k eliminaci rizika výskytu ztrát klíčových informací.

Práce je členěna do sedmi částí. První čtyři části se věnují terminologii a teoretickým poznatkům o průmyslové špionáži, metodám k získávání informací a škodám způsobených průmyslovou špionáží. Seznamují s historií průmyslové špionáže na prvních případech, dále se sdílením informací a koloběhu dat v globalizovaném světě a s ekonomickým soupeřením firem. V konkrétních číslech podává hodnocení rizik s ohledem na geopolitickou situaci, jak jsou v jednotlivých zemích často vnímána. Zbývající části se již věnují konkrétním způsobům boje a ochrany proti průmyslové špionáži, jednotlivým případům průmyslové špionáže globálního konkurenčního prostředí se zaměřením na různé specifické případy. V závěru práce jsou vyhodnoceny škody, doporučena opatření k eliminaci potenciálu rizika z napadení a nastíněny způsoby ochrany před průmyslovou špionáží.

ABSTRACT

STEJSKAL, R. *Industrial Espionage and Economic Competition of Businesses : Bachelor thesis.* České Budějovice : The College of European and Regional Studies, o. p. s., 2012. 92 p. Supervisor : Ing. Jiří Dušek, Ph.D.

Key words: economic competition, competition, competitive advantage, industrial espionage

The bachelor thesis solves what is the impact of economic competition and pursuit to competitive advantage of companies on industrial espionage. The main target is analysis history of industrial espionage, method of getting and share of information, economic competition of companies, impacts of industrial espionage on affected subjects and task of intelligence agencies. The thesis analyzes cases of industrial espionage of global competitive world and put suggestions to elimination of risk on damage of key information.

The bachelor thesis has been divided in seven parts. The first four parts describe terminology and theoretical knowledge's above industrial espionage, method to getting of information and damages where was caused by industrial espionage. The first parts inform with history of industrial espionage in a first cases, furthermore with share of information and cycle of data in global competitive world and with economic competition of companies. In real numbers present evaluation of risk in view of the geopolitical situation how are often sensed in individual countries. The remaining parts concern on real methods of fight and protection against industrial espionage of global competitive world already with concern on different specifically cases. In the conclusion of the thesis there are evaluated the damages also are preventive actions to elimination of risk an attack recommended and the methods of protection against industrial espionage describe.

OBSAH

Úvod

Společnosti se v současné době nacházejí ve stále silnějším konkurenčním prostředí, které vychází ze stále větší deregulace, otevírání trhů a technologických změn výroby. Zákazníci stupňují tlak na zlepšování technických parametrů výrobků a současně na snižování ceny nových produktů dodávaných na trh. Výrobci jsou tak nuceni hledat levnější lokality výroby, přesouvat tak i svá technologická a vývojová know-how a snažit se využívat všechny možnosti k tomu, aby jejich výrobky byly konkurenceschopné. Jsou obory, kde vývoj spojený se zavedením nového produktu na trh vyžaduje nemalé náklady.

S příchodem nových forem komunikace, stále více propojeného světa a informačních kanálů, se stává pro společnosti životně důležité, získávat včasné relevantní informace o konkurenci založené na soustavném monitoringu trhu. Tímto způsobem mohou být společnosti více konkurenceschopné a získají dobrý základ pro správné strategické rozhodování. Společnosti jsou důsledkem silného konkurenčního boje nuceny maximálně využívat všechny zdroje informací k analýzám o konkurentech, o jejich postavení na trhu, jejich produktech a informacích o nových technologiích. K získávání informací slouží jak legální veřejné zdroje, tak ale i zdroje neveřejné, jejichž použití je mnohdy nelegální či přinejmenším neetické. Používání metod k osvojení si dokonalejších technologií a nových výrobků tou nejlehčí cestou, tedy pouhou krádeží, je staré jako lidstvo samo a špionáž je obecně považována za jedno z nejstarších řemesel na světě.

Po skončení studené války se špionážní potenciál, který dříve více působil v oborech vojenské výroby, přeorientoval na špionáž průmyslovou. Průmyslová špionáž se tak zostřila a zintensivnila. Prostředky vázané na vojenskou a politickou špionáž byly přeorientovány na špionáž vědecko-technickou.

Vzhledem k těmto faktům a aktuálnosti problému v prostředí dnešního globálního světa si i v období po přechodu ze studené války na současné vysoce konkurenční prostředí tento problém zasluhuje naši pozornost. Zpracováním tohoto tématu se pokusím analyzovat historii průmyslové špionáže, poukázat na projevy současných špionážních praktik, a umožním tak získat alespoň základní informace o situaci v dnešním konkurenčním prostředí.

1 Cíl a metodika bakalářské práce

Hlavním cílem bakalářské práce je analyzovat historii průmyslové špionáže a v porovnání se současnými případy ji ukázat v dnešní podobě, v projevech současných špionážních praktik a v období po přechodu ze studené války na současné vysoce konkurenční prostředí. Prezentovat tak průmyslovou špionáž ne jako zašlou nepoužívanou metodu dávné minulosti, ale jako činnost neustále aktivní a v podmínkách globálního prostředí nadále velmi intenzivně používanou. Objasnit příčiny jejího vzniku a dle osobních zkušeností autora ji komentovat v současných podmínkách globálního trhu a ekonomického soupeření firem. Čína, dnešní nejrychleji rostoucí ekonomika, hladoví po technologii, a ani často nechápe západní pojem autorských práv. Průmyslová špionáž je v současných podmínkách velmi obtížně identifikovatelná, kontrolovatelná, s vysokým indexem hospodářské škodlivosti a bezpečnostního rizika pro společnost.

Bakalářská práce je integrována do třech hlavních částí.

První, teoretický oddíl, má tři části. V úvodní kapitole „Cíl a metodika BP“ je charakterizován cíl a metodický postup práce. V druhé kapitole práce sumarizuje teoretické poznatky o průmyslové špionáži, informace o tajných službách, metodách a škodách v konkrétních číslech následkem průmyslové špionáže. Třetí kapitola rozborem literatury stručně popisuje historii na prvních případech průmyslové špionáže a analyzuje důvody, které vedou k „nesmrtelnosti“ tohoto počínání.

Analytický oddíl je integrován do dalších dvou kapitol. Čtvrtá kapitola analýzou dalších navazujících projevů o sdílení informací, koloběhu dat a o ekonomickém soupeření firem poukazuje na vazby k hlavnímu tématu práce. V konkrétních číslech poukazuje na rizika ztráty dat s ohledem na geopolitickou situaci podle toho, jak jsou v jednotlivých zemích často vnímána. Pátá kapitola analyzuje samotné příčiny, které vedou k ekonomickému soupeření firem a trendy obchodní spolupráce.

V syntetické části, v šesté a sedmé kapitole, práce poukazuje na možnosti způsobů boje a ochrany k eliminaci rizik napadení a dopadů případného napadení průmyslovou špionáží a demonstruje zveřejněné případy průmyslové špionáže současnosti. Šestá kapitola odvozuje z konkrétních hrozeb možné způsoby boje a ochrany před průmyslovou špionáží. Sedmá kapitola prezentuje jednotlivé případy průmyslové špionáže globálního konkurenčního prostředí po pádu „železné opony“. Svým výběrem případů se zaměřuje na různé specifické případy.

Pro naplnění cílů této práce jsou věcné informace čerpány z pracovních i osobních zkušeností autora práce pracujícího více než dvacet let v oddělení vývoje komponentů pro automobilový průmysl. Hlavní metoda použitá v bakalářské práci je analýza, pomocí které byly zjišťovány dostupné informace o historii průmyslové špionáže a případech z globálního konkurenčního prostředí. Analýzou literatury, analogií a komparativní metodou byly zkoumány podružné aspekty průmyslové špionáže. Práce vychází z řady odborných publikací k tématice špionáže a konkurenčního zpravodajství, dále z odborných časopisů a denního tisku, především z odborného měsíčníku Technik a Technického týdeníku. Byly využity výsledky studie společnosti McAfee podniknuté v šesti zemích, které byly porovnávány a vyhodnocovány. Analyticko-syntetickou metodou byly vyvozeny závěry a doporučena opatření. Zároveň je však třeba podotknout, že vzhledem k dynamickému vývoji v této oblasti existuje jen omezený počet relevantních a aktuálních informačních zdrojů. Mezi primární zdroje práce patří literatura, ale na rozdíl od vojenské špionáže se průmyslová špionáž nestala předmětem k většímu zpracování v odborné literatuře. Existuje o ní tedy jen omezený počet literárních zdrojů, což je příčinou, že bylo v práci ve větší míře využito i ostatních zdrojů informací z veřejně dostupných internetových stránek.

2 Průmyslová špionáž

Průmyslová špionáž je činnost provozovaná různými subjekty, kterými mohou být různé státní organizace, komerčními subjekty či jednotlivé osoby. Cílem této činnosti je získání utajovaných informací z oblasti průmyslu a jejich následného využití pro vlastní prospěch.

GIFFORD[1] o průmyslové špionáži říká: „Průmyslová špionáž se zabývá sledováním firem nebo organizací, aby zjistila, jaké inovace a plány mají ve své činnosti a aby ilegálně získala tajemství o nových výrobcích, technologiích, vzorcích nebo výrobních procesech. Výzkum a vývoj nových produktů může trvat řadu let a stát spousty peněz. Pro některé společnosti je odhalení tajemství konkurentova produktu nejrychlejším a nejlevnějším způsobem, jak získat konkurenční výhody a náskok. Průmyslovou špionáž provádějí i jednotlivé země, které sledují ekonomiku ostatních zemí.

Bezpečnostní fórum Bádenska-Württemberska uvedlo, že prostřednictvím průmyslové špionáže jsou firmy zkoumány konkurencí. Proto se při průmyslové špionáži také často hovoří o konkurenčním špehování, hospodářské špionáži nebo konkurenční špionáži. Pátrající podniky mají zesílený zájem o:[2]

- Informace o konkurenci, trhu, technologických postupech a zákaznících,
- Aktuální know-how k vývojům výrobků a výrobních technikách,
- Cenové informace,
- Kalkulace,
- Koncepční studie.

2.1 Tajné služby a průmyslová špionáž

Tajné služby pracují vskrytu a chránit výsledky svého tajného pátrání před přístupem ostatních je součástí jejich úkolu, Pramenů o „válce v temnotách“ je poskrovnu a jsou málomluvné stejně jako ty, které se týkají přímo špionáže. Kde tedy se

[1] GIFFORD, C. *Svět špionáže.* Havlíčkův Brod : Nakladatelství Fragment, s.r.o., 2006. s. 18. ISBN 80-253-0227-X.
[2] *SiFo-Studie 2009/10 : Know-how-Schutz in Baden-Württemberg.* 1. vyd. Stuttgart : Steinbeis Edition, 2010. s. 21. ISBN 978-3-941417-20-5.

můžeme dozvídat podrobnosti o „tajných vědomostech“ těchto institucí? Jak lze mít jistotu, že získané informace nejsou součástí nějaké (tajné) dezinformační strategie?[3]

Zatímco špionáž je tak stará jako svět sám, tajné a zpravodajské služby vznikly teprve před několika desetiletími. První úřední tajná služba byla založena na obranu proti německé špionáži v Londýně před necelými sto lety – v roce 1909 – za ministerského předsedy Asquitha a pod názvem *Secret Service Bureau*. Mělo trvat jen několik let, než britský příklad následovaly i další země: Německo konstituovalo první tajnou službu v roce 1913, Rusko roku 1917, Francie roku 1935 a Spojené státy roku 1942. Dnes si i ta nejchudší země připadá suverénní teprve tehdy, až když provozuje aspoň velký aparát takové služby.[4]

„*Tajná služba musí zůstat tajnou*“ – tolik výstižné vyjádření amerického generála George C. Marshalla. To je také důvod, proč akta tajných zpravodajských služeb odpočívají v dobře zajištěných trezorech, některé dokonce na věčné časy. Například archivy britské „Secret Intelligence Service“ jsou, stejně jako dříve, stále uzavřeny – včetně různých dokumentů z 16. a 17. století.[5]

Proto, aby se zájemce dostal k informacím o práci tajných služeb, uchyluje se také k takzvaným „otevřeným zdrojům“. Ve spojených státech je zmíněný zákon – Freedom of Information Act – podstatnou součástí investigativní žurnalistické práce, součástí, bez které by nebyla možná různá odhalení, ke kterým v minulosti došlo. Ve Velké Británii vstoupil podobný zákon v platnost 1. ledna 2005. V Německu naopak až do konce roku 2005 i nadále platil princip „úředního tajemství“, to znamená, že s veškerými informacemi, které mají v Německu k dispozici veřejná úřední místa, se i mimo nezbytnost tyto informace skutečně ochraňovat do té doby stále ještě zacházelo jako s materiálem „důvěrným“ nebo dokonce „tajným“. Teprve v lednu 2006 vstoupil konečně i v Německu v platnost zákon o svobodném přístupu k informacím, který v červenci 2005 předložila zelenorudá vláda kancléře Gerharda Schrödera. Tím

[3] ULFKOTTE, U. *Válka v temnotách : skutečná moc tajných služeb.* 1. vyd. Praha : Ikar, 2007. s. 14. ISBN 978-80-249-0959-2.
[4] ULFKOTTE, U. *Válka v temnotách : skutečná moc tajných služeb.* 1. vyd. Praha : Ikar, 2007. s. 20. ISBN 978-80-249-0959-2.
[5] PIEKALKIEWICZ, J. *Historie světové špionáže : agenti, systémy, akce.* 1. vyd. Praha : Naše vojsko, 2004. s. 11. ISBN 80-206-0738-2.

i německý občan získává zásadní právo nahlédnout do materiálů různých institucí a úřadů. Státní tajemství jsou z toho pochopitelně i nadále vyňata.[6]

Každý zájemce o problematiku tajných služeb narazil v květnu 2005 na rozsáhlou síť čínských špionů, koordinovaných z Belgie, které řídila Číňanka Li-Li Whuang, a kteří v Nizozemsku, Velké Británii a Německu vyzvídali údaje firem, mimo jiné u francouzského dodavatele automobilových součástí, ve firmě Valeo. Čínské špiony objevila v témž období i švédská zahraniční tajná služba SAEPO (Säkerhetpolisen) v řadách studentů na výměnném pobytu. A Florida International University oznámila, že otevírá první soukromou špionážní školu ve Spojených státech, na které mají být pro americké služby připravování budoucí vyhodnocovači a analytici. Pokud nasbíráme velké množství takových zpráv, dostatečně se rozšíří vhled do světa tajných služeb, od okolí dříve izolovaného.[7]

2.2 Hlavní úkoly průmyslové špionáže

Hlavním úkolem tajné služby je informační funkce, to znamená získávání informací; potom následuje ochranná funkce, kterou se rozumí pasivní ochrana proti nepřátelské špionáži a sabotážím. Třetím úkolem je kontrašpionáž neboli ofenzivní průzkum cizích zpravodajských služeb. Čtvrtým úkolem jsou tajné informace, k nimž se počítají sabotáže, diverze, subverze a psychologické vedení války. Různorodé informace, které se dostanou do centrály, se pak člení podle svého významu, porovnávají s ostatními prameny a odpovědní pracovníci je analyzují. Tyto informace mají sloužit jako pomůcka pro rozhodování politiků a vojáků, umožnit jim včas rozpoznat zámysly veřejného, nebo potenciálního protivníka tak, aby vedení státu mohlo správně a v pravý čas reagovat. K prvořadým úkolům tajných služeb patří nepřetržité shromažďování politických informací. Část se získává oficiální cestou prostřednictvím diplomatů, část vyhodnocováním tiskových zpráv, rozhlasového a televizního vysílání, literatury, analýz statistiků, důkladným pozorováním politického života a hospodářských procesů v určité zemi.[8]

---

[6] ULFKOTTE, U. *Válka v temnotách : skutečná moc tajných služeb.* 1. vyd. Praha : Ikar, 2007. s. 15-16. ISBN 978-80-249-0959-2.
[7] ULFKOTTE, U. *Válka v temnotách : skutečná moc tajných služeb.* 1. vyd. Praha : Ikar, 2007. s. 19-20. ISBN 978-80-249-0959-2.
[8] PIEKALKIEWICZ, J. *Historie světové špionáže : agenti, systémy, akce*. 1. vyd. Praha : Naše vojsko, 2004. s. 12. ISBN 80-206-0738-2.

Získávání západních technologií patří k prvořadým úkolům východních tajných služeb. Navzdory enormním vlastním investicím do výzkumu a rozvoje v posledních třiceti letech měli Sověti pouze malé vyhlídky v příštích desetiletích na snížení své závislosti na Západě, především co se týče technologií. I když v sovětském hospodářském systému a v managementu byly plánované obsáhlé reformy, SSSR byl ještě dlouhou dobu závislý na západních inovacích. Aby tento odstup byl zmírněn, vysílaly východní tajné služby rok co rok své nejlepší agenty a špiony do západních průmyslových center. Měli získat kopie výkresů, zkušební vzorky, nebo testovací přístroje, se kterými by mohl být zlepšen technologický stav a výkonnost sovětského zbrojního i jiného průmyslu a snížena závislost na špičkové produkci ze západních skladů.[9]

Cíle ruských špionů jsou dnes trochu jiné než jejich předchůdců z KGB a GRU. Zatímco dříve se pídili hlavně po politických rozhodnutích, nyní hlavně shromažďují poznatky z vojensko-technické, vědecké a průmyslové, dále o přírodních zdrojích. Odhaduje se totiž, že v některých strategicky důležitých technologiích zaostává Rusko za vyspělým Západem až o dvacet let.[10]

2.3 Metody průmyslové špionáže

Průmyslová špionáž je v současnosti jedním z nejčastěji publikovaných projevů zpravodajské aktivity, který se dnes stále častěji nalézá převážně v podnikatelském světě velkých firem, nežli v tajných službách států. Průmyslová špionáž a její metody se odvíjí od úrovně jejich technologických možností, je mnohdy označována za technologickou nebo kancelářskou špionáž. Novinové titulky plní také internetová špionáž. Korporace utrpí každým rokem ztráty duševního vlastnictví za miliardy dolarů kvůli nezákonnému kopírování a prodeji obchodních tajemství konkurenci na černém trhu za účelem obohacení nebo kvůli vydírání.

Během 90. let dvacátého století, kdy dochází k největšímu boomu tohoto druhu výzvědné činnosti, se ujímají různé druhy a metody průmyslové špionáže.

---

[9] PIEKALKIEWICZ, J. *Historie světové špionáže : agenti, systémy, akce*. 1. vyd. Praha : Naše vojsko, 2004. s. 497. ISBN 80-206-0738-2.

[10] PACNER, K. *Atomoví vyzvědači studené války*. 1. vyd. Praha : Epocha, 2009. s. 476. ISBN 978-80-7425-001-9.

Vedle tradičního kopírování dokumentů a plánů se jedná povětšinou o různé druhy odposlechů:[11]

- elektronický odposlech,
- telefonní odposlech,
- rádiový odposlech,
- počítačová špionáž.

V roce 1992 na bezpečnostní konferenci IFIP/SEC '92 z příspěvku o „informační kriminalitě" (Fortrie I.F.B.: „IT Crime – An Intelligence Report") vyplynulo, že anglické a americké tajné služby disponují schopností odposlouchávat celých 100 % satelitního spojení, 85 % radiové komunikace, 90 % telefonních spojů, a dokonce 75 % vybraných poštovních spojů.[12]

Česká společnost Probin, specialista na technologie proti odposlechům a ochranu soukromí, se spojila s francouzským lídrem v oblasti telekomunikační bezpečnosti, společností TRCOM. Na náš trh se tak dostává nejvyspělejší řešení pro ochranu před odposlechy. Speciální software s názvem Cryptosmart chrání přenos dat, volání i SMS. Software je dostupný na SD kartě pro telefony s operačním systémem Android nebo ve speciálním telefonu S:PHONE, který slouží výhradně k šifrovanému volání. Novinkou je také USB disk, se kterým je možné šifrovaně volat a přenášet data, pokud je uživatel připojen k internetu na počítači. I když o vydání příkazu k odposlechu a záznamu telekomunikačního provozu může podle současné legislativy rozhodnout pouze soud, případy z poslední doby ukazují, že reálná praxe je zcela odlišná. Šifrovací technologie jsou tak zatím jedinou možností, jak své informace chránit před útoky zvenčí.[13]

Elektronický odposlech – většina firem provádí velkou část svých transakcí či řízení prostřednictvím radiového vysílání (mobilní telefony, monitorovací systémy, systémy pro ostrahu budov, faxy, dálnopisy, apod.). Dnešní moderní monitorovací systémy jsou schopny odposlechu zvuku či obrazu pomocí mikrovlnné či radiové techniky (odposlech faxů, odposlech informací ze záření monitorů, apod.). A právě

---

[11] *Metody špionáže: Průmyslová špionáž* [online]. Specialista.info, 2006 [cit. 2011-11-04]. Dostupné z WWW: <http://www.magazin.specialista.info/view.php?cisloclanku=2006013001>.

[12] *Třetí světová válka* [online]. 1.9.2007 [cit. 2012-01-03]. Dostupné z WWW: <http://www.pravoslav.gts.cz/zn_doby/vres.htm>.

[13] Ochrana soukromí před odposlechy. *Technik.* 2012, č. 4/2012, s. III. ISSN 1214-9802.

tento vysoký stupeň elektronizace organizace vede k nutnosti chránit svá elektronická komunikační a informační zařízení, neboť ta se stávají nejčastějším terčem sledování a odposlechů.

Telefonní odposlech – v době mobilních telefonů donedávna existoval omyl ohledně jejich možného odposlechu. Mobilní operátoři totiž často tvrdili, že mobilní telefony jsou bezpečné a není možné je odposlouchávat. Ano, tak tomu opravdu do roku 1994 bývalo, nežli švédské zpravodajské služby přišly na metodu, jak tento problém odstranit. V současnosti není téměř pro nikoho nemožné tuto metodu při patřičném vybavení zvládnout. U pevných telefonních linek se často používaly typické „štěnice" o kterých bude pojednáno v následujícím odstavci. Modernější bezdrátové pevné telefonní přístroje mají sice implementovanou jakousi slabou ochranu proti odposlechu, kterou však není těžké při patřičných znalostech překonat. Např. v Británii tyto telefony fungovaly ve dvou pásmech (49 MHz a 1 900 MHz – zde je určitá paralela s mobilní komunikací). Paradoxem je, že pokud přístroj vysílá na nízkém pásmu, lze do vzdálenosti 200 m od cíle umístit obyčejný přijímač, naladit frekvenci a pak pouze monitorovat hovory (daný bezdrátový telefon pak vysílá po určitou dobu na stejném pásmu).

Rádiový odposlech – miniaturní rádiové vysílače („štěnice") mohou být maskovány v jakékoliv věci, jejíž velikost ukrytí vysílače dovoluje. Většina radiomikrofonů pracuje v pásmu 30 MHz – 25 GHz, přičemž všeobecně platí, že čím nižší kmitočet, tím mohutnější přístroj a větší dosah. Kvůli složitější zachytitelnosti se používají atypické modulace (pulsní kódové, digitální, subnosné, modulace v rozprostřeném pásmu, apod. – tradiční AM a FM modulace jsou snadno odhalitelné a proto se v přístrojích téměř neobjevují). Miniaturizované přijímače jsou definované jako „prostředky rychlého nasazení", což znamená, že většinou fungují jako záloha či podpora již existujícího odposlechového kanálu. Jednou z největších akcí umisťování štěnic v historii se během studené války stala dohoda mezi USA a SSSR o vzájemném poskytnutí lepších budov pro velvyslanectví uzavřená v roce 1968. Obě země si měly vzájemně v Moskvě a Washingtonu nechat postavit budovu moderního velvyslanectví. Jenže USA naivně věřilo Sovětům, že myslí vše upřímně a díky tomu dostali budovu prošpikovanou odposlechovými zařízeními. Rusové dokonce udělali to, že do betonu přimíchali velké množství funkčních i nefunkčních čipů, díky čemuž se těžko rozlišovalo, která štěnice ve zdi je funkční a která ne.

Počítačová špionáž – v době globální informatizace světa, kdy většina firem a organizací vytváří svoje informační báze dat a datové sklady, je velmi snadné nejen

potenciálního konkurenta zneschopnit vyřazením výpočetní techniky, ale také vytěžit jeho datové sklady a získat tak zajímavé informace o konkurenci. Právě pro tento účel jsou firmami zaměstnáváni různí šikovní hackeři, crackeři, „bílé límečky“ a počítačoví bezpečnostní experti. V některých společnostech již tento systém začíná pomalu a jistě přerůstat do paranoidní ochrany dat před samotnými zaměstnanci organizace, takže nakonec jsou informace přístupné pouze úzké elitě TOP managementu dané organizace, pro jejich práci však nejsou příliš efektivně využitelné. A tak vznikají data pro data. Podívejme se však na typické druhy počítačové špionáže, kterou je možné využít v kontextu průmyslové špionáže: napadení a likvidace počítačové sítě / databázových serverů, odposlech informačních kanálů / datové komunikace, podvržené informace / transakce.

Metod, jak výše uvedených cílů dosáhnout, existuje nepřeberné množství – počítačové viry, spaming, cracking, akce přímého napadení, skryté transakce, sledování paketů, skenování počítačové sítě, napadení uživatelských účtů, apod. - vždy je nutné jasně definovat, čeho chceme dosáhnout a vědět jaké výpočetní prostředky nám jsou dostupné.[14]

2.3.1 Echelon, anglosaský odposlouchávací systém

Evropská unie varuje před anglosaským odposlouchávacím systémem, který prověřuje provoz na internetu.

Echelon zachycuje denně na 3 miliardy zpráv z družic včetně telefonních a internetových, obojí představuje asi 90 % údajů. Přes tři čtvrtiny zachycených informací se předává do centrály NSA ve Fort Meade. Tam je okamžitě třídí obrovské počítače, přezdívané Dictionary (Slovníky), podle klíčových slov a adres. Programy na rozlišení hlasů Voicecast zase umožňují identifikovat vybrané hlasy, a tím mimo jiné sledovat pohyby jejich majitelů. Počítače, které patří k nejmohutnějším na světě, dokáží rovněž rozlousknout většinu cizích kódů.[15]

Evropská unie se připravuje bezprecedentně varovat své občany před hrozbou jejich soukromí, kterou zosobňuje vysoce kontroverzní globální odposlouchávací síť

[14] *Metody špionáže: Průmyslová špionáž* [online]. Specialista.info, 2006 [cit. 2011-11-04]. Dostupné z WWW: <http://www.magazin.specialista.info/view.php?cisloclanku=2006013001>.
[15] PACNER, K. *Kosmičtí špioni.* 1. vyd. Praha : Albatros, 2005. s. 104. ISBN 80-00-01686-9.

Echelon, provozovaná především americkou a britskou špionážní službou, napsal v sobotu 26. května 2001 deník Guardian.

V dosud nezveřejněném dokumentu Evropského parlamentu naléhá tato instituce na jednotlivce i na podniky, aby při elektronické komunikaci prostřednictví e-mailu i faxů používali šifrovací systémy na ochranu před jejich odposlouchávání. Poslanci Evropského parlamentu totiž shromáždili přesvědčivé důkazy, že anglosaské špionážní služby odposlouchávají veškerý e-mailový a internetový provoz prostřednictvím sítě Echelon.

Tento pracovní dokument poslanců Evropského parlamentu bude tvořit podstatu zprávy z dočasného parlamentního výboru pro síť Echelon, která má být zveřejněna. Dokument dochází k závěru, že prvotním účelem tohoto integrovaného systému špionážních satelitů a odposlouchávacích zařízení je „odposlouchávat soukromé a komerční komunikace a nikoliv vojenský provoz“. Tento dokument, který je důsledkem prvního vyšetřování na vysoké úrovni systému Echelon, je publikován po mnoha letech rostoucího znepokojení ohledně využívání této špionážní sítě. I když je existence systému Echelon známa už od šedesátých let, žádná vláda dosud oficiálně nepřiznala, že se na práci tohoto systému podílí.

Připravovaná zpráva poslanců Evropského parlamentu přichází shodou okolností ve stejnou dobu jako varování, že by se Echelon mohl stát novou kybernetickou „tajnou policií“. V nové knize Body Secrets o americkém Národním úřadu pro bezpečnost a jeho stycích s britským střediskem pro odposlouchávání v Cheltenhamu GCHQ, varuje James Bamford, který je považován za čelnou autoritu na Národní úřad pro bezpečnost: „Skutečným problémem je to, zda Echelon nyní likviduje individuální právo na soukromí, což je základním lidským právem.“

Systém Echelon provozují Spojené státy, Velká Británie, Kanada, Austrálie a Nový Zéland. Echelon vznikl za účelem shromažďování špionážních informací za studené války. V posledních letech jeho jedinečné globální odposlouchávací schopnosti vyvolávají obvinění, že je Echelon zneužíván k získávání soukromých a důvěrných obchodních sdělení.

Vyšetřování poslanců Evropského parlamentu vyvolala tvrzení, že prý Spojené státy využily Echelonu ke krádeži důvěrných informací od svých evropských konkurentů. Z dokumentu Evropského parlamentu však vyplývá, že poslanci nenašli žádné důkazy o tom, že by byl systém Echelon systematicky využíván pro průmyslovou špionáž.

Dokument Evropského parlamentu nepřímo varuje Velkou Británii, jedinou členskou zemi Evropské unie, která se podílí na systému Echelon, že stát, který se podílí na elektronickém odposlouchávání občanů Evropské unie a podniků v Evropské unii, porušuje Evropskou konvenci o lidských právech i zákon Evropské unie.

Poslanci Evropského parlamentu charakterizovali jako „neuspokojivou a politováníhodnou" absenci demokratického dohledu nad tajnými službami v několika členských zemích a naléhali na Evropskou unii, aby zajistila, že bude šifrovací software lehce přístupný pro jednotlivce i pro podniky, aby si mohli chránit své komunikace.

Neil Mac Cormick, náměstek předsedy britského parlamentního výboru pro Echelon za Skotskou nacionalistickou stranu, konstatoval: „Lidé by měli považovat e-mail za totéž jako pohlednice z dovolené. To znamená, že si na ně mohou napsat, co chtějí, ale nesmějí být překvapeni, když si to někdo přečte."

Někteří aktivisté za právo na soukromí namítají, že zpráva poslanců Evropského parlamentu nezachází dost daleko. Naléhají na výbor Evropského parlamentu, aby začal vyšetřovat nové odposlouchávací systémy, které mají odstranit dosavadní neefektivnost systému Echelon. Varují také, že šifrovací systémy, které jsou komerčně k dispozici, dokáží špionážní služby bez problémů dešifrovat. Dokument Evropského parlamentu se nyní studuje na britském ministerstvu zahraničních věcí a na britském ministerstvu vnitra.

„Národní bezpečnost kontra individuální lidská práva, to je složité téma," konstatoval jeden činitelé britské vlády, který zná zprávu Evropského parlamentu.

Britská vláda popírá, že je Echelon využíván pro průmyslovou špionáž, ale přiznává, že jedním z cílů tohoto systému je „znemožňovat průmyslovou špionáž, kterou provádějí jiní."[16]

Dříve byla špionům z francouzské *Direction Générale de la Sécurité Extérieure* (dále DGSE) nápomocna i státní firma Air France. Kanadské a americké tajné služby v roce 1992 nabádaly obchodníky, aby s touto společností nelétali; ukázalo se totiž, že v sedadlech první třídy jsou na interkontinentálních letech namontovány štěnice. A bývalý ředitel CIA Robert Gates řekl: „Francouzi nasazují agenty na zahraniční firmy, kradou aktovky amerických obchodníků, v letadlech Air France instalují do

[16] *Evropská unie varuje před anglosaským odposlouchávacím systémem, který prověřuje provoz na internetu* [online]. Britskelisty, 2001 [cit. 2011-08-11]. Dostupné z WWW: <http://www.britskelisty.cz/0105/20010528d.html>.

sedadel první třídy štěnice a užívají i dalších metod klasické špionáže, jen aby se dostali k ekonomickým informacím.“[17]

2.4 Škody způsobené průmyslovou špionáží

Vedle politické špionáže měla zejména v bipolárně rozděleném světě velký význam i hospodářská špionáž. Důvod k tomu byl velice jednoduchý. Průmyslová výroba na vysoké úrovni vyžaduje obrovské miliardové náklady na vývoj, nepočítaje v to objem času a nároky na personál. Špionáž naproti tomu vede ke stejnému cíli, je však přitom nesrovnatelně levnější.[18]

Jen v samotném Německu jsou hospodářské škody, způsobené na základě průmyslové špionáže, experty odhadovány na více než 20 miliardy Euro za rok.[19]

„*Na základě zjištění průzkumu společnost McAfee odhaduje, že škody způsobené ztrátou dat dosáhly v celosvětovém měřítku v roce 2008 výše 1 bilionu dolarů. Jedná se přitom o konzervativní dohad*,“ uvádí prezident a výkonný ředitel společnosti McAfee Dave DeWalt.[20]

Rozvíjející se země jsou k ochraně duševního vlastnictví více motivovány a vynakládají na ochranu více prostředků než vyspělé státy. Firmy z Brazílie, Číny a Indie utrácejí za zabezpečení více peněz než ty z Německa, Velké Británie, USA a Japonska. Společnost McAfee zveřejnila výsledky studie *Unsecured Economies: Protecting Vital Information*.

Studie podniknutá mezi CIO (Chief Information Officers) v 6 zemích se soustředila na koloběh klíčových informací: kde duševní vlastnictví vzniká, kde jsou tyto informace celosvětově uchovávány, jak se dále přenášejí a jak dochází k jejich ztrátám a únikům. Společnosti, které se účastnily průzkumu, odhadují, že celkem utrpěly pouze v loňském roce ztráty duševního vlastnictví v hodnotě 4,6 miliard USD

---

[17] ULFKOTTE, U. *Válka v temnotách : skutečná moc tajných služeb.* 1. vyd. Praha : Ikar, 2007. s. 286. ISBN 978-80-249-0959-2.
[18] PIEKALKIEWICZ, J. *Historie světové špionáže : agenti, systémy, akce*. 1. vyd. Praha : Naše vojsko, 2004. s. 13. ISBN 80-206-0738-2.
[19] WEYERSTALL, N. *Schutz vor Folgen der Industriespionage: Informationen auf Abwegen* [online]. Sicherheit.info, 2008 [cit. 2011-08-12]. Dostupné z WWW: <http://www.sicherheit.info/SI/cms.nsf/si.ArticlesByDocID/2101215?Open&SessionID=2559532-140656>.
[20] *McAfee Unsecured Economies Report* [online]. Resources.mcafee.com, 2009 [cit. 2011-10-12]. Dostupné z WWW: <http://resources.mcafee.com/content/NAUnsecuredEconomiesReport>.

a byly nuceny utratit asi 600 milionů dolarů za likvidaci škod vzniklých z narušení dat.[21]

Už v roce 2009 zveřejnila americká Purdue University unikátní studii, podle níž v důsledku krádeží duševního vlastnictví utrpěly firmy po celém světě škody v hodnotě více než bilionu dolarů během jediného roku 2008. Poradenská společnost PricewaterhouseCoopers odhaduje, že celá polovina hospodářské kriminality ve stejném roce padá na konto samotných zaměstnanců firem, kteří ve snaze si přivydělat či zvýšit svou cenu na trhu práce často kromě běžných krádeží vynášeli i citlivá firemní data s vidinou jejich zpeněžení.[22]

Autor práce uvádí, že vzniklou škodu způsobenou průmyslovou špionáží lze však jen velmi obtížně vyčíslit. Převod škody na přesnou finanční hodnotu úniku znalostí nebo technologií lze vyjádřit pouze určitou hodnotou, kterou představuje zejména pro jejího vlastníka nebo uživatele. Stejně tak i následně vzniklá či hrozící škoda se může skládat z mnoha dalších různých položek. Například také ze škody, která vznikla nebo i jen hrozila potenciálním neuzavřením kontraktu. V těchto případech je vyčíslení vzniklé škody velmi obtížné a může se mnohdy pohybovat na samé hranici spekulace. Vzhledem k neexistenci téměř jakékoliv známé metodiky je každý pokus o vyčíslení nákladů škody prakticky jako kladení základních kamenů této problematiky. Při stanovení reálné hodnoty úniku know-how pro vlastníka se soudní znalci pohybují v oblasti, která není ani v současnosti dostatečně probádaná a zmapovaná.

2.5 Šedá ekonomika v oblasti průmyslové špionáže

Čísla šedé ekonomiky se skládají ze zastíraných činností, které obsahují jak legální část výroby, tak i nelegální produkci zboží a poskytování služeb. Nepochybně k jedné z mnoha zastíraných činností patří i průmyslová špionáž.

Přední ekonomové nedávno oznámili, že čínská šedá ekonomika neboli příjmy získané neoficiálními podnikatelskými praktikami a z pochybných a často nelegálních zdrojů, by mohla představovat až třicet procent HDP země.

Wang Xiaolu, místoředitel Národního ekonomického ústavu pro výzkum v Pekingu, a jeho tým publikovali začátkem července výzkum o šedé ekonomice v Číně,

---

[21] *McAfee Unsecured Economies Report* [online]. Resources.mcafee.com, 2009 [cit. 2011-10-12]. Dostupné z WWW: <http://resources.mcafee.com/content/NAUnsecuredEconomiesReport>.

[22] *Špioni v továrnách* [online]. Probin.cz, 2011 [cit. 2011-11-02]. Dostupné z WWW: <http://www.probin.cz/cz/37.spioni-v-tovarnach>.

který ukazuje, že nečisté příjmy horních dvaceti procent občanů tvoří více než osmdesát procent celkových „šedých příjmů“ v Číně.

Průzkum odhalil, že šedé příjmy městské populace (které nejsou zahrnuty v žádné oficiální statistice) činily v roce 2008 9,26 trilionů yuanů (téměř 26 trilionů Kč), což je ekvivalent přibližně třiceti procent čínského HDP z daného roku.

Wang a jeho tým také zjistili, že hlášené roční platy funkcionářů Komunistické strany Číny (KS Číny) nejsou nijak vysoké, ale suma jejich šedých příjmů může být daleko větší. Tyto nekalé výdělky samozřejmě nepodléhají daním a mohou pocházet z různých zdrojů, např. úplatky, zpronevěra veřejných fondů, laskavosti od podniků apod.[23]

Podle zprávy v tisku „obchodní obrat“ průmyslové špionáže ve Spojených státech dosahuje částky kolem jedné miliardy dolarů ročně, přičemž na veškerý vědecký výzkum připadají zhruba dvacet dvě miliardy.

Pokud jde o průmyslovou protišpionáž, zvýšily se například zisky Pinkertonovy agentury z pěti miliónů dolarů v roce 1949 na 43 milióny dolarů v roce 1963. Z celkového počtu pěti set největších amerických společností jsou plné čtyři stovky stálými zákazníky Pinkertonovy agentury.

Průmyslová špionáž tedy rozhodně stojí za to, abychom se jí zabývali.[24]

[23] *Šedá ekonomika v Číně roste rychleji než HDP* [online]. Velká Epocha, 2010 [cit. 2011-11-14]. Dostupné z WWW: <http://www.velkaepocha.sk/2010091614566/Bujici-seda-ekonomika-v-Cine.html>.
[24] BERGIER, J. *Průmyslová špionáž.* 1. vyd. Praha : Orbis, 1974. s. 11-12. ISBN 605-22-826.

3 Historie průmyslové špionáže

Získávání nových technologií patřilo a patří nadále k nejdůležitějším úkolům tajných služeb. Zpravodajská činnost byla již v dávných dobách nezbytná pro vojenské operace, ovšem teprve během industrializace se staly předmětem průmyslové špionážní činnosti jako takové. Krádeže technologií a postupů jsou známé již od starověku. Získat všemožná výrobní tajemství se lidé pokoušeli už od prehistorických dob. Dokáži si představit, jak již v prehistorické době, kdy první kmeny Homo sapiens objevily tajemství ohně, mohly být tyto kmeny předmětem první „průmyslové špionáže" ze strany méně úspěšných kmenů.

„Byla jednou jedna krásná princezna a jedno velké tajemství…" Tak by mohla docela dobře začínat pohádka z „Tisíce a jedné noci". Jde však o příběh skutečný, zapsaný ve starých čínských letopisech.

Tím tajemstvím byla výroba hedvábí. (Evropané nemohli a nechtěli uvěřit, že je hedvábí produktem housenek, a proto se pídili po způsobu výroby hedvábného vlákna.) Jednou se ona krásná princezna vypravila na cestu do ciziny. Na hlavu si posadila nádherný klobouk s čerstvými květinami – a v nich ukryla larvy bource morušového, které pak odevzdala svému indickému milenci. Takovým způsobem se dostalo hedvábí za hranice Číny. Je to úplně klasický případ průmyslové špionáže, který se udál zhruba tisíc let před začátkem našeho letopočtu.[25]

Vyzvědače, či chcete-li tajné agenty, používali už egyptští faraónové, sloužili Alexandrovi Makedonskému při jeho tažení do Persie a Indie a samozřejmě i římským císařům.

Starověk a středověk už znaly také průmyslovou špionáž. Například Arabové usilovali o získání výrobního tajemství tzv. řeckého ohně, kterým Řekové zapalovali nepřátelské lodě při obraně Konstantinopole. Skutečně se jim podařilo ukrást jeho recepturu a později „řecký oheň" s úspěchem použili i při válkách s křižáky. Arabové byli vůbec velmi zdatní průmysloví špioni. Od Číňanů tajně získali návod na střelný prach a rakety, kterým příznačně říkali „čínské šípy". A zřejmě právě Arabům pak ve 14. století „vyfoukl" výrobní tajemství střelného prachu benediktinský mnich

[25] BERGIER, J. *Průmyslová špionáž.* 1. vyd. Praha : Orbis, 1974. s. 23. ISBN 605-22-826.

a alchymista Berthold Schwarz, který je podle legendy považován za jeho evropského vynálezce.

Když už jsme se zmínili o alchymii, právě tento záhadami obestřený obor je považován za krycí profesi mnoha středověkých špionů. Na pražském dvoře císaře Rudolfa II. se například pohybovali vyhlášení angličtí alchymisté a okultisté John Dee a Edward Kelley, patrně agenti královny Alžběty. Ne náhodou vypověděl císař prvního z nich ze země a druhý nakonec po mnoha peripetiích zemřel ve vězení hradu v Mostě. Vedle nich působil tehdy v rudolfínské Praze nenápadný manžel půvabné anglické básnířky Vestonie, jistý Jan Lew, vystupující jako rada anhaltského knížete Kristiána. O jeho skutečné činnosti svědčí dochované šifrované zprávy, které z Čech posílal svému zaměstnavateli. Lew v Praze zůstal i po smrti císaře Rudolfa a zdá se, že měl prsty v přípravě stavovského povstání. V letech 1617 a 1618 se v jeho nepříliš složitě šifrovaných zprávách stále častěji objevují poznámky o „pohledávkách husitů". Nemusíme být příliš důvtipní, abychom pochopili, že se jednalo o protestantské šlechtice. A určitě ne náhodou byl v bitvě na Bílé hoře právě Lewův zaměstnavatel Kristián z Anhaltu vrchním velitelem vojsk „zimního" krále Fridricha Falckého.

Tajným agentem ve službách Francie byl i rodilý Benátčan a rokokový dobrodruh a svůdce Giacomo Casanova. V té době se prakticky překrývala diplomacie a špionáž, což v jistých ohledech platí vlastně dodnes. Husarský kousek se podařil například Klemensi Metternichovi v době, kdy byl rakouským vyslancem na dvoře francouzského císaře Napoleona. V roce 1807 se od své milenky a Napoleonovy sestry, neapolské královny Karoliny Muratové, dozvěděl, že se Napoleon hodlá rozvést se svou manželkou Josefinou a zajímá se o sestru ruského cara Alexandra I. Proto rychle předešel váhající Rusy a zajistil své zemi důstojný mír tím, že zprostředkoval Napoleonův sňatek s dcerou rakouského císaře Marií Louisou.[26]

3.1 První případy průmyslové špionáže

Špionáž pracovních postupů mohla být problémem již v raném věku. Existují důkazy, jak ukazuje klasický příklad přísně střeženého tajemství výroby hedvábí, že se neustále podnikaly pokusy o nasazení špionů s cílem odhalit tajemství vynálezů. Tak to

[26] BAUER, J. *Tajnosti tajných služeb* [online]. 21 století.cz, 2003 [cit. 2011-08-11]. ISSN 0040-1064. Dostupné z WWW: <http://www.21stoleti.cz/view.php?cisloclanku=2003091828>.

bylo např. s porcelánem, prvním parním strojem, první továrnou na kontinentě nebo s kaučukem a s dalšími milníky na cestě průmyslové špionáže.

3.1.1 Porcelán

Případ je specifický osobou špiona, francouzského jezuitského pátera d'Entrecolesa, misionáře a špiona v jedné osobě, jak již počátkem osmnáctého století dokázal velmi podrobně a komplexně předávat průmyslové informace z Číny.

V nejdelší tajné válce, kterou vedli nejnápaditější špioni již staletí, šlo o tajemství výroby porcelánu, nazývaného též „bílé zlato". Číňané vyráběli porcelán pravděpodobně již v 7. století. V Evropě se několik kusů porcelánu objevilo teprve koncem 13. století. V pozdějších staletích zdobil nádherný porcelán stůl každého monarchy, ale nikdo nevěděl, jak se vyrábí. Toto tajemství se Číňané pokoušeli obestřít mýty a legendami. Vyprávělo se, porcelánová masa se nachází kdesi na posvátném místě pod zemí, kde ji střeží démoni. Na podnět bohů se pak pod horskými paprsky slunce mění v porcelán. Čínský porcelán měl po staletí v Evropě mimořádně vysokou cenu. Jeho složení bylo i pro evropské učence záhadou. Někteří ve vší vážnosti tvrdili: „určitou masu složenou ze sádry, želvích vajec, skořápek ústřic a podobných substancí prohněte otec rodiny, tajně ji zakope v zemi a tajemství svěří pouze svým dětem. Hmota se pak nechá 80 let uležet, aniž by spatřila světlo světa. Pak ji potomci vykopou…"

V některých kronikách se uvádí, že Japonci tajemství výroby porcelánu znali již v době kolem narození Krista – dozvěděli se je při své cestě Koreou. Avšak titíž kronikáři se zmiňují o japonských řemeslnících v 17. století, kteří cestovali do Číny, aby se zde dopátrali tajemství výroby pravého, ušlechtilého porcelánu. Poté, co portugalští kupci roku 1543 poprvé vstoupili na japonskou půdu, ovládli postupně veškerý export tamějšího porcelánu. V té době nebylo tajemství výroby porcelánu v Evropě známo. Teprve v 18. století se jednomu špionovi podařilo celý postup odhalit. Byl to francouzský jezuitský páter d'Entrecoles, misionář v Číně. Jednoho dne navštívil „tajné město" King-tö-čen, sídlo císařské manufaktury na porcelán. Tam žilo, podle jeho údajů, na tehdejší dobu nepředstavitelné množství dělníků – přes milion lidí. Již ve svém prvním dopise, který došel do Paříže v září 1712, páter d'Entrecoles velmi živě líčil své dojmy z „tajného města": „Hlavní město porcelánu leží, obklopeno vysokými

kopci, na rovině provincie Ťiang-si. Protékají zde řeky. Na větší z nich je přístav o délce více než jedné míle. Někdy jsou zde vidět lodě, seřazené do dvou až tří řad za sebou…[27]

Ve dne v noci hoří 3 000 pecí. Nejsou zde žádné městské hradby a tak se město rozpíná na všechny strany. Ulehčuje to také dopravu surovina hotových výrobků z lodí do dílen a opačně. Při veškerém obyvatelstvu, které čítá přibližně milión duší, můžeme napočítat 18 000 hrnčířských rodin. Denně se spotřebuje 10 000 tun obilí a 1 000 prasat, o koňském a psím ani nemluvě…“ King-tö-čen je vystavěno v pravidelných tvarech. Ulice se protínají v pravém úhlu a vedou podél bloků domů stejné velikosti. Bohatí kupci bydlí v luxusních obydlích, město však obklopuje i velké množství chudých rodin. Děti, invalidé, slepci a nemocní jsou zaměstnáni, aby si drcením barev vydělali na živobytí. Městu vládne mandarín s pomocí spolehlivých policistů. Každou ulici má na starosti správce, jemuž je na každých deset domů k dispozici úředník. V noci se zřizují střežené zábrany, které čas od času kontroluje sám mandarín.

Cizinci nesmějí ve městě bydlet. Zůstávají buď na svých lodích, nebo jsou ubytování u známých, kteří za ně musí ručit. Aktivity a bohatství města se dotýkají jen a jen obchodu porcelánem. V dílnách se pracuje systémem pásové výroby. Každá keramika projde asi 60 rukama.

Páter d’Entrecolles zde pozoroval výrobu porcelánu velmi pozorně a vše si přesně zaznamenával. Jeho zprávy pravidelně docházely do Francie. I přes nedůvěru a zvláštní pozornost úřadů se mu dokonce podařilo zaslat do vlasti kaolín. Evropanům však k výrobě materiálu, podobného čínskému porcelánu, chyběla právě tato důležitá součást, kaolín, sestávající z jílových minerálů, živce, granitu a pegmatitu.

Za objevení kaolinu v Evropě můžeme poděkovat náhodě. Okolo roku 1700 přišel jeden mistr kovář ve Vogtlandu na nápad, použít bílé, vyschlé bahno z aueského údolí namísto mouky k pudrování paruk. V roce 1707 se lékárník J. F. Böttger spolu s fyzikem E. von Tschirnhaussenem rozhodli použít tento materiál jako plastickou hlínu. V Evropě tak poprvé vznikl pravý tvrdý porcelán, obsahující kaolín, který Číňanům po staletí záviděl celý svět. Tenkrát bylo tajemství přísně střeženo, Böttgerova laboratoř byla opravdovou pevností a dělníkům hrozilo doživotní vězení, jestliže někomu prozradí sebemenší detail. Avšak mazaného špiona nemohou odradit žádné zákazy ani bezpečnostní opatření. O devět let později byl porcelán vyroben i ve Vídni, následně francouzské tajemství vyzvěděli Angličané a zahájili výrobu porcelánu. Muž

[27] PIEKALKIEWICZ, J. *Historie světové špionáže : agenti - systémy - akce*. 1. vyd. Praha : Naše vojsko, 2004. s. 180-182. ISBN 80-206-0738-2.

jménem William Cookworthy si v Londýně přihlásil patent k postupu výroby porcelánu a díky svým dobrým stykům získal monopol pro jeho výrobu a dovoz suroviny. V té době bylo v Anglii běžné, že si průmyslníci obstarali nejnovější technické postupy špionáží a ty si pak zabezpečili monopolními privilegii. Těmto praktikám poprvé učinilo přítrž odstranění monopolu na porcelán v roce 1796. V tomto roce založilo několik občanů v Manchesteru a Liverpoolu „Protimonopolní a protipatentní sdružení". Byla to první organizace světa, která vyhlásila otevřený boj průmyslové špionáži.[28]

3.1.2 Parní stroj

Případ je jedním z prvních, kdy prostřednictvím průmyslové špionáže dokázal úspěšný špion získat značnou konkurenční výhodu a využil ji k v soukromém podnikání ke značným ziskům.

Anglickému kováři Thomasi Newcomenovi se v roce 1716 podařilo zkonstruovat první tzv. ohnivý stroj, jak se tenkrát říkalo atmosférickému parnímu stroji. Tento stroj, vynalezený k odčerpávání vody z důlních šachet, samozřejmě přilákal do Velké Británie velké množství špionů. Prvním člověkem na kontinentě, který odhalil tajemství této konstrukce a vbrzku vyrobil věrnou kopii, byl Joseph Emanuel Fischer von Erlach. Dodnes sice stojí ve stínu svého slavnějšího otce Johana Bernarda, stavitele Schönbrunnu a Karlskirche, i on však patří k největším rakouským stavitelům.

Joseph Emanuel se narodil 13. září 1693 v dunajské metropoli. Již časně ho otec připravoval na povolání stavitele a v mladém věku již návrhy překresloval načisto. Roku 1713 získal dvacetiletý Joseph Emanuel císařské stipendium, studoval na univerzitě v holandském Leydenu a v roce 1720 odešel na rok do Anglie. Právě v té době se ve Vídni zabývali myšlenkou odvodnění uherských dolů, které bylo stále naléhavějším problémem. Zvláštní zájem poutaly v Anglii Newcomenem zkonstruované parní stroje, úspěšně používané na dolech v Birminghamu. Fischer vícekrát navštívil dílny u Birminghamu a maskován za dělníka získal rozměry, podle nichž zhotovil skici. Špionáž budoucího inženýra se vyplatila. Když se mladý muž roku 1722 vrátil zpět do Vídně, neznal pouze anglický stroj, ale vymyslel sám „různé užitečné vynálezy".

Z těchto nabytých vědomostí začal Fischer „vytloukat" kapitál. Zabýval se stavbou prvního atmosférického parního stroje na evropském kontinentě, který byl již

[28] PIEKALKIEWICZ, J. *Historie světové špionáže : agenti - systémy - akce*. 1. vyd. Praha : Naše vojsko, 2004. s. 180-182. ISBN 80-206-0738-2.

v roce 1722 nasazen na dole Althandl v Horních Uhrách (dnešní Nová Baňa na jižním Slovensku). V témže roce se Joseph Emanuel Fischer von Erlach osvědčil jako inženýr ve službách knížete Schwarzenberga ve Vídni: „Pan Fischer von Erlach konečně dohotovil ohnivý stroj v knížecí schwarzenberské zahradě, aby mohla být voda padající z rezervoárů do fontán pumpována zpět," poznamenal o deset let později kronikář Küchelbecker. Stroj byl spuštěn v roce 1723 a vyvolal obrovskou pozornost.

Počátkem roku 1732 odcestoval nyní již velice zaměstnaný Fischer von Erlach opět do Uher a uzavřel zde 8. července 1732 velice lukrativní smlouvu s dvorní komorou na dva parní stroje pro dílo v Banské Štiavnici, kde se dolovalo zlato a stříbro. V lednu 1934 je první parní stroj připraven k provozu. Ještě v červenci téhož roku uzavřel kontrakt na další stroje a objednávky se jen hrnuly. Fischer byl ve všech projektech vlastním konstruktérem, vedoucím inženýrem a současně samostatným podnikatelem, což mu přinášelo obrovské zisky. A ještě více. Po dokončení nejdůležitějších prací dal úspěšný špion roku 1735 dvoru najevo, že by jeho „užitečné služby" mohly být odměněny baronským titulem.

První model „ohnivého stroje" Josepha Emanuela Fischera von Erlach je vystaven v technickém muzeu ve Vídni společně s náčrty asi nejstaršího parního stroje na kontinentě. Ještě dnes jsou důkazem průkopnické činnosti na poli průmyslové špionáže.[29]

3.1.3 Kaučuk

Specifikum tohoto případu je v jeho souvislostech, kdy i přes patentovou ochranu došlo k prolomení technologie, což mělo za následek její dynamický rozvoj a nárůst spotřeby cenné suroviny. Je asi i jedním z případů zcizení zdroje přírodní průmyslové suroviny. Zajímavý je i tím, že za své činy byl úspěšný hospodářský špion povýšen do šlechtického stavu.

Ve druhé polovině 19. století se Brazílie stala dějištěm jednoho z nejpozoruhodnějších případů na poli průmyslové špionáže. Země na Amazonce platila za největšího vývozce kaučuku, nazývaného také „plačící dřevo". Již v roce 1734 se podařilo dopravit do Anglie první vzorek, ale nikdo nevěděl co si s ním počít. Jednoho dne pak kdosi objevil, že třením (to Rub) kousku této gumy se mohou odstraňovat

[29] PIEKALKIEWICZ, J. *Historie světové špionáže : agenti, systémy, akce*. 1. vyd. Praha : Naše vojsko, 2004. s. 183. ISBN 80-206-0738-2.

z papíru čáry, provedené tužkou, odtud označení „Rubber“. První patent na kaučuk ohlásil v květnu 1791 Angličan Samuel Peal a dlouho poté o tom nebylo nic slyšet. Teprve v roce 1845 si nechal patentovat nový způsob zpracování kaučuku, vulkanizaci, Američan Charles Goodyear. Tato náhodně objevená metoda tvořila vlastní základ kaučukového průmyslu. Goodyear podnikal všechno možné pro utajení svého postupu, protože špioni konkurence nezůstávali nečinní. To rozpoutalo lavinu procesů. Když se Goodyearovi podařilo prodloužit patent o 7 let, mělo to pro něj pouze symbolickou hodnotu. Když v roce 1860 zemřel, zanechal po sobě dluhy ve výši půl miliónu dolarů, na tehdejší dobu horentní sumu.

Kaučukový průmysl se velmi brzy stal prvořadým cílem průmyslových špionů. I přes všechna ochranná opatření vynalézali stále nové a nové triky, aby se jim podařilo získat tajné podklady pro vulkanizaci, použití plnidel a tvářecí gumy.

Obrovským rozvojem kaučukářského průmyslu vzrostly nároky na zásobování surovinou, a tím Brazílii, jedinému vývozci tohoto materiálu, nastaly zlaté časy. Brazilci, lpící na svém monopolu, viděli v každém cizinci potenciálního hospodářského špiona, který by se mohl pokusit vyvézt semena kaučukovníku ze země a založit někde jinde plantáže pro pěstování tohoto „plačícího dřeva“. To se skutečně v roce 1876 podařilo britskému dobrodruhovi Henrymu Wickhamovi. Procestoval povodí Amazonky a prozkoumal v té době téměř neprozkoumanou náhorní plošinu Tapajos, „Terra prohibitiva“ – zakázanou zemi, kde v džungli získal semena kaučukovníku.

Wickhamovi se podařilo nalodit se svými semeny, aniž by vzbudil větší podezření u přístavní policie. Když byl dotazován na obsah svých zavazadel, řekl, že semena pocházejí ze vzácného stromu a nakoupil je pro londýnskou botanickou zahradu. V Londýně pak nechal zasít okolo 7000 semen, která všechna vzešla a následně vzrostlé sazenice byly dopraveny do anglických kolonií Cejlonu, Indie a Malajsie a zde vysázeny. Kaučukovník se zde aklimatizoval bez větších problémů a plantáže se staly nejdůležitějším zdrojem příjmů těchto zemí. Již po několika letech mohl tento region exportovat okolo 3 miliónů tun gumy ročně.

Henryho Wickhama za jeho činy povýšila královna Viktorie do šlechtického stavu. Je to asi první vyznamenání tohoto druhu pro hospodářského špiona.[30]

[30] PIEKALKIEWICZ, J. *Historie světové špionáže : agenti, systémy, akce*. 1. vyd. Praha : Naše vojsko, 2004. s. 186-187. ISBN 80-206-0738-2.

3.1.4 Pneumatiky

Také v tehdejším Československu na „poli“ průmyslové špionáže aktivně působila československá vědeckotechnická rozvědka.

Podle PACNERA[31] československá vědeckotechnická rozvědka získala v letech 1970 až 1989 celkem 9 310 materiálů, z toho 7 procent dostalo hodnocení nejvyššími známkami 1-2. Třetina těchto materiálů putovala do továren, pětina vojenskému výzkumu a výrobě, ostatní potravinářskému průmyslu, školství a základnímu výzkumu.

SOBEK[32] ve své knize uvádí: „Počátkem šedesátých let naše motoristická veřejnost zaregistrovala podstatné zvýšení kvality pneumatik Barum. Pro osvěžení paměti připomeňme, že značka Barum vznikla spojením tří československých výrobců pneumatik: Baťa, Rubena, Matador. Vědeckotechnické rozvědce se totiž podařilo získat od předního světového výrobce novou technologii jejich výroby. Po najetí výroby syntetického kaučuku v Kralupech se u nás výroba pneumatik v Otrokovicích i v tehdejším Gottwaldově (dnes Zlíně) rozběhla naplno. Pneumatiky Barum se počaly úspěšně uplatňovat i na zahraničním trhu a s ohledem na jejich cenu i kvalitu šla dobře na odbyt.“

[31] PACNER, K. *Československo ve zvláštních službách : pohledy do historie československých výzvědných služeb 1914-1989. Díl IV., 1961-1989.* 1. vyd. Praha : Themis, 2002. s. 643. ISBN 80-7312-013-5.
[32] SOBEK, V. *Pomohli jsme sestřelit Powerse : tajemství Vědeckotechnické rozvědky ČSSR.* 1. vyd. Praha : Futura, 2011. s. 36. ISBN 978-80-86844-67-1.

4 Sdílení informací, koloběh dat v globalizovaném světě

Potřeba a důležitost aktuální informace se vyžaduje ve všech oborech byznysu a managementu. V koloběhu informací není problém data shromažďovat a uchovávat, ale vhodně je organizovat a třídit vhodným způsobem, aby byla připravena okamžitě a snadným způsobem k dispozici. Pokud jde o data v počítačích, je známým jevem, že objem dat se každé dva roky více než zdvojnásobí.

Svět je uprostřed informační revoluce, o níž mnozí tvrdí, že bude mít podobně dalekosáhlý dopad na politiku, ekonomiku a kulturu, jako kdysi měla průmyslové revoluce. Rozhodně ovlivňuje způsob, jak spolu státy a další mezinárodní aktéři ekonomicky soupeří, a to včetně špionáže na poli světové konkurence.

V květnu roku 1996 Raymond Kendal, britský generální tajemník Interpolu, řekl: *„Studená válka skončila. Roli největšího nepřítele státu převzal organizovaný zločin. Evropa je nyní jednou obrovskou kriminální scénou, sahající od Atlantiku až po Ural. Jen při dokonalém využití informací lze zločin zlikvidovat již v samém zárodku.“*[33]

Podle JIRÁSKA[34] by se informatika stěží rozvíjela tak dynamicky, kdyby k tomu nebyly ekonomické důvody. Prosadila se rychlostí, hromadností, ukládáním, tříděním a vybavováním dat a informací. V tom je nedostižitelná a má před sebou otevřenou budoucnost.

4.1 Zdroje průmyslové špionáže

Přestože lze řadu „odborných“ poznatků získat z veřejných zdrojů, je nasazení špionů pro tajné získávání informací i nadále nezbytné. Pracovníci tajné služby mají jedno společné, a sice vědomí, jak je jejich činnost důležitá. Nicméně ke snížení rizika prozrazení tajemství je potřebné každou zpravodajskou službu rozdělit do několika samostatných rezortů, takže se každý setkává pouze s informacemi, které potřebuje bezpodmínečně znát ke splnění svého úkolu.

---

[33] SMITH, M. *Britské tajné služby.* 1. vyd. Praha : Ivo Železný, 1998. s. 266. ISBN 80-237-3556-X.
[34] JIRÁSEK, J. *Agenda příštích let.* 1. vyd. Praha : Professional Publishing, 2006. s. 110. ISBN 80-86946-04-5.

To že jen dobře organizovaná tajná služba může něčeho dosáhnout, potvrzují slova bývalého šéfa CIA McConeho: „Všechny války našeho století, i I. světová, vznikly na základě chybného zhodnocení situace, na základě nedostatečných a špatně vyhodnocených informací.“[35]

Podle SOBKA[36] nebylo nikdy lehké získat informace nebo dokumentaci, avšak práce pouhým získáním nekončila. Zajistit jejich využití také nebylo lehké, někdy to bylo dokonce těžší. Získané informace se zhodnotí teprve tím, že se dostanou na pracoviště, která je mohou využít. Čím je dokumentace cennější, tím větší je nebezpečí, že se prozradí její původ a bude ohrožen zdroj, který ji poskytl. Není-li informace využita, stává se bezcennou a úsilí vynaložené k jejímu získání je ztraceno. Bezpečnost zdroje je v rozvědkách základním zákonem.

4.1.1 Legální zdroje informací

Co je legálním profesním odvětvím nazývaným strategický marketing a co je nelegální činností, nazývanou krádeží informací, zneužitím informací v obchodním styku, až špionáží? Kde je hranice strategického marketingu a špionáže? Existují nějaká oficiální technická nebo etická kritéria pro její určení? Tyto otázky si určitě občas položí každý člověk, který ve svém profesním zaměření zastává odpovědnou pracovní funkci a řeší problémy, o kterých nemá s nepovolanými osobami mluvit.

Lidé i sdělovací prostředky jsou zvyklé nazývat špionáží to, co se týká informací ve vztahu ke státním zájmům. V případě komerčních organizací se obvykle hovoří o zneužití informací v obchodním styku, vytunelování know-how nějaké firmy a podobně. Jde však v podstatě o totéž, pouze vlastník a cílená informační aktiva jsou rozdílná. A pokud se omezíme na technický rozvoj, ekonomiku nebo chování nadnárodních globálně působících společností, pak zde se smazávají i poslední rozdíly.

Stát může pro svoje účely zlegalizovat použití technických prostředků pro napadání cizích informačních systémů (například odposlech), zatímco pro komerční zjišťování strategických informací je tato technika zakázána, takže marketingový specialista musí hledat jiné, legální prostředky. Ale tato technika je dostupná

---

[35] PIEKALKIEWICZ, J. *Historie světové špionáže : agenti, systémy, akce*. 1. vyd. Praha : Naše vojsko, 2004. s. 12. ISBN 80-206-0738-2.
[36] SOBEK, V. *Pomohli jsme sestřelit Powerse : tajemství Vědeckotechnické rozvědky ČSSR*. 1. vyd. Praha : Futura, 2011. s. 20. ISBN 978-80-86844-67-1

a nedělejme si iluze, že není v mnoha případech i používána. Na čem by vydělávaly organizace, nabízející otevřeně na internetu takovou techniku a služby?

IT usnadnila ohromným způsobem práci jak strategickému marketingu, tak oné tajemné činnosti „agentů“. Mohutné informační systémy, pracující na bázi bezdrátového přenosu signálu, umožní těmto lidem pracovat z domu. Nemusí opustit svoji pracovnu, a pokud mají dostatečnou praxi ve vyhledávání potřebných informací, umí posoudit důvěryhodnost jejich zdrojů a najít způsob ověření pravdivosti, případně najít zdroj doplňující informace, mají velkou část sběru informací v ruce. I velmi důležité informace se objevují na veřejných stránkách, anebo jsou přenášeny bez šifrování na nechráněných sítích. Další otázkou je jejich třídění, analýza a prvotní závěry. Zde asi můžeme hovořit o úplně stejné práci marketingového specialisty, investigativního novináře i „agenta“. Jakmile vkročí tito lidé do terénu, zase mají mnoho společného v legální činnosti. Marketingový specialista použije „mystery shopping“ (fiktivní nákup), aby pomocí najaté osoby, vydávající se za kupujícího, prověřil poctivost a loajálnost obchodního partnera. Investigativní novinář požádá přítelkyni, aby se na úřadě zajímala o pozemek, protože má podezření, že se tam na úřadě děje s pozemky něco nekalého. A onen „agent“ si půjčí cizí identitu a zajímá se o spolupráci s výzkumným centrem, kde se podle informací z předchozí fáze zjišťování mohou nacházet informační aktiva, která mají vysokou hodnotu pro jeho zaměstnavatele (a pochopitelně i firmu, která je vlastní). Pozor, totéž může dostat za úkol i vedoucí strategického marketingu konkurenční high-tech firmy, soupeřící o státní zakázky! Všichni tři použili sociální inženýring (způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace – poznámka autora). Kdo z nich jednal legálně a kdo nikoliv? Kdo může být stíhán a kdo nikoliv? A vlastně za co a kdo by to mohl posoudit? Zkušenost říká, že když to zjistí obchodní partner, tak se naštve a přestane obchodovat. Když to zjistí úřad, dá si na onu přítelkyni v budoucnu pozor a novináře nebude zvát na tiskové konference, případně podá trestní oznámení na neznámého pachatele. Když to zjistí ono významné centrum výzkumu, tak vyhodí ředitele pro bezpečnost informací a za mnoho milionů nějaké vhodné měny zahájí obdobnou odvetnou akci. A pokud byl oním provinilým a odhaleným „agentem“ zrovna „agent státní“, je z toho na veřejnosti nanejvýš parlamentní komise nebo perfektní téma pro volební kampaň. V tichosti může dojít k nějakému odškodnění onoho významného centra, podle toho, jak významné je a kdo je jeho vlastníkem. Velmi často není ani třeba použít při získávání informací sociální inženýring. Lidé i na vysokých pozicích úředních a komerčních nemají povědomí o ochraně informací a organizace jdou

obvykle cestou od jednoho extrému ke druhému: mizivá ochrana a doslova dům otevřených dveří nebo paranoidní přehnaná opatření, která nakonec mají opačný účinek. Takže pokud se osoba s přiměřenou kvalifikací, ať je to marketingový specialista, investigativní novinář nebo „agent“, seznámí s určitým oborem a začne se v něm naprosto legálně pohybovat, má šanci většinu informací získat naprosto legálním způsobem. Stačí, aby měl zkušenosti s prací s informacemi, měl dobře definovaná cílená informační aktiva, přirozené a dál rozvíjené systémové analytické myšlení se schopností nakonec provést syntézu, čas a prostředky potřebné k práci.[37]

4.1.2 Nelegální zdroje informací

Pro firmu jsou důležité zejména informace od jiných firem, které jí pomohou zvýšit konkurenční výhodu. Přitom však tyto informace nejsou zpravidla veřejně dostupné a jsou získatelné pouze za úplatu a po ošetření užití oněch informací ve smlouvě mezi klientem a poskytovatelem informace. Vedle toho ale zájemce o maximálně přínosné informace své vlastní informace, které tvoří jeho konkurenční výhodu, také utajuje. Z toho důvodu zde existuje problém kvality veřejně nabízených informací od firem. Mohou být bezcenné pro konkurenci jako odborníka ve stejném oboru. Aby firma svou konkurenční výhodu na trhu mezi více firmami udržovala či posilovala, musí být schopna získávat co nejvíce utajovaných informací od konkurence.[38]

4.2 Duševní vlastnictví jako mezinárodní oběživo a hodnocení hrozeb

Duševní vlastnictví je stále oblíbenějším cílem kybernetických podvodníků. Podle odborníků byly průniky do firemních dat ve zvýšené míře organizovány skupinami „kybernetické mafie“. Kybernetičtí zločinci se pomocí sofistikovaných technik cíleného phishingu (podvodná technika používaná na Internetu k získávání

[37] KŘEPELKOVÁ, H. *Marketing nebo průmyslová špionáž?* [online]. Ictsecurity.cz, 2011 [cit. 2011-7-01]. Dostupné z WWW: <http://ictsecurity.cz/sk/pdf/serial-o-informacnej-bezpecnosti/marketing-nebo-prumyslova-spionaz-serial-o-informacni-bezpecnosti-ze-vsech-uhlu.pdf>.

[38] MAREK, J. *Využitelnost veřejně poskytovaných informací od firem* [online]. Risk-Management.cz, 2011 [cit. 2011-7-01]. Dostupné z WWW: <http://www.risk-management.cz/clanky/Vyuzitelnost-verejne-poskytovanych-informaci-od-firem.pdf>.

citlivých údajů) stále častěji zaměřují na vedoucí pracovníky. 39 % respondentů pokládá ochranu duševního vlastnictví před zloději z vnějšku organizace za největší problém vůbec.

Zaměstnanci kradou duševní vlastnictví kvůli finančnímu zisku, a aby získali konkurenční výhodu na trhu práce. Stále větší množství zaměstnanců přistupuje k firemním datům s cílem ukrást klíčové informace a obohatit se. S pokračováním celosvětové recese a úbytkem legálním pracovních příležitostí se uchazeči o zaměstnání častěji uchylují ke krádežím dat svého současného zaměstnavatele, o nichž soudí, že by mohla být zajímavá pro budoucího zaměstnavatele. Domnívají se, že tímto způsobem zvýší svoji hodnotu na trhu práce. 42 % respondentů pokládá za největší hrozbu pro své klíčové informace právě odcházející zaměstnance.[39]

Studie Unsecured Economies společnosti McAfee navrhuje, aby schopnost zabezpečit duševní vlastnictví byla pokládána za klíčovou pro hodnocení bezpečnosti investic v Brazílii, Japonsku a Číně. Celých 60 % odpovídajících z Číny uvádělo, že větší zabezpečení je důvodem, proč duševní vlastnictví a další citlivé informace mají raději uloženy mimo vlastní zemi. Zajímavé je i hodnocení hrozby pro duševní vlastnictví ze zeměpisného pohledu. Politika ochrany dat a vnímání hrozeb jsou ovlivněny geopolitickými odlišnostmi. Firmy zúčastněné v průzkumu pokládají (z různých legislativních, kulturních a ekonomických důvodů) za problematické země především Čínu, Pákistán a Rusko (viz graf č. 1).

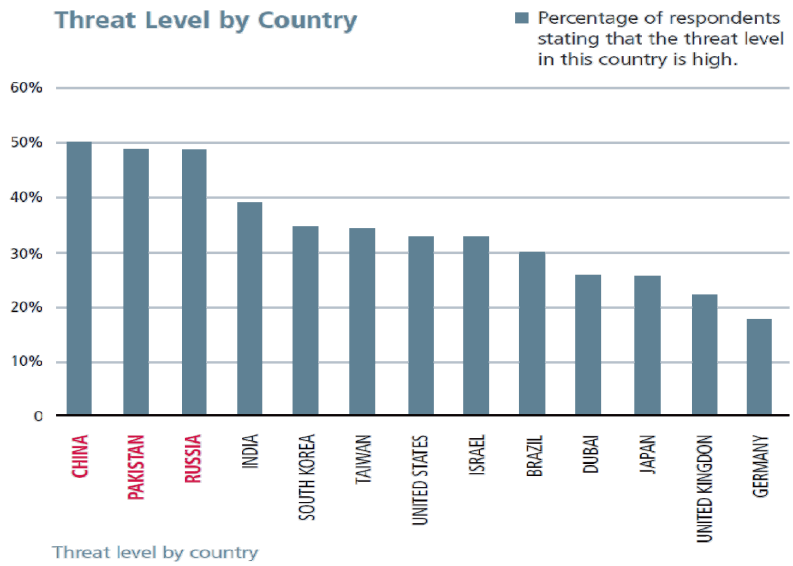
Přímo v jednotlivých zemích jsou často vnímána přednostně rizika ztráty dat s ohledem na geopolitickou situaci. V Číně se firmy často domnívají, že hrozby jejich duševnímu vlastnictví mají původ v USA nebo na Tchaj-wanu, indické firmy mají obavy z Pákistánu. Americké firmy se obávají především úniku dat do Ruska či Číny. Naopak například indické firmy se uchovávat citlivá data v Číně obávají mnohem méně. I řada čínských firem se ale snaží citlivá data uchovávat raději mimo svoji zemi.

V případě Pákistánu odrazuje respondenty především existence fundamentalismu v zemi či přítomnost teroristických skupin. Outsourcing v Pákistánu je proto mnohem méně rozšířený než v sousední Indii. Rusko je někdy pokládáno za

[39] *McAfee Unsecured Economies Report* [online]. Resources.mcafee.com, 2009 [cit. 2011-10-12]. Dostupné z WWW: <http://resources.mcafee.com/content/NAUnsecuredEconomiesReport>.

oblíbené sídlo kybernetických zločinců. Respondenti se mnohdy domnívají, že místní mafie jsou vládou tiše tolerovány.[40]

Graf č. 1: Vnímání rizik podle jednotlivých zemí, graf ze studie Unsecured Economies: Protecting, Vital Information společnosti McAfee[41]



Studie dále poukazuje na další zajímavá čísla:[42]

- **Jaký je podíl firem, které na zabezpečení informací věnují 20 % nebo více z celkových výdajů na IT?**
  - Indie... 35 %,
  - Čína... 33 %,
  - Brazílie... 27 %,
  - Německo... 20 %,
  - USA... 19 %,
  - Japonsko... 10 %,
  - Velká Británie... 4 %.

44 % dotazovaných britských firem věnuje na zabezpečení dokonce méně než

[40] *McAfee Unsecured Economies Report* [online]. Resources.mcafee.com, 2009 [cit. 2011-10-12]. Dostupné z WWW: <http://resources.mcafee.com/content/NAUnsecuredEconomiesReport>.
[41] *McAfee Unsecured Economies Report* [online]. Resources.mcafee.com, 2009 [cit. 2011-10-12]. Dostupné z WWW: <http://resources.mcafee.com/content/NAUnsecuredEconomiesReport>.
[42] *McAfee Unsecured Economies Report* [online]. Resources.mcafee.com, 2009 [cit. 2011-10-12]. Dostupné z WWW: <http://resources.mcafee.com/content/NAUnsecuredEconomiesReport>.

5 % z celkového rozpočtu na IT. Průměrná roční ztráta vyplývající z narušení duševního vlastnictví byla v rámci průzkumu stanovena na 4,6 milionu dolarů. Přitom ve Velké Británii to bylo v průměru „pouhých“ 375 tisíc dolarů ve srovnání se 7,2 miliony dolarů v Číně.

- **Co je pokládáno za největší rizika pro firemní data?**
    - Vnitřní nepřítel... 68 %,
    - Softwarová zranitelnosti, proces záplatování... 51 %,
    - Kybernetický terorismus... 38 %,
    - Průmyslová špionáž... 36 %.

5 Ekonomické soupeření firem

Competitive Intelligence (dále CI), konkurenční zpravodajství, benchmarking jsou prostředky k získávání včasné relevantní informace o konkurenci založené na soustavném sledování trhu. Tímto způsobem mohou být společnosti konkurenceschopné a získají dobrý základ pro správné strategické rozhodování.

5.1 Konkurence a konkurenčnost

Soudobé uvažování o tom, jaká může být nebo by měla být budoucnost podniku, se začíná od jeho konkurenčnosti, od jeho schopnosti konkurovat, utkat se na kolbišti trhu s rivaly, obstát a zajistit si alespoň na nějaký čas prosperitu. Nemá-li podnik takovou schopnost, je jeho snaha marná.

Definice konkurenčnosti mívá několik komponent:[43]

1. Zaprvé je třeba schopnosti dostat se na trh (překonat vstupní tržní bariéry).
2. Zadruhé být s to soupeřit s jinými podniky a na trhu se udržet (s přiměřeným ziskem). Někdy se tato složka zpřísňuje výrokem, že má jít o náročné mezinárodní trhy, nikoli o snadno přístupné trhy periferní (lokální).
3. Zatřetí se bere v úvahu nikoli jednotlivý, tím méně nahodilý výsledek tržního střetu, nýbrž takový, který hned nezaniká, ale trvá po krátkou a ještě lépe po střední nebo snad i delší dobu (což závisí na charakteru produkce a poptávce po ní).

   K tomu se může přidat podmínka, že se podnik posléze dokáže z trhu stáhnout (překonat výstupní bariéry) a přitom neztratit vydělaný zisk.

5.2 Competitive Intelligence (CI), konkurenční zpravodajství

Mnohdy se v souvislosti s tímto pojmem můžeme setkat i s názvy komerční zpravodajství, podnikatelské zpravodajství. Někteří pohlíží na konkurenční zpravodajství jako na průmyslovou špionáž, tedy jako na neetickou a nelegální aktivitu.

---

[43] JIRÁSEK, J. *Souboj mozků v řízení.* 1. vyd. Praha : Alfa Publishing, s.r.o., 2004. s. 20. ISBN 80-86851-01-X.

Problém je ten, že si lidé mylně myslí, že zpravodajská činnost je získávání tajných informací. Ve skutečnosti je základ Competitive Intelligence (dále jen CI) v procesu systematického získávání informací z otevřených zdrojů a následné analýze těchto informací. CI je proces sledování vnějšího prostředí, které se zaměřuje na získávání a zpracování podstatných informací sloužících k nabytí konkurenční výhody a pro podporu dlouhodobého plánování. Může se říci, že CI je informační proces o konkurenci a snaha být vždy před ní.

Competitive Intelligence se v českém prostředí vymezuje podle terminologické databáze TDKIV jako „zjišťování, sledování a vyhodnocování konkurenčního prostředí (firmy, organizace) s cílem odhalit slabé a silné stránky konkurence, rozpoznat její strategické záměry. Zahrnuje analýzu a syntézu dat, resp. informací, které se transformují do strategických znalostí, shromažďování informací o konkurenci a sledování subjektů firemního okolí (trh, stát, právo a legislativa, politické a demografické souvislosti)“.[44]

CI je tedy proces, při kterém podniky sledují a vyhodnocují informace o svých konkurentech a o prostředí, ve kterém podnikají. Na základě sběru těchto informací pak dochází k jejich analýze či syntéze a dále k tomu, že jsou výsledné poznatky a znalosti aplikovány. CI se využívá zejména při snaze dostihnout a předhonit konkurenční firmy, nebo naopak udržet si již získanou výhodu a náskok oproti ostatním. Mezi činnosti, které mohou z CI těžit nejvíce, patří asi z největší míry strategické plánování, ale využití je možné nalézt nejen zde. CI lze aplikovat taktéž na taktické úrovni, například jako nástroj podpory prodeje či k eliminaci momentů překvapení atd.[45]

Účastníky procesu CI jsou v ideálním případě všichni pracovníci organizace, jejich míra účasti je však různá podle role, kterou v procesu hrají. Úlohy jednotlivých aktérů vycházejí z tzv. zpravodajského cyklu, který popisuje obecné zásady organizovaného informování (zpravodajství) a který má čtyři hlavní fáze:[46]

---

[44] *KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV)* [online]. 2003. Praha : Národní knihovna České republiky, 2003 [cit. 2012-02-22]. Dostupný z WWW: <http://aleph.nkp.cz/F/?func=direct&doc_number=000000438&local_base=KTD>.

[45] ŠMEJKAL, P. *Role informačního specialisty v procesu competitive inteligence* [online]. ProInflow: Časopis pro informační vědy, 2010 [cit. 2012-20-02]. ISSN 1804-2406. Dostupné z WWW: <http://pro.inflow.cz/sites/default/files/pdfcisla/ProInflow_12010.pdf>.

[46] MOLNÁR, Z. *Potřeba, místo a úloha Competitive Intelligence profesionála v organizaci* [online]. Sborník konference systémová integrace 2008, CSSI, 2008 [cit. 2012-02-17]. Dostupné z WWW: <http://si.vse.cz/archive/proceedings/2008/potreba-misto-a-uloha-ci-profesionala-v-organizaci.pdf>.

- Identifikace informačních potřeb: vyplynutí z cílů organizace a rolí jejich pracovníků.
- Sběr informací: vyhledávání v relevantních zdrojích a dotazování relevantních osob.
- Analýza informací: prezentace získaných informací v kontextu potřeb nebo tvorba závěrů.
- Komunikace informací: různé formy předávání zpracovaných informací a závěrů uživatelům.

5.3 Benchmarking v oblasti průmyslu

Benchmarking… Ještě dříve, než se stačil dostavit k odbornému překladu, se angloamerický výraz vžil. Co vlastně původně znamená?

„Bench“ je pracovní stůl nebo lavice, podobně zní německý výraz „ponk“ (Bank), u nás zdomácnělý. „Mark“ je znamení, značka. Benchmark znamenal původně rysku, kterou si truhlář vyznačil na pracovním stole a pak k ní přiřezával lišty, prkna, fošny. Odtud se výraz dostal do manažerské a obecné mluvy.[47]

5.3.1 Definice benchmarkingu

Je dost čtenářů, kteří než začnou rozmýšlet, chtějí „definici“ toho, čím se mají obírat. Není to ani nejpoučnější, ani nejrychlejší způsob. Nikoli nadarmo varují znalci, že každá definice kulhá.

Benchmarking je standard pro srovnání měření a je zaměřen zejména na porovnávání s přímými konkurenty.

Podstatu představuje srovnávací analýza. Kladou se proti sobě konkurenční vlastnosti podniku a jeho tržních rivalů. Takové vlastnosti, jako je nabídka, charakter výrobků nebo služeb, kvalita, technologie, výkon při jejich zhotovování, pohotovost a kompletnost dodávky, cena na trhu, servis atd. Někteří odborníci používají vtipný bonmot, že jde o „souměření pro soupeření“[48].

---

[47] JIRÁSEK, J. *Benchmarking a konkurenční zpravodajství.* 1. vyd. Praha : Profess Consulting, s.r.o., 2007. s. 5. ISBN 978-80-7259-051-3.
[48] JIRÁSEK, J. *Agenda příštích let.* 1. vyd. Praha : Professional Publishing, 2006. s. 85. ISBN 80-86946-04-5.

5.3.2 Zaměření benchmarkingu

Zde by málo pomohl nějaký výčet. Porovnává se všechno, co má nějaký podstatný vliv na naši tržní pozici. Nic podstatného by se nemělo opominout a také nic zveličovat.

Je třeba mít na zřeteli, že se obsah může měnit. Každá doba má své priority, které rozhodují o konkurenčnosti. Žádný výkon není jednou provždy daný. O konkurenčnosti je třeba uvažovat ve vývoji.

Předmětem srovnávání může být výrobek, služba, různé procesy přípravy a provádění výroby, obchodu, financování, může se týkat zdrojů, jako jsou kvalifikovaní lidé, technika, materiál, anebo také marketingu, financování nebo organizace atd.[49]

Do benchmarkingu se jistě pustí podniky, které jsou si vědomy tržního napětí, mají s ním nějaké zkušenosti; potřebují hlavně systematiku, opakované porovnání, širší přehled, určité vědecky podložené zásady atd. U nich benchmarking brzy splývá se strategickým řízením.

Ale i podniky, které nejsou dost vynalézavé, nemají zkušenost s mezipodnikovým srovnáváním, mohou v benchmarkingu najít poučení a inspiraci. Na co nestačí samy, mohou se učit od druhých. Nemusejí „vynalézat kolo“ ani „objevovat Ameriku“. Ovšem vystavují se riziku, že přebírání cizích vzorů zanedbají vlastní.[50]

Benchmarking je poměrně nový obor a přitom krajně významný a nadále rostoucí. Praktická zkušenost potvrzuje, že bez osobního nasazení, nebo aspoň podpory ze strany vrcholového vedení se benchmarking nevydaří. Hodně pomáhá uvědomit si, že naše vlastní strategie bez uvážení schopností protivníka zůstává kusá, nedodělaná, nespolehlivá.[51]

5.3.3 Benchmarking v české praxi

Benchmarking má za sebou jinošská léta, stal se uznávaným pomocníkem řízení, zejména vrcholového, pronikl doslova do celého světa. Česká praxe zůstala povážlivě pozadu. Jen tenká menšina podniků přijala benchmarking (kolem 10 % středních

[49] JIRÁSEK, J. *Benchmarking a konkurenční zpravodajství.* 1. vyd. Praha : Profess Consulting, s.r.o., 2007. s. 13. ISBN 978-80-7259-051-3.
[50] JIRÁSEK, J. *Benchmarking a konkurenční zpravodajství.* 1. vyd. Praha : Profess Consulting, s.r.o., 2007. s. 14. ISBN 978-80-7259-051-3.
[51] JIRÁSEK, J. *Benchmarking a konkurenční zpravodajství.* 1. vyd. Praha : Profess Consulting, s.r.o., 2007. s. 16. ISBN 978-80-7259-051-3.

a velkých) a naprostá většina stěží ví, často vůbec neví, oč jde. Ještě horší je to v mimoprůmyslových oborech, ve školství, ve zdravotnictví, ve státní a veřejné správě a podobně. I tam, kde se neodehrává silový tržní zápas, kde se organizace spolu neutkávají na trhu, má smysl poznávat své postavení a usilovat o prvenství.

Podle JIRÁSKA[52] je benchmarking v české praxi nasazován velmi pomalu a velmi málo. Podnikatelská vrstva v minulých letech měla slibné možnosti a také jich z nemalé části využila: privatizace bez kontroly, otevřené „naše banky“, které mlčky přihlížely zadlužování podniků, rozchvácení velkých podniků, ústup z mnoha tradičních trhů a konečně něco, nad čím náš svět zahanbeně žasl – „tunelování“ podniků ve prospěch soukromého bohatství.

JIRÁSEK[53] dále poukazuje na problém velkých podniků s vlastním výzkumem a vývojem, technickým vybavením, rozvinutou dělbou práce, často exportující své zboží do celého světa, kdy pod cizí kontrolu přešly více než 2/3 českého průmyslového majetku a kdy vedení těchto podniků dostávají úkoly od svých centrál, jsou zvenčí hodnoceny a i odměny vedení závisí na vnějším rozhodnutí. Pak také i benchmarking je vtažen do těchto poměrů a jeho používání může diktovat cizí centrála.

Podle JIRÁSKA[54] mohou ovšem i podniky, divize, sektory cizích majitelů získat silnější postavení, když se v dohodě se svou zahraniční centrálou dají do benchmarkingu.

Bohužel, problematika benchmarkingu je v současném českém prostředí spíše popelkou než rutinně zvládnutou formou učení se, konstatuje NENADÁL.[55]

5.4 Trendy obchodní spolupráce

V důsledku ekonomického soupeření a snaze po vyšším zisku jsou firmy nuceny lokalizovat výroby a mnohdy i svá vývojová centra do oblastí s levnější pracovní silou. Má to ovšem i svá úskalí v případě nedokonalé ochrany investic.

---

[52] JIRÁSEK, J. *Benchmarking a konkurenční zpravodajství.* 1. vyd. Praha : Profess Consulting, s.r.o., 2007. s. 22. ISBN 978-80-7259-051-3.
[53] JIRÁSEK, J. *Benchmarking a konkurenční zpravodajství.* 1. vyd. Praha : Profess Consulting, s.r.o., 2007. s. 22. ISBN 978-80-7259-051-3.
[54] JIRÁSEK, J. *Benchmarking a konkurenční zpravodajství.* 1. vyd. Praha : Profess Consulting, s.r.o., 2007. s. 22. ISBN 978-80-7259-051-3.
[55] NENADÁL, J., VYKYDAL, D., HALFAROVÁ, P. *Benchmarking : mýty a skutečnost : model efektivního učení se a zlepšování.* 1. vyd. Praha : Management Press, 2011. s. 8. ISBN 978-80-7261-224-6.

„My“ tam postavíme jeden objekt (cukrovar, elektrárnu, v evropském pojetí „My“ třeba magnetické rychlovlaky), který oni obratem 10x zkopírují, naučí se to a nakonec začnou vyvážet a konkurovat nám na třetích trzích.

Oni sem v rámci vzájemného obchodu vyvezou své zboží, navíc v násobně větší hodnotě (i té podceněné) než my k nim. Díky podhodnocené ceně se nevyplatí zde nic vyrábět, je lepší se účastnit hry na bublinu přidané hodnoty (nákup za 100, prodej za 600, jéje my jsme produktivní). V podstatě se sami manévrujeme do podobného začarovaného kruhu, jakým trpí Afrika s dovozem dotovaných potravin z EU.

„My“ investujeme tak, že tam postavíme novou fabriku, přivezeme novou technologii, možná kvůli tomu dokonce zavřeme něco tady a nahradíme obchodním zastoupením.

Oni investují způsobem, že skoupí naše firmy, které mají nějakou nesnadno nahraditelnou hodnotu. Ať jde o technologie nebo přirozený monopol, prostě vše co nelze z Číny dovézt. A jsou díky momentální situaci levně k mání.

Nebo aktuálně chtějí investovat do výroby energie ze slunce. Sluneční farmy vybaví čínskými kolektory a nechají si od nás vyplácet dotace příštích dvacet let. To vše s vynikající garantovanou návratností.[56]

[56] *Investice Čína vs Západ, 3:0* [online]. Zadluzení.cz, 2010 [cit. 2011-11-04]. Dostupné z WWW: <http://www.zadluzeni.cz/2010/01/investice-cina-vs-zapad-30.html>.

6 Boj a ochrana proti průmyslové špionáži

Dnešní nejrychleji rostoucí čínská ekonomika hladoví po technologii a často nechápe západní pojem autorských práv. Z těchto důvodů je jistě zapotřebí účinné ochrany a obrany proti průmyslové špionáži.

Ochrana obchodního tajemství, důvěrných informací a know-how je pro každého podnikatele z hlediska jeho fungování klíčová. Tato nemajetková práva představují v podnikání výhodu ve vztahu ke konkurenci. Je možné se proti špionáži bránit, a jak? Někdo by mohl namítnout, že nejlepší ochrana proti průmyslové špionáži je dát výrobek rychle na trh. Jistě se vyplatí být rychlý, určovat trendy a být první. Nechat si něco patentovat je jistě časově náročné, ale je ochranou jednou z nejúčinnějších.

Naopak je třeba přiznat, že neexistuje žádná metoda, která by mohla správní radě spolehlivě a včas signalizovat, že v jejím podniku dochází nebo došlo k akcím průmyslové špionáže. Nejčastěji se to zjistí podle poklesu zisků a pak přicházejí zprávy podrobnější. Konkurence přijde na trh s novým výrobkem dříve nebo ve stejnou dobu jako podnik, u něhož byl onen výrobek vyvinut – a při tom jej nabízí za nižší cenu.[57]

6.1 Hrozby a ochrana ekonomických zájmů firem

Dle hrozby napadení je možné rozdělit ochranu na vnitřní a vnější: vnitřní (ochrana proti útokům zevnitřku organizace) – zvláštní režim, lidský faktor / bezpečnostní služba, vnější ochrana počítačové sítě, zálohování dat a informací, režimy práce s datovými nosiči, apod. vnější (ochrana proti útokům zvenčí) – technologická aktivní ochrana (biometrické systémy, kontroly vstupu, monitorovací a kamerové systémy, apod.), pasivní ochrana dat a spojů (firewally, stínění datových a komunikačních spojů, filtrování, apod.) a lidská ochrana (bezpečnostní služba).

Metody obrany proti průmyslové špionáži lze kategorizovat podle oblasti, které se má daná ochrana týkat:[58]

---

[57] BERGIER, J. *Průmyslová špionáž.* 1. vyd. Praha : Orbis, 1974. s. 184. ISBN 605-22-826.

[58] *Metody špionáže: Průmyslová špionáž* [online]. Specialista.info, 2006 [cit. 2011-11-04]. Dostupné z WWW: <http://www.magazin.specialista.info/view.php?cisloclanku=2006013001>.

- **lidé / zaměstnanci** – v počítačové síti je řešením vytvoření uživatelských účtů a vyřešení přístupových práv; v rámci fyzické ochrany informací je nutné klasifikovat informace (např. stupně utajení) a vytvořit specifickou metodiku řešení přístupů k jednotlivým třídám informací.

- **informace** – v počítačové síti jde opět o klasifikaci informací a specifikaci přístupu k nim dle uživatelských práv; v rámci fyzické ochrany je nutné používat trezory, bezpečnostní zámky, části budovy se zvláštními režimy, ochrana lidmi (bezpečnostní služba), apod.

Průmyslová špionáž často využívá mezery v objektové či počítačové bezpečnosti daných firem. Díky tomu také vznikají bezpečnostní agentury, které se specializují na ochranu proti konkrétním druhům hrozeb. Průmyslová špionáž je trend, který se do značné míry pojí s konkurenceschopností firem, ale většina informací o jednotlivých metodách či pokusech o napadení není veřejně prezentována, což má za následek celkově malé znalosti o tomto druhu špionážní činnosti.

6.1.1 Vnitřní hrozby úniku utajovaných informací

Interní hrozby zahrnují spektrum jednotlivců, kteří by potenciálně mohli ukrást, nebo způsobit únik vládních nebo firemních utajovaných informací. Zahrnují vše od nespokojených zaměstnanců, až po zvědavé hackery, kteří jsou za krádeže informací placeni. Insideři se ovšem od hackerů liší. Na rozdíl od nich se nesnaží hledat mezery v zabezpečení sítě, naopak - insideři už jsou uvnitř a k datům mají přístup, takže ukrást data je pro ně jenom otázkou vypálení CD nebo zkopírování na USB disk.[59]

Stále větší množství zaměstnanců přistupuje k firemním datům s cílem ukrást klíčové informace a obohatit se. S pokračováním celosvětové recese a úbytkem legálním pracovních příležitostí se uchazeči o zaměstnání častěji uchylují ke krádežím dat svého současného zaměstnavatele, o nichž soudí, že by mohla být zajímavá pro budoucího zaměstnavatele. Domnívají se, že tímto způsobem zvýší svoji hodnotu na

[59] JOSHUA, P. *Informační válka, kybernetické útoky a rostoucí hrozba insiderů* [online]. Velká Epocha, 2010 [cit. 2011-10-26]. Dostupné z WWW: <http://www.velkaepocha.sk/2010122115706/Informacni-valka-kyberneticke-utoky-a-rostouci-hrozba-insideru.html>.

trhu práce. 42 % respondentů pokládá za největší hrozbu pro své klíčové informace právě odcházející zaměstnance.[60]

6.1.2 Oblasti vnějších hrozeb firemní špionáže

Externím hrozbám před firemní špionáží se musí čelit v několika oblastech:[61]

- **V oblasti personální:**
- zabránit kontaktování a vytěžování zaměstnanců firmy konkurencí pod falešnými záminkami a činit na základě toho potřebná opatření,
- zabránit fingovaným zaměstnáním zaměstnanců konkurence ve vlastní firmě,
- zabránit získávání informací konkurencí formou vydírání,
- atd.
- **Napadení počítačových sítí:**
- zabránit přímé krádeži počítačových nosičů informací nebo jejich nelegálnímu kopírování,
- zabránit technickému získávání informací z počítačových sítí.
- **Odposlouchávání a sledování nelegálními prostředky:**
  Prostředky audio, video, audiovideo a dalšími speciálními zpravodajskými technickými prostředky a postupy využívajícími tyto technické prostředky.
- **Přímému narušení vlastnických práv:**
  Jde například o vloupání s cílem krádeže různých nosičů informací (dokumentů, médií apod.).

6.1.3 Hrozby pro duševní vlastnictví ze zeměpisného pohledu

Politika ochrany dat a vnímání hrozeb jsou ovlivněny geopolitickými odlišnostmi. Firmy zúčastněné v průzkumu pokládají (z různých legislativních, kulturních a ekonomických důvodů) za problematické země především Čínu, Pákistán a Rusko.

Přímo v jednotlivých zemích jsou často vnímána přednostně rizika ztráty dat s ohledem na geopolitickou situaci. V Číně se firmy často domnívají, že hrozby jejich

---

[60] *McAfee Unsecured Economies Report* [online]. Resources.mcafee.com, 2009 [cit. 2011-10-12]. Dostupné z WWW: <http://resources.mcafee.com/content/NAUnsecuredEconomiesReport>.
[61] BRABEC, F. *Ochrana bezpečnosti podniku.* 1. vyd. Praha : EUROUNION s.r.o., 1996. s. 164-165. ISBN 80-85858-29-0.

duševnímu vlastnictví mají původ v USA nebo na Tchaj-wanu, indické firmy mají obavy z Pákistánu. Americké firmy se obávají především úniku dat do Ruska či Číny. Naopak například indické firmy se uchovávat citlivá data v Číně obávají mnohem méně. I řada čínských firem se ale snaží citlivá data uchovávat raději mimo svoji zemi.

V případě Pákistánu odrazuje respondenty především existence fundamentalismu v zemi či přítomnost teroristických skupin. Outsourcing v Pákistánu je proto mnohem méně rozšířený než v sousední Indii. Rusko je někdy pokládáno za oblíbené sídlo kybernetických zločinců. Respondenti se mnohdy domnívají, že místní mafie jsou vládou tiše tolerovány.[62]

6.1.4 Odlišnosti v přístupu k ochraně životně důležitých informací

Rozvíjející se země jsou k ochraně duševního vlastnictví více motivovány a vynakládají na ochranu více prostředků než vyspělé státy. Firmy z Brazílie, Číny a Indie utrácejí za zabezpečení více peněz než ty z Německa, Velké Británie, USA a Japonska. 79 % respondentů z Číny a 68 % z Indie uvedlo, že jejich firmy investovaly do zabezpečení svého duševního vlastnictví, aby tak získaly konkurenční výhodu.[63]

6.2 Legislativa na ochranu duševního vlastnictví před průmyslovou špionáží

Stav české legislativy v oblasti ochrany duševního vlastnictví je v současné právní úpravě patentů plně v souladu se závazky vyplývající pro oblast práv průmyslového vlastnictví z mezinárodního práva veřejného a z komunitárního práva.[64]

---

[62] *McAfee Unsecured Economies Report* [online]. Resources.mcafee.com, 2009 [cit. 2011-10-12]. Dostupné z WWW: <http://resources.mcafee.com/content/NAUnsecuredEconomiesReport>.
[63] *McAfee Unsecured Economies Report* [online]. Resources.mcafee.com, 2009 [cit. 2011-10-12]. Dostupné z WWW: <http://resources.mcafee.com/content/NAUnsecuredEconomiesReport>.
[64] *Stav české legislativy v oblasti ochrany duševního vlastnictví* [online]. BusinessInfo.cz, 2009 [cit. 2012-01-15]. Dostupné z WWW: <http://www.businessinfo.cz/cz/clanek/podnikatelske-prostredi/stav-ceske-legislativy-duse-vlastnictvi/1000520/51563/>.

6.2.1 Národní legislativa chránící duševní vlastnictví

V České republice je ochrana obchodního tajemství, důvěrných informací a know-how pro každého podnikatele, z hlediska jeho fungování, klíčová. Tyto nemajetková práva představují v podnikání výhodu ve vztahu ke konkurenci:[65]

- **Obchodní tajemství**

Dle § 17 (obchodního zákoníku č. 513/1991 Sb.), obchodní tajemství tvoří veškeré skutečnosti obchodní, výrobní či technické povahy související s podnikem, které mají skutečnou nebo alespoň potenciální materiální či nemateriální hodnotu, nejsou v příslušných obchodních kruzích běžně dostupné, mají být podle vůle podnikatele utajeny a podnikatel odpovídajícím způsobem jejich utajení zajišťuje. Do obchodního tajemství spadá veškeré know-how, veškerá technická a výrobní dokumentace (zdrojové i binární kódy, programová dokumentace, databáze atd.). Samozřejmě, že např. softwaru a databázím je poskytována vedle i ochrana autorskoprávní. Stejně tak lze do kategorie obchodního tajemství zařadit např. marketingové strategie, vnitřní způsob fungování společnosti, strategická rozhodnutí a podnikatelské záměry. Ochrana je ovšem poskytována jen skutečnostem nikoliv běžně dostupným, k nimž se v příslušné oblasti podnikání nelze dostat, aniž by byly porušeny právní předpisy chránící před nekalou soutěží či trestněprávními předpisy (přetahování zaměstnanců, průmyslová špionáž atd.). Za obchodní tajemství nelze považovat účetní závěrky společnosti, kterou jsou většinou již přístupné na internetu v elektronické podobě ve sbírce listin. Aby ochrana ze zákona byla poskytnuta určitým skutečnostem, musí podnikatel určitým způsobem zajišťovat jejich ochranu. Zajištění ochrany lze chápat jako základní zajištění bezpečnosti majetku (budov, automobilů) před jejich narušením ze strany nevítaných hostů a rovněž tak zajištění ve smluvních dokumentech či vnitřních řádech podnikatele.

Aby obchodní tajemství bylo chráněno, nestačí si toto dohodnout smluvními stranami či určité informace jednostranně (i písemně) prohlásit za obchodní tajemství. Podmínkou je naplnění všech zákonných znaků.

Podnikatel má výlučné právo tímto obchodním tajemstvím nakládat, zejména udělit svolení k jeho užití a stanovit podmínky takového užití (licenční smlouvou) nebo

---

[65] JANSA, L. *Ochrana obchodního tajemství, důvěrných informací a know-how v podnikání* [online]. Právo IT, 2007 [cit. 2012-01-12]. Dostupné z WWW: <http://www.pravoit.cz/article/ochrana-obchodniho-tajemstvi-duvernych-informaci-a-know-how-v-podnikani>.

jej jako know-how vložit do základního kapitálu společnosti. Zpřístupnit obchodní tajemství je možné v rámci dispozic s podnikem (smlouvou o prodeji či nájmu podniku) nebo samostatnou smlouvou.

Při porušení obchodního tajemství náleží dotčenému podnikateli právo požadovat zdržení se porušování tohoto tajemství, odstranění závadného stavu, náhrady škody, přiměřeného zadostiučinění i v penězích. Tato ochrana je absolutní a působí vůči všem a vůči jakémukoliv způsobu porušení ochrany obchodního tajemství. Vedle toho zná obchodní zákoník ochranu relativní, která se uplatní mezi soutěžiteli v rámci hospodářské soutěže. Skutková podstata spočívá v tom, že jednající jiné osobě neoprávněně sdělí, zpřístupní, pro sebe nebo pro jiného využije obchodní tajemství, které může být využito v soutěži a o němž se dověděl:

a) tím, že mu tajemství bylo svěřeno nebo jinak se stalo přístupným (např. z technických předloh, návodů, výkresů, modelů, vzorů) na základě jeho pracovního vztahu k podnikateli nebo na základě jiného vztahu k němu (obchodní smlouvy), popřípadě v rámci výkonu funkce, k níž byl soudem nebo jiným orgánem povolán (např. likvidátor, správce konkursní podstaty, exekutor),
b) vlastním nebo cizím jednáním příčícím se zákonu (např. nález ztracených dokumentů obsahujících obchodní tajemství, krádež, průmyslová špionáž).

Ochrana obchodnímu tajemství je poskytována i trestněprávními předpisy, konkrétním ustanovením o trestném činu zneužívání informací v obchodním styku. Podle tohoto ustanovení ten, kdo v obchodním styku zneužije informace nikoli veřejně přístupné, které získal z důvodu svého zaměstnání, povolání, postavení nebo své funkce může se dopustit trestného činu.

Je běžné, že v rámci činnosti podnikatele přicházejí do styku s předmětem obchodní tajemství jak zaměstnanci, tak i třetí osoby (např. externí poradci). Proto lze jen doporučit sjednat v příslušných smlouvách pod sankcemi povinnost mlčenlivosti.

- **Důvěrné informace**

Vedle pojmu obchodní tajemství se objevuje v obchodním zákoníku ještě pojem „důvěrné informace“. Důvěrné informace jsou chráněny ve spojení s činností statutárního či kontrolního orgánu obchodní společnosti nebo v rámci uzavírání smluv podnikatelem.

Každý člen statutárního orgánu či kontrolního orgánu společnosti (jednatel, člen představenstva či dozorčí rady apod.) je povinen dle § 194 odst. 5 obchodního zákoníku (resp. jeho přiměřeného užití) zachovávat mlčenlivost o důvěrných informacích

a skutečnostech, jejichž prozrazení třetím osobám, by mohlo společnosti způsobit škodu.

Co se týká ochrany důvěrných informací v rámci kontraktační činností podnikatele (§ 271 obchodního zákoníku), a to ve stadiu před uzavřením smlouvy, pak podmínkou pro přiznání informaci statut „důvěrné“ je její výslovné označení smluvní stranou jako důvěrné. Takové označení může být písemné či ústní a může se vztahovat k písemně (tj. i v elektronické podobě) i ústně poskytnuté informaci. Doporučujeme vždy z důvodu průkaznosti označovat za důvěrné informace písemně. Případně, je-li známo, že při jednání o uzavření obchodního či jiného kontraktu budou sdělovány potenciální druhé smluvní straně informace, které jsou podstatné a mohly by být jakýmkoliv způsobem zneužity, pak je vhodné pod hrozbou sankcí uzavřít písemnou dohodu o ochraně důvěrných informací. Shrnuto dle ustanovení § 271 obchodního zákoníku platí, že jestliže si strany při jednání o uzavření smlouvy navzájem poskytnou informace označené jako důvěrné, nesmí strana, které byly tyto informace poskytnuty, je prozradit třetí osobě a ani je použít v rozporu s jejich účelem pro své potřeby, a to bez ohledu na to, zda dojde k uzavření smlouvy, či nikoli. Za důvěrné lze tedy označit i informace, které nenaplňují znaky obchodního tajemství, ale podnikatel hodlá tyto informace držet v tajnosti. Pro definici obchodního tajemství je tedy rozhodující hledisko objektivní a pro definici důvěrných informací hledisko subjektivní.

V případě porušení mlčenlivosti ve vztahu k důvěrným informacím vzniká odpovědnost za škodu a povinnost k její náhradě (skutečná škoda a ušlý zisk) na straně toho, kdo tuto povinnost porušil.

- **Know-how**

Dle § 118 občanského zákoníku know-how patří mezi tzv. „jiné majetkové hodnoty“ a tvoří jej výrobní, technické, technologické a jiné zkušenosti, znalosti a dovednosti, které lze využít v podnikání. Know-how je většinou součástí obchodního tajemství (není tehdy, není-li vázáno na podnikatele) s tím, že obchodní tajemství může zahrnovat (vzhledem k tomu, že je širším pojmem) i jiné skutečnosti, které nespadají pod know-how. Vzhledem k tomu, je možné výše uvedené závěry vztahující se k ochraně obchodního tajemství vztáhnout přiměřeně i na kategorii know-how.

Pod pojem know-how lze s úspěchem podřadit i předměty průmyslového vlastnictví, jako jsou vynálezy (chráněné jinak patenty) a technická řešení (chráněná jinak užitými vzory). Nicméně na ochranu těchto předmětů nelze spoléhat, jelikož jejich uvedením na trh se stanou veřejně dostupnými a tudíž nechráněnými.

Ze shora uvedeného vyplývá, že je důležité, aby každý podnikatel střežil skutečnosti a informace, které mají pro jeho fungování a podnikatelský úspěch význam. Proto je na místě chránit obchodní tajemství, důvěrné informace i know-how již v okamžiku jejich existence a nikoliv teprve poté, kdy dojde k jejich nechtěnému prozrazení.

6.2.2 Nadnárodní legislativa chránící duševní vlastnictví

Bohužel neexistuje žádná mezinárodní organizace zaměřená na ochranu duševního vlastnictví před průmyslovou špionáží. Jednotlivé země mají své vlastní zákony a pravidla vztahující se k tomuto problému; různé země mají odlišnou legislativu, někdy přísnější, jindy tuto kriminalitu téměř zcela opomíjející. Přijmout legislativní změny je každopádně komplikovaným a časově náročným procesem; v zemích Evropské unie se o to snaží organizace jako ENISA. Firmy by však neměly spoléhat na pomoc ze strany vlád, legislativy apod., ale měly by své duševní vlastnictví a citlivé informace dokázat ochránit před útoky vlastními silami.[66]

6.3 Patentová ochrana

Již 7. ledna 1791, vydali revolucionáři v Paříži zákon, který měl chránit práva vynálezců, avšak jinou formou než dnes. Tento zákon povoloval řádnou průmyslovou špionáž mimo hranice státu. Zabezpečoval totiž „jednomu každému, kdo jako první vyrobí ve Francii zahraniční výrobek, stejnou zákonnou ochranu jako vynálezci“. Žádná jiná země na světě dodnes nepobízela své občany tak nepokrytě k průmyslové špionáži.[67]

Průmyslová špionáž zavdala podnět ke zrodu patentu jako opatření, které má vynálezci zabezpečit výlučné právo k využití vynálezu a zajistit, aby po vynálezcově smrti byl objev zachován pro společnost. Proto je v patentním spise uveden popis vynálezu.[68]

---

[66] *McAffee - Firmy by neměly spoléhat na pomoc ze strany vlád nebo legislativy* [online]. Ictsecurity.cz, 2010 [cit. 2011-12-12]. Dostupné z WWW: <http://ictsecurity.cz/10/06/1-prumyslova-spionaz/mcaffee-firmy-by-nemely-spolehat-na-pomoc-ze-strany-vlad-nebo-legislativy.html>.

[67] PIEKALKIEWICZ, J. *Historie světové špionáže : agenti, systémy, akce*. 1. vyd. Praha : Naše vojsko, 2004. s. 182. ISBN 80-206-0738-2.

[68] BERGIER, J. *Průmyslová špionáž.* 1. vyd. Praha : Orbis, 1974. s. 30-31. ISBN 605-22-826.

Před 75 lety (16. února 1937) získala americká chemická společnost DuPont patent na nylon. Vlákno jemné, pevné, pružné, odolné a první plně syntetické polyamidové vlákno, které bylo údajně pojmenováno podle měst New York a Londýn, se stalo jedním z jejích nejúspěšnějších produktů. Zlepšilo kvalitu štětin v zubním kartáčku, v němž se nejprve představilo, ale způsobilo převrat i v odívání a řadě dalších oborů.[69]

6.3.1 Patenty

Patenty jsou ochranné dokumenty, které se udělují na vynálezy. Majitel patentu má výlučné právo chráněný vynález využívat, poskytovat souhlas k využívání jiným osobám (což se děje licenční smlouvou) a má i právo převést patent na jinou osobu. Vynález, na který byl udělen patent, např. výrobek, zařízení k výrobě, chemická látka nebo výrobní postup, nesmí být bez souhlasu majitele vyráběn, nabízen k prodeji nebo využíván třetí osobou pro průmyslové nebo komerční účely. Pokud se patent týká výrobních postupů, majitel může třetím osobám zakázat tyto postupy používat. Zápovědní právo se vztahuje i na výrobky, které jsou přímým výsledkem chráněného postupu. Patenty jsou udělovány na vynálezy, které jsou nové, jsou výsledkem vynálezecké činnosti a jsou průmyslově využitelné. Z patentovatelnosti jsou vyloučeny objevy, vědecké teorie, matematické metody, pouhé vnější úpravy výrobků, plány, pravidla a způsoby vykonávání duševní činnosti, programy počítačů, pouhé uvedení informace. Patent nemůže být udělen na vynálezy, které jsou v rozporu s obecnými zájmy, zejména zásadami lidskosti a veřejné morálky, dále na způsoby prevence, diagnostiky a léčení lidí a zvířat, odrůdy rostlin a plemena zvířat a biologické způsoby jejich pěstování a šlechtění.[70]

Aby byl český vynález chráněný a nikdo nemohl po dobu 20 let recepturu jen tak ukrást, je potřeba každý rok uhradit předepsaný poplatek. A to za každý stát, ve kterém je chráněn. Zatímco v prvních letech je to tisícikoruna ročně, poplatky postupně narůstají. Za patnáctý rok už musí držitel patentu uhradit 14 tisíc korun a každý další

[69] Před 75 lety získal DuPont patent na nylon. *Technik.* 2012, č. 6/2012, s. IV. ISSN 1214-9802.
[70] *Patenty a užitné vzory* [online]. PatentCentrum, 2010 [cit. 2011-11-16]. Dostupné z WWW: <http://patentcentrum.cz/prehled-sluzeb/patenty-a-uzitne-vzory/>.

rok roste udržovací poplatek vždy o dva tisíce. Teprve po dvaceti letech je vynález volný a může ho využít každý odkaz (blíže viz příloha 2 a 3).[71]

6.3.2 Užitné vzory

Užitným vzorem, který je někdy nazýván „malý patent“ lze chránit technické řešení, které je nové, přesahuje rámec pouhé odborné dovednosti a je průmyslově využitelné. Za technická řešení se nepovažují objevy, vědecké teorie a matematické metody, pouhé vnější úpravy výrobků (sledující estetické účely), plány, pravidla a způsoby vykonávání duševní činnosti, programy počítačů a pouhé uvedení informace. Z ochrany jsou vyloučena technická řešení, která jsou v rozporu s obecnými zájmy, zejména zásadami lidskosti a veřejné morálky, dále odrůdy rostlin a plemena zvířat, jakož i biologické reprodukční materiály a způsoby výroby nebo pracovní činnosti. Předměty, které je možno chránit patentem a užitným vzorem jsou tedy srovnatelné, užitným vzorem oproti patentu však nelze chránit biologické reprodukční materiály a jakékoliv „způsoby“.

Užitné vzory se zapisují do rejstříku na základě tzv. registračního principu, kdy Úřad zapíše užitný vzor do rejstříku, aniž by zkoumal, zda předmět přihlášky vyhovuje kritériím novosti a tvůrčí úrovně, tj. zda je způsobilý k ochraně. V tom je hlavní rozdíl od systému patentového.

Vzhledem k tomu, že zápisem užitného vzoru do rejstříku Úřadu vzniká ochrana, jejíž účinky plně odpovídají účinkům patentu, lze užitným vzorem získat ochranu řešení způsobilého k zápisu mnohem rychleji než patentem. To má význam zejména u předmětů, které jsou v době zajišťování ochrany již připraveny k uvedení na trh, přičemž vzhledem k poměrně dlouhému řízení o udělení patentu by zůstaly dlouhou dobu (nebo případně vůbec) bez ochrany.

Bez souhlasu majitele zapsaného užitného vzoru nikdo nesmí technické řešení chráněné užitným vzorem při hospodářské činnosti vyrábět, uvádět do oběhu nebo upotřebit. Majitel zapsaného užitného vzoru, stejně tak jako u vynálezu, je oprávněn

[71] *Český hojivý vynález chrání patenty v Evropě i Americe. Má vydělat miliony* [online]. iDNES.cz, 2011 [cit. 2011-12-16]. Dostupné z WWW: <http://finance.idnes.cz/cesky-hojivy-vynalez-chrani-patenty-v-evrope-i-americe-ma-vydelat-miliony-1rh-/podnikani.aspx?c=A111207_111611_podnikani_sov>.

poskytnout souhlas k využívání předmětu užitného vzoru (licence) jiným osobám nebo na ně užitný vzor převést.[72]

6.3.3 Možnosti přihlášek patentů a užitných vzorů do zahraničí

Národní cestou přihlašovatel může přihlásit vynález přímo v každém státu, ve kterém chce mít vynález chráněn. K tomu je nutno v každém státu zvolit spolupracujícího patentového zástupce, který je oprávněn zastupovat přihlašovatele před příslušným úřadem, přeložit popis vynálezu, patentové nároky a anotaci do úředního jazyka tohoto úřadu a zaplatit poplatky. Veškeré informace týkající se přihlášení vynálezu, vlastního řízení o přihlášce a výše poplatků včetně lhůt k jejich placení pak podá zvolený zástupce.

Cestou „Evropského patentu“ v případě, pokud si přihlašovatel přeje získat patent pouze pro státy Evropské unie, pak je možno podat žádost o evropský patent u Evropského patentového úřadu (EPO) v Mnichově. Tak jednou přihláškou lze získat ochranu ve všech smluvních zemích Evropské patentové organizace (EPO). Také v tomto případě musí mít přihlašovatel ze země, která není členem EPO, zástupce oprávněného zastupovat před EPO. Popis vynálezu, patentové nároky a anotace musí být přeloženy do jednoho z úředních jazyků EPO, což je angličtina, němčina a francouzština. Ve stejném jazyku pak musí být formulář žádosti o evropský patent.

Cestou mezinárodní přihlášky – PCT pokud se týká mezinárodní přihlášky podané podle Smlouvy o patentové spolupráci (PCT), pak jedinou přihláškou podanou v Úřadu průmyslového vlastnictví (ÚPV) můžete získat ochranu ve všech smluvních státech (k 1. 1. 2000 jich bylo 106) a čtyři regionální patenty (včetně evropského). I v tomto případě však musí být přihlašovatel zastoupen, a to patentovým zástupcem nebo advokátem. Mezinárodní přihláška se podává v ÚPV v angličtině, němčině nebo francouzštině, ve stejném jazyce pak musí být i žádost o mezinárodní přihlášku. Od 1. 1. 1999 je možno podat přihlášku i v češtině s tím, že je nutno do jednoho měsíce od podání mezinárodní přihlášky předložit překlad do jednoho ze shora uvedených jazyků.[73]

---

[72] *Patenty a užitné vzory* [online]. PatentCentrum, 2010 [cit. 2011-11-16]. Dostupné z WWW: <http://patentcentrum.cz/prehled-sluzeb/patenty-a-uzitne-vzory/>.

[73] *Patenty a užitné vzory* [online]. PatentCentrum, 2010 [cit. 2011-11-16]. Dostupné z WWW: <http://patentcentrum.cz/prehled-sluzeb/patenty-a-uzitne-vzory/>.

V roce 2012 podepsali ICT Unie (Information and Communication Technology) a Úřad průmyslového vlastnictví (ÚPV) memorandum o spolupráci. Oba subjekty budou spolupracovat mj. na rozvoji a podpoře podnikání zejména malých a středních podniků, a to prostřednictvím využívání systému ochrany práv průmyslového vlastnictví. Hlavním cílem společných aktivit ICT Unie a ÚPV je účinně přispět k trvalému zvyšování konkurenceschopnosti ČR.[74]

6.4 Průmyslová protišpionáž

Firmy se musí smířit s tím, že je nutné investovat do rozvoje konkurenčního zpravodajství, investovat a vychovávat specialisty pro tento nový obor. V těchto firmách by se měl klást důraz na vznik nových oddělení zabývajících se touto problematikou a jejich zaměstnancům by měl být zajištěn ten nejlepší přístup k informacím. Zároveň by ale firmy neměly zapomínat ani na ochranu svého Know-how, tedy nabytých znalostí, poznatků a zkušeností z vývoje nových technologií, výroby a produktů, které nepodléhají patentům a licencím.

Už Gustav Krupp pochopil význam průmyslové špionáže a v roce 1920 si zřídil vlastní organizaci pro tyto účely. Podařilo se jí například zachránit před Francouzi těžká děla Max, z kterých Němci v roce 1918 ostřelovali Paříž. Zvlášť nutné je vyzdvihnout několik amerických organizací, a sice Pinkertonovu, agentury Globe a Intersat. Odhaduje se, že koncem 19. století měly soukromé policejní instituce amerických podnikatelů asi 150 000 agentů. Pinkertona a Kruppa lze právem označit za duchovní otce a iniciátory moderní průmyslové protišpionáže. Také Anglie má svou protišpionážní organizaci, kterou je skupina M.I.S v Londýně, financovaná zřejmě prostřednictvím Intelligence Service. Snahou této organizace je provádět spíše prevenci a seznamovat zainteresované pracovníky se všeobecnými metodami a technikami ochrany průmyslu. Každý bezpečnostní systém je sice finančně náročný, ale na druhé straně se podniku vyplatí, zvláště tam, kde se jedná o choulostivou výrobu. Rozsah průmyslové špionáže by bylo možné podstatně snížit i tím, kdyby autoři vynálezů, průmyslových a užitných vzorů, počítačových programů a další tvůrčí pracovníci byli

[74] ICT Unie a ÚPV podepsaly memorandum. *Technik.* 2012, č. 2/2012, s. III. ISSN 1214-9802.

po zásluze odměňováni a nemuseli výsledky své tvůrčí práce prodávat jinému, kdo je řádně ohodnotí, i za cenu, že se jejich dílo dostane do zahraničí.[75]

V oblasti podnikové bezpečnosti a průmyslové protišpionáže je třeba zvlášť vyzvednout pět amerických organizací, totiž Burnsovu, Pinkertonovu a Wackenhutovu agenturu, jakož i agentury Globe a Interstat.

Pinkertonova agentura je samozřejmě institucí klasickou, s níž se můžeme setkat jak v článcích starých čísel novin, tak i v učebnicích dějepisu.[76]

Allan Pinkerton, dvaačtyřicetiletý Skot, pracoval v Chicagu jako policejní detektiv, ale roku 1850 odešel a založil si vlastní detektivní kancelář Pinkertonovu národní detektivní agenturu, která se specializovala na stíhání vlakových lupičů. Na jejím ústředí v Chicagu visel štít s obřím okem a firemním sloganem „My nikdy nespíme“. Toto heslo odráželo jeho smělou ctižádost i domýšlivé mínění o vlastní osobě, které bylo pro Pinkertona příznačné.[77]

Anglie má také svou protišpionážní organizaci, kterou je skupina M.I.S., zřejmě financován Intelligence Service.

Francie pochopitelně nezůstává pozadu a má přinejmenším jednu instituci, která se profesionálně zabývá průmyslovou protišpionáží. Zmínka o této organizaci se objevila ve stručné a poněkud tajemně znějící poznámce v 633. čísle časopisu „Enterprise“ dne 29. října 1967: „Je to poprvé, co ve Francii nabízejí bezpečnostní poradny své služby podnikům“. Francouzský orgán pro průmyslovou protišpionáž se jmenuje P.S.I. (Protection des Secrets Industriels) – Ochrana průmyslových tajemství.[78]

Francouzská domácí tajná služba *Direction de la Surveillance du Territoire* (DST) je organizačně přičleněna k policii a podléhá ministru vnitra. DST má ve 22 francouzských oblastech poradní zařízení, která mají chránit francouzské podniky před průmyslovou špionáží. Tato celoplošná síť má v kompetenci nejenom zbrojní průmysl, ale ochraňuje i francouzský automobilový průmysl, farmaceutické podniky a telekomunikační firmy.[79]

---

[75] ŠPINDLER, K. *Průmyslová špionáž co o ní víme?* [online]. Technický týdeník, 2006, roč. 54, č. 4 [cit. 2011-10-12]. ISSN 0040-1064. Dostupné z WWW: <http://www.techtydenik.cz/detail.php?action=show&id=907&mark=>.

[76] BERGIER, J. *Průmyslová špionáž.* 1. vyd. Praha : Orbis, 1974. s. 175. ISBN 605-22-826.

[77] VOLKMAN, E. *Dějiny špionáže : tajný svět špionů, vyzvědačů a rozvědčíků od starověku až do doby po 11. září.* 1. vyd. Praha : Fortuna Libri, 2008. s. 97-98. ISBN 978-80-7321-387-9.

[78] BERGIER, J. *Průmyslová špionáž.* 1. vyd. Praha : Orbis, 1974. s. 178. ISBN 605-22-826.

[79] ULFKOTTE, U. *Válka v temnotách : skutečná moc tajných služeb.* 1. vyd. Praha : Ikar, 2007. s. 264-265. ISBN 978-80-249-0959-2.

Je třeba si uvědomit, že zajišťování bezpečnosti je úkol, který se nedá řešit improvizací. Pod výrazem „průmyslová protišpionáž“ se skrývají především aktivity v zajišťování bezpečnosti. Podstatou protišpionáže je totiž především snaha docílit, aby nepřátelští špióni podávali svým šéfům falešné informace. Posláním šéfa bezpečnostní služby v průmyslovém podniku není chytat špióny – právě tak, jako není úkolem odborníka pro požární ochranu hasit požáry. V obou případech jde totiž o akce preventivní. Odborník pro protipožární ochranu zavádí v místnostech a budovách opatření, která mají zabránit požáru. Odborník pro zajištění bezpečnosti v průmyslu zase organizuje pohyb informací tak, aby nedocházelo k jejich vyzrazení.[80]

[80] BERGIER, J. *Průmyslová špionáž.* 1. vyd. Praha : Orbis, 1974. s. 180-181. ISBN 605-22-826.

6.5 Prosperující firma a bezpečnost informací

Někdy v této souvislosti trochu nadneseně hovoříme o firemní kontrašpionáži nebo o ochraně proti špionáži konkurence.

6.5.1 Ochrana před únikem informací (proti firemní špionáži)[81]

- **Ochrana know how – intelektuálního majetku firmy:**
  - ochrana informací o přípravách, průběhu a výsledcích výzkumu a vývoje,
  - ochrana informací z oblasti licenční problematiky,
  - ochrana patentů, vynálezů a ochranných známek,
  - ochrana informací o provozních (výrobních) technologiích a postupech,
  - ochrana informací o organizačních a organizačně-technických systémech,
  - ochrana softwarového vybavení apod.
- **Ochrana informačních systémů:**

  a) ochrana písemných dokumentů:

  Představuje velice významnou oblast realizace firemní bezpečnosti. Jde o to, aby bylo stanoveno:
  - které písemnosti jsou utajované či důvěrné,
  - kdo má k utajovaným a důvěrným informacím přístup a v jakém rozsahu,
  - stanovení režimu zpracování, evidence a ukládání, jakož skartování a archivování utajovaných a důvěrných písemností,
  - za jakých podmínek mohou být písemnosti přenášeny a převáženy mimo objekt firmy apod.

  Úkolem soukromých detektivů je především:
  - zajistit kontrolu dodržování režimu práce s důvěrnými a utajovanými písemnostmi,
  - detektivní prověrky osob, které mají pracovat nebo pracují s utajovanými a důvěrnými písemnostmi,
  - detektivní rozpracování osob, u nichž je důvodné podezření, že porušují režimová opatření platná pro práci s důvěrnými a utajovanými firemními písemnostmi.

---

[81] BRABEC, F. *Ochrana bezpečnosti podniku.* 1. vyd. Praha : EUROUNION s.r.o., 1996. s. 160-163. ISBN 80-85858-29-0.

b) *ochrana počítačových databází:*

Komplexní systém ochrany dat (informací) v počítačích je ucelený komplex technických prostředků, funkcí a služeb systému, který uživateli zajistí ochranu dat před jejím zneužitím, ztrátou apod. Takový systém se musí starat o ochranu před:

- zneužitím dat,
- počítačovými viry,
- zneužitím nepotřebných dat,
- zneužitím archivovaných dat,
- zneužíváním přenášených dat…

Hovoříme-li o ochraně počítačových databází, je třeba mít na zřeteli především počítačové sítě. Odposlouchávání komunikace lze snadno a neoprávněně získat důvěrné informace. Zvláště nebezpečná je možnost tímto způsobem získat přihlašovací heslo uživatele.

- **Ochrana ostatních informačních systémů:**

  Ostatními informačními systémy můžeme rozumět například elektronické bezpečnostní systémy

- **Ochrana ekonomických informací:**

  Předmětem podnikatelských aktivit je nesporně činnost směřující ať bezprostředně nebo následně k obchodním aktivitám. To vše přímo souvisí s ekonomikou firmy. Proto takové informace dotýkající se obchodních aktivit a dalších ekonomických výsledků firmy jsou objektem, k jejichž získání směřují různé aktivity konkurenčního boje. Není sporu o tom, že tyto informace mají pro podnikatelský subjekt i pro jeho konkurenci značný význam. Proto jejich ochrana musí stát v popředí zájmu detektivní služby zajišťující ochranu bezpečnostních zájmů firmy. Ochrana ekonomických informací souvisí s realizací:

- režimové ochrany ekonomických informačních systémů,
- detektivních prověrek osob, které v rámci takového systému pracují s důvěrnými a utajovanými skutečnostmi nebo které by s ohledem na přístup k systému mohly svými zásahy zkreslovat a jinak ohrožovat věrohodnost takovýchto informací,
- detektivního rozpracování pracovníků, u nichž na základě prověrek či informací z jiných informačních zdrojů vzniklo podezření z možného úniku ekonomických informací nebo z jejich negativního ovlivňování,
- detektivních dezinformačních opatření transformovaných vybudovanými dezinformačními kanály ke konkurenci.

- **Ochrana personálních informací:**

  Personální aspekt se prolíná do všech oblastí činnosti podnikatelského subjektu i bezpečnostních činností. Proto také informace o zaměstnancích firmy či pracovnících bezpečnostní služby jsou cennou informací pro konkurenci. Takovéto informace umožňují konkurenci hledat a nacházet slabé články řetězu v různých systémech, takovéto osoby získávat, korumpovat a jinak na ně působit, aby pracovaly ve prospěch konkurence. Proto ochrana informací o vlastních zaměstnancích, včetně pracovníků bezpečnostní služby, je významnou součástí komplexní bezpečnosti firmy.

6.6 Etické kodexy firem

Obsah „etiky“ není lehké jednoznačně definovat a pohled každého na etiku může být velmi rozdílný. Právo nemůže (při obrovském množství situací a problémů) poskytnout do detailu odpověď na každou otázku. Otevírá se tak prostor pro podnikatelskou etiku. Díky globalizaci přichází do kontaktu různé kultury a je důležité najít společný jazyk pro řešení problémů. Čím je větší rozsah ekonomických aktivit, tím větší je také morální zodpovědnost. Samotné podnikání firem nemá definovány řádné normy, nebo všeobecně uznávané normy pro etické standardy, které stanovují styl etického jednání firem.

Úkolem veřejného sektoru v etické oblasti je vytvářet komplexní podmínky pro to, aby podnikatelská sféra realizovala svoji ekonomickou činnost při dodržování určitých etických zásad.[82]

Stále více podniků shrnuje své přesvědčení o etickém řízení do různých etických kodexů. V pokročilých podnicích se netýkají jen a výlučně etiky, ale svazují v jedno etické zásady s výkonností. Často se etický kodex tak stává vlastně pracovním kodexem, souborem zásad, podle nichž se v podniku, v instituci mají vykonávat práce.

Obvyklý obsah poslání podniku a kodexu dobrého chování zahrnuje:

- Odpovědnost za produkci (výrobky, služby),
- Vztah k zákazníkům,
- Vztah k dodavatelům,
- Vztah k zaměstnancům,

[82] DUŠEK, J., PROTIVA, V. *Veřejná ekonomika.* České Budějovice : Vysoká škola evropských a regionálních studií, 2007. s. 47. ISBN 978-80-86708-43-0.

- Vztah k místní správě a občanským zájmům,
- Vztah k vlastníkům (opatřovatelům kapitálu),
- Sdílené hodnoty (stakeholding) a etiku (morálku).

Etické kodexy mohou mít různou podobu i obsah. Například mohou vytyčovat dosud nedosažený, avšak dosažitelný etický ideál. Mohou zvláště vytyčovat „na čem se sjednocujeme“ atp. Jazyk těchto prohlášení bývá slavnostní, mírně nadnesený, aby bylo hned cítit, že to, co proklamuje, má hluboké oprávnění.[83]

[83] JIRÁSEK, J. *Benchmarking a konkurenční zpravodajství.* 1. vyd. Praha : Profess Consulting, s.r.o., 2007. s. 81-82. ISBN 978-80-7259-051-3.

7 Případy průmyslové špionáže globálního konkurenčního prostředí

Největší úctu si vždy zasluhovali bezpečnostní a vojenské technologie, což je typický trend, který však během „studené války“ byl překonán technologickou špionáží skrze všechny vědní obory. Skutečný rozsah a důsledek průmyslové špionáže popisuje hlášení dvojitého agenta KGB, který prezentoval, že KGB v roce 1979 zcizila v západních zemích na 58 000 dokumentů a 5 800 průmyslových vzorů, které umožnili zahájit 162 nových projektů a urychlily více jak 1 200 již existujících výzkumů.

Po skončení „studené války“ došlo k značnému uvolnění, které se samozřejmě odrazilo i na volnějším přístupu k průmyslovým a technologickým tajemstvím, čehož využily některé firmy či speciální sekce státních zpravodajských agentur (např. francouzská DGSE - *Direction Générale de la Sécurité Extérieure* v USA). Přesto lze v tomto období cítit silný přesun tohoto druhu špionáže ze státního aparátu do komerčního sektoru.

Ovšem vedle zesílení útoků proti jednotlivým firmám a organizacím vznikají i snahy o lepší a kvalitnější zabezpečení firemních tajemství. Vznikají tak auditorské a bezpečnostní firmy, které mají za úkol střežit technologická tajemství ve všech podobách – od technických výkresů po projektová data v elektronické podobě.[84]

V moderním světě špionáže musí dobrodružství ustoupit vědě a technice. Mnohé technické vynálezy vděčí za svůj vznik špionáži, protože původně byly vyvinuty pro její potřeby. Jeden příklad za všechny: vesmírní technika. Poté, co v roce 1957 tehdejší Sovětský svaz vyslal na oběžnou dráhu kolem Země první umělou družici, špionáži se okamžitě otevřely nové možnosti, které byly obratem využity. Špionážní satelity se staly osvědčenou zbraní studené války a používají se dodnes.[85]

7.1 Airbus versus Boeing

V roce 1994 byla odposlouchávána komunikace mezi aeroliniemi Saudské Arábie a společností Airbus. Zprávy z odposlechů byly zasílány americké firmě Boeing,

---

[84] *Metody špionáže: Průmyslová špionáž* [online]. Specialista.info, 2006 [cit. 2011-11-04]. Dostupné z WWW: <http://www.magazin.specialista.info/view.php?cisloclanku=2006013001>.
[85] REITZ, M. *Špioni, kteří měnili svět : od faraonů po Matu Hari.* 1. vyd. Praha : Víkend, 2008. s. 236. ISBN 978-80-86891-80-4.

která kontrakt za 6 miliard amerických dolarů nakonec vyhrála. Tento případ je zajímavý svým politickým kontextem.

Zdaleka nejsilnější zbraní, alespoň podle expertů, je špionážní systém Echelon, který vznikl ve spolupráci USA, Velké Británie a dalších zemí po druhé světové válce a přibližně od roku 1978 sloužil k monitorování telefonních hovorů. USA a další zúčastněné země existenci Echelonu po mnoho let popíraly a doposud se jedná o jeden z nejutajovanějších projektů na světě. V 90. letech minulého století se však kolem něho rozvířila ostrá debata mezi Evropskou unií a USA, protože byl podezříván z průmyslové špionáže ve prospěch amerických podniků. EU dokonce zřídila speciální komisi, která se jeho činností zabývá. Ze zprávy, kterou tato komise vydala, vyplynulo, že sice neexistuje jasný a nevyvratitelný důkaz, že USA Echelon používají pro průmyslovou špionáž, nicméně v některých případech je toto podezření oprávněné. Například telefonní linky evropského výrobce letadel Airbus Industrie byly sledovány v roce 1994, během jeho vyjednávání o kontraktu v hodnotě 6 miliard dolarů se saúdskoarabskou vládou a leteckou společností.[86]

7.2 Informace od francouzské tajné služby

Více než u ostatních západních služeb je v popředí zájmu služby DGSE ekonomická špionáž. Sídlo francouzské tajné služby se nachází v Paříži na bulváru Mortier proti bazénu des Tourelles. Novináři si zvykli označovat tak tajnou službu. Profesionálové však nazývají ústředí jinak: „bouda“, „barák“, „bejvák“.[87]

Aktivitu v této oblasti dokumentují některé případy z minulých let. Tak například firma Siemens přišla v roce 1994 o zakázku v hodnotě čtyř miliard marek na dodávku vlakových souprav ICE do Jižní Koreje. Příslušné informace předtím vypátrala francouzská tajná služba DGSE a předala je Siemensovu konkurentovi, firmě GEC Alsthom, která nakonec do Jižní Koreje – na místo německého ICE – dodala francouzský vlak TGV. Tento typ špionáže má ve Francii dlouhou tradici.

Už *Office National du Commerce Extériuer* před první světovou válkou členili podle geografických hledisek a skupin zboží. Každý francouzský vývozce měl mít možnost získat od této instituce cenné podněty a opatřit si materiály o svých

[86] *Americká špionáž náprava selhání* [online]. Computerworld.cz, 2000 [cit. 2011-11-10]. Dostupné z WWW: <http://computerworld.cz/archiv/americka-spionaz-naprava-selhani-17263>.
[87] FALIGOT, R., KROP, P. *"Bazén" : francouzská tajná služba (1944-1984)* Praha : Themis, 1998. s. 4. ISBN 80-85821-53-2.

konkurentech a cílové zemi. Na tom se nic nezměnilo dodnes. Ředitel francouzské kontrašpionáže při domácí tajné službě DST roku 1995 řekl, že šest z deseti případů, které jeho instituce zpracovává, patří do oblasti ekonomické špionáže. Zamlčel však přitom, že sama DGSE je ve Spojených státech, ve Velké Británii a v Německu na tomto poli organizací zdaleka nejaktivnější.

Roku 1990 otevřela DGSE nové „speciální oddělení č. 7" pro „rozsáhlé zakázky do jiných států". V tomto oddělení se přes dvacet odborníků DGSE zabývá tím, jak by získali co největší množství informací o zhruba tisíci nejdůležitějších průmyslových bossích světa; s těmito informacemi je pak možno buď udělat dojem při vyjednávání o zakázkách – anebo v případě nabytí lze s jejich pomocí trochu zatlačit stylem ne podobným vydírání.[88]

7.3 Aféra Leuna

Na aféře Leuna je zvlášť dobře vidět souhra francouzské mocenské politiky, hospodářství a tajných služeb. Nelze si nepovšimnout politické aféry, když ropný koncern Elf převzal v souvislosti s privatizací majetku NDR od Institutu pro správu majetku (*Treuhandanstalt*) roku 1990 rafinerii v Leuně a benzinové pumpy Minol. Milionové úplatky při tom plynuly i do kapes německých politiků a stran.[89]

Na „seznamu" údajně figurují nejen bývalý ministři vlády exkancléře Helmuta Kohla ministr dopravy Krause a ministr bez portfeje a šéf Kohlova kancléřského úřadu Bohl, ale také náměstci ministrů obrany a financí Agnes Hürlandová-Büningová a Manfred Carstens, jakož i někdejší zemský premiér Saska-Anhaltska, kde se Leuna nachází, Werner Münch.

Následně se Šéf německé Křesťansko-demokratické unie (CDU) Wolfgang Schäuble omluvil všem německým občanům za nezákonné financování strany a za to, že strana zklamala důvěru voličů.[90]

---

[88] ULFKOTTE, U. *Válka v temnotách : skutečná moc tajných služeb.* 1. vyd. Praha : Ikar, 2007. s. 285. ISBN 978-80-249-0959-2.
[89] ULFKOTTE, U. *Válka v temnotách : skutečná moc tajných služeb.* 1. vyd. Praha : Ikar, 2007. s. 289. ISBN 978-80-249-0959-2.
[90] *Schäuble se omluvil Němcům* [online]. iDNES.cz, 2000 [cit. 2011-10-25]. Dostupné z WWW: <http://zpravy.idnes.cz/schauble-se-omluvil-nemcum-d0v-/zahranicni.aspx?c=000118_184350_zahranicni_jpl>.

Francouzští agenti jsou podle všech známek nablízku i při prodeji firem. Aspoň v případě takzvané aféry *Leuna* patřilo během vyjednávání s firmou Leuna mezi poradce a zplnomocněnce firmy Elf pět pracovníků DGSE, které vedl plukovník DGSE Pierre Léthier. Na aféře *Leuna* a na historii naftového koncernu Elf je zvlášť dobře vidět souhra francouzské (mocenské) politiky, hospodářství a tajných služeb.

Státní podnik Elf, založený roku 1963 generálem de Gaullem, sloužil od poloviny šedesátých let k tomu, aby poskytoval perfektní krytí francouzským agentům působícím v cizině. Prvním ředitelem mocného podniku byl zakladatel DGSS (*Direction général des services spéciaux* – zahraniční tajná služba, která existovala v letech 1943 a 1944) a někdejší ministr obrany Pierre Guillaumat. Prostřednictvím firmy Elf dostávali skrytou podporu zpravidla pofrancouzští afričtí politici a přes Elf se do Afriky dodávaly i zbraně (maskované jako výbava pro těžbu nafty).[91]

7.3.1 Prvopočátky kauzy Leuna

Předseda německé opoziční Křesťanskodemokratické unie (CDU) Wolfgang Schäuble zůstal i po krizovém zasedání vedoucích grémií strany ve své funkci. To byl hlavní výsledek narychlo svolané mimořádné schůze vedení CDU, které se znovu zabývalo důsledky neustále se prohlubujícího finančního skandálu, který vyšel na povrch a ohrožoval samu politickou stabilitu ve Spolkové republice na konci roku 1999.

Svého čestného předsednictví se kvůli aféře vzdal bývalý předseda strany Helmut Kohl.

Schäuble nabídl v úvodu zasedání své odstoupení, širší předsednictvo strany mu však jednomyslně vyjádřilo důvěru. Generální tajemnice Angela Merkelová potvrdila informace, které předtím pronikly z jednacích kruhů, že v případě Schäubleho odstoupení podá užší vedení rovněž kolektivní demisi.

Čtyřbodové usnesení obsahuje kromě vyjádření důvěry dosavadnímu vedení v čele se Schäublem také omluvu židovským spoluobčanům za nepřijatelné zdůvodnění ilegálních převodů peněz v hesenské zemské organizaci strany údajnými dary židovských exulantů. Dále obsahuje úkol připravit pro dubnový sjezd strany návrh změn stanov tak, aby se v budoucnu nemohly opakovat nyní odhalené finanční

[91] ULFKOTTE, U. *Válka v temnotách : skutečná moc tajných služeb.* 1. vyd. Praha : Ikar, 2007. s. 288. ISBN 978-80-249-0959-2.

nesrovnalosti, a konstatování, že bývalý kancléř Helmut Kohl porušuje svým odmítáním přispět k objasnění skandálu povinnosti čestného předsedy.

V souvislosti s privatizací petrochemického kombinátu ve východoněmecké Leuně uvádí středeční německý list Stuttgarter Nachrichten jména významných politiků Křesťanskodemokratické unie (CDU) zabředlé v rozsáhlém finančním skandálu. Jsou mezi nimi i bývalí ministři vlády exkancléře Helmuta Kohla Günther Krause a Friedrich Bohl, kteří možná dostali úplatky za prodej rafinerie francouzskému koncernu.

Deník se odvolává na německé vyšetřovatele, na něž se obrátili jejich kolegové ze Švýcarska v šetření souvisejícím s aférou.

Podle zjištění švýcarských úřadů, jež zkoumají peněžní toky při prodeji rafinerie koncernu Elf Aquitaine, pomáhali politikové CDU obchodníkovi Dieteru Holzerovi, který prý hraje v prodeji klíčovou úlohu. Podle televize ZDF přes jeho firmu v Lichtenštejnsku Delta International plynuly úplatky ve výši 50 miliónů marek. Švýcarská prokuratura Holzera podezírá z podvodu, padělání listin a praní peněz.

Kohl byl znovu naléhavě vyzván, aby zveřejnil jména dosud anonymních dárců, kteří v uplynulých letech přispívali do stranické pokladny, aniž byly jejich dary řádně evidovány. Bylo mu zároveň doporučeno, aby se - dokud tento požadavek nesplní - čestného předsednictví v CDU prozatím vzdal, což Kohl také učinil.

Schäuble uvedl, že při obtížných, ale otevřených a intenzivních jednáních dali všichni členové vedení strany přednost odpovědnosti vůči celé zemi a zachování demokracie v ní před osobními zájmy. Oznámil, že aférou se bude vedení znovu zabývat v neděli, kdy by mělo projednat zprávu auditorské firmy o výsledcích prověrky stranických financí.

Finanční aféru CDU odstartoval před Vánoci bývalý spolkový kancléř Helmut Kohl, když v televizním interview přiznal, že v letech 1993-98 přijal 1,5 až dva miliony marek na darech v rozporu se zákonem. Zdůvodnil to tím, že dárcům dal čestné slovo, že jejich jména udrží v tajnosti, a údajnou potřebou pomoci východoněmeckým organizacím strany ve finanční tísni (blíže viz příloha 1).[92]

---

[92] *Schäuble se omluvil Němcům* [online]. iDNES.cz, 2000 [cit. 2011-10-25]. Dostupné z WWW: <http://zpravy.idnes.cz/schauble-se-omluvil-nemcum-d0v-/zahranicni.aspx?c=000118_184350_zahranicni_jpl>.

7.4 Průmyslová špionáž v Renaultu

Hned v prvních týdnech roku 2011 strhávala pozornost médií i politiků z celého světa francouzská automobilka Renault kvůli špionážní aféře nebývalých rozměrů. Ve hře byly čtyři miliardy eur investované do vývoje nového elektromobilu, úplatky na tajných kontech ve Švýcarsku a Lichtenštejnsku a především nová „ekonomická válka", jak situaci ve špehované automobilce pojmenoval francouzský ministr průmyslu Eric Besson.

7.4.1 Podezřelí manažeři

První zprávy hovořily o tom, že minimálně tři klíčoví zaměstnanci podílející se na vývoji nových modelů Renaultu vynášeli z podniku klíčové informace a prodávali je konkurenčním firmám z Číny. Byť sama asijská velmoc jakoukoli vinu popírala, diskuse o rostoucí roli průmyslové špionáže a nebezpečí, které s sebou rozvoj informačních technologií a s ním spojené sofistikovanější metody špionů přinášejí, nabíraly na obrátkách. Vyzrazení informací se pravděpodobně týká elektromobilů.

Přestože ani nyní nejsou známy detaily celé kauzy, francouzský ministr průmyslu Eric Besson v rozhovoru pro RTL označil situaci za velmi vážnou a zmínil se i o ohrožení francouzského průmyslu. Nevyhnul se ani použití termínu ekonomické války, které podle něj na situaci přesně sedí. Renault se svým japonským partnerem Nissan investovaly do vývoje elektromobilů čtyři miliardy eur (99 miliard korun). Pouze vývoj baterie přišel obě automobilky na 1,5 miliardy eur (37 miliard korun). Ve vývojovém centru nedaleko Paříže pracuje 1 700 techniků.[93]

Stovky tisíc eur na konta ve Švýcarsku a Lichtenštejnsku posílala čínská firma, tvrdí Le Figaro s odvoláním na informace vyšetřovatelů.

Dva ze tří vysoce postavených činitelů automobilky Renault, obviněných z průmyslové špionáže, mají tajná konta ve Švýcarsku a Lichtenštejnsku. S odvoláním na informace vyšetřovatelů to ve svém úterním vydání píše francouzský deník Le Figaro.

Na účtu v Lichtenštejnsku je údajně 130 000 eur, na švýcarském kontě 500 000 eur. Podle informací vyšetřovatelů a soukromých detektivů, které Renault najal již

[93] VAIDIŠOVÁ, K. *Renault zradili vlastní manažeři* [online]. IHNED.cz, 2011 [cit. 2012-03-04]. Dostupné z WWW: <http://byznys.ihned.cz/c1-49260100-renault-zradili-vlastni-manazeri>.

v srpnu loňského roku, kdy přišlo na obviněné udání zevnitř firmy, na tyto účty posílala peníze čínská firma se sídlem v Pekingu, Power Grid Corporation.

Tato firma se specializuje na distribuci elektřiny. Ve snaze zamaskovat tok peněz finance putovaly přes banky v Šanghaji a na Maltě, uvádí Le Figaro.

„Je to práce profesionálů," řekl v listu Le Monde druhý muž automobilky, provozní ředitel Patrick Pelata. Firma je podle něj obětí organizované mezinárodní sítě.

Podle Pelaty unikla data týkající se nákladů a ekonomického modelu programu. Hlavní prvky technologie, která zahrnuje kolem 200 patentů, ale zůstaly utajeny. Program elektrovozu je klíčovým prvkem strategie, do níž Renault investuje miliardy eur spolu s japonskou partnerskou skupinou Nissan.

Zdroje Le Figaro ale o jeho tvrzení pochybují. „Výrobce zatím pořádně neví, jaké informace se podařilo prodat," tvrdí. Dříve deník informoval, že šlo o data týkající se nové technologie baterie do elektromobilu, která by měla být uvedena na trh po roce 2012.

Čína popírá jakoukoli účast svých firem. „Tato obvinění jsou nezodpovědná a nepodložená," prohlásil 3. ledna 2011 mluvčí čínského ministerstva zahraničních věcí, Hong Lei.

Trojici manažerů čeká 14. ledna 2011 předběžné slyšení a zřejmě i formální výpověď z firmy, která na ně následně podá žalobu. Dále tak uvolní ruce ve vyšetřování francouzské policii.[94]

7.4.2 Průmyslová špionáž jako nástroj manipulace a podvodu

Případ podkopal vztahy Francie s Čínou, protože vyšetřovatelé podle vládních zdrojů zkoumali možné spojení špionážních aktivit s Čínou.

Francouzská automobilka Renault připustila, že v údajném případu průmyslové špionáže se možná stala jen obětí manipulace a podvodu. Ministryně hospodářství a financí Christine Lagardeová prohlásila, že pokud se obvinění ze špionáže nepotvrdí, bude z toho muset Renault vyvodit náležité důsledky.

Renault v lednu odvolal tři manažery a podal na neznámé pachatele žalobu za průmyslovou špionáž zaměřenou na jeho program elektrického automobilu. Případ

---

[94] VOLF, T. *Špionáž v Renaultu: Podezřelí manažeři mají v cizině tajná konta s miliony* [online]. IHNED.cz, 2011 [cit. 2011-11-03]. Dostupné z WWW: <http://byznys.ihned.cz/c1-49439160-spionaz-v-renaultu-podezreli-manazeri-maji-v-cizine-tajna-konta-s-miliony>.

podkopal vztahy Francie s Čínou, protože vyšetřovatelé podle vládních zdrojů zkoumali možné spojení špionážních aktivit s Čínou.

V případu padala velmi silná slova, francouzský ministr průmyslu Erik Besson mluvil dokonce o „ekonomické válce“.

Provozní ředitel Renaultu Patrick Pelata v listu Le Figaro prohlásil, že „určitý počet indicií nás vede k pochybnostem“. Podle něj existují dvě možnosti - buď jde skutečně o špionáž a manažeři dokonale chrání své zdroje, „nebo je Renault obětí manipulace, jejíž povahu neznáme, avšak mohlo by jít o podvod“.

Provozní šéf Renaultu dodal, že ve druhém případě by navrhl obviněné manažery vzít zpět a jakoukoli nespravedlnost napravit třeba i vyvozením důsledků pro nejvyšší vedení. „Až vyšetřování skončí, přijmeme všechny důsledky až po nejvyšší úroveň firmy, to znamená včetně mě,“.

Lagardeová v rozhovorů pro rozhlasovou stanici RMC vyzvala k urychlenému vyřešení případu a přijetí „všech důsledků“. „Dnes je důležité dostat se k pravdě, a to rychle, a pokud by se podezření ukázala jako nepodložená, nechť je spravedlnosti učiněno zadost, ať je obnovena důvěra a vyplaceno odškodné,“ uvedla ministryně, „Nemělo by se střílet bez míření a obviňovat bez důkazů,“ dodala.

Francouzská tajná služba nyní podle právníka Renaultu Reinharta stále vyšetřuje existenci bankovních účtů ve Švýcarsku a Lichtenštejnsku. Existence těchto účtů je klíčovou součástí obvinění, a dokud se nenajdou, zřejmě zůstane obvinění bez důkazů. Všichni tři manažeři jakoukoli vinu popírají.[95]

7.5 Lex Nokia

Nokia má ve finské ekonomice tak významné postavení, že si z důvodu obav před možným únikem informací o nově vyvíjených produktech prosadila požadavek na zákon, na jehož základě smí zaměstnavatelé sledovat elektronickou poštu svých zaměstnanců. Podle některých právníků zákon porušuje základní svobody zakotvené ústavou. Zákon zaměstnavatelům dovoluje číst e-maily zaměstnanců z obavy, že vynesou ven firemní know-how. Co je to za demokracii, která toleruje zákony porušující základní svobody zakotvené v ústavě?

---

[95] *Renault: Špionáž mohla být podvod, vyhozené manažery vezmeme zpět* [online]. Byznys.ihned.cz, 2011 [cit. 2011-11-03]. Dostupné z WWW: <http://byznys.ihned.cz/zpravodajstvi-evropa/c1-50925470-renault-spionaz-mohla-byt-podvod-vyhozene-manazery-vezmeme-zpet>.

Finský parlament 4. března 2009 schválil zákon, na jehož základě smí podniky sledovat elektronickou poštu svých zaměstnanců. Zákonu se lidově říká Lex Nokia, protože o jeho přijetí se výrazně zasloužil i přední světový výrobce mobilních telefonů Nokia, jehož domovskou zemí je právě Finsko. Před několika týdny Nokia hrozila, že neprojde-li přijetí zákona v parlamentu, z Finska se na protest odstěhuje.

Zákon neumožní kontrolu obsahu elektronických dopisů, ale jen všeobecnou kontrolu toho, kam korespondence zaměstnanců směřuje. Nokia totiž již několikrát uvedla, že právě díky úniku informací elektronickou poštou přišla o významná obchodní i technologická tajemství a že zlepšení kontroly e-mailu by jí pomohlo tuto průmyslovou špionáž omezit.

Návrh zákona ale má ve Finsku celou řadu kritiků. Podle některých právníků například „Lex Nokia" porušuje základní svobody zakotvené v ústavě. Další kritiku budí skutečnost, že zákon nebude platit jen pro průmyslové podniky, ale i pro univerzity a bytová družstva.

Oponenti poukazují i na fakt, že pro průmyslové špiony není problém požadované údaje z pracovního počítače nahrát a přenést je domů, odkud je dále pošlou ze své soukromé emailové adresy.[96]

7.6 Neoprávněné užívání technologie LG u BMW a Audi

V říjnu roku 2011 se objevil nový případ o neoprávněném užívání technologie. Případ je poučný z pohledu patentové ochrany, kdy perspektivní LED technologie naráží na patentové zábrany. Společnost LG žaluje BMW a Audi, že neoprávněně využívá ve světlometech patentovanou technologii značky.

Automobilům BMW a Audi hrozí zákaz prodeje v Jižní Koreji. Je to kvůli tomu, že vozy používají LED světla společnosti Osram. S tou se momentálně kvůli patentům soudí koncern LG. U soudu korejský gigant žádá o předběžné opatření, které má porušování práv zastavit.[97]

Patent se netýká přímo dvou automobilek, ale společnosti Osram, která vozům dodává osvětlující komponenty. Podle žaloby neoprávněně užila technologii chráněnou

---

[96] *Firmy mohou sledovat emaily pracovníků* [online]. Lidovky.cz, 2009 [cit. 2011-11-30]. Dostupné z WWW: <http://byznys.lidovky.cz/tiskni.asp?r=moje-penize&c=A090304_221230_ln_ekonomika_abc>.

[97] *BMW a Audi hrozí v Koreji zákaz prodeje. Kvůli LED světlům* [online]. iDNES.cz, 2011 [cit. 2012-03-04]. Dostupné z WWW: <http://auto.idnes.cz/bmw-a-audi-hrozi-v-koreji-zakaz-prodeje-kvuli-led-svetlum-pem-/automoto.aspx?c=A111008_165249_automoto_vok>.

sedmi patenty společnosti LG. Součástí žaloby je také požadavek na zastavení prodejů vozů v Jižní Koreji.

Situace je ovšem pikantní v jiném smyslu. Vývoj, který je chráněn patenty LG, je dílem Osramu. Korejská společnosti si však od německého dodavatele některé technologie koupila a patentovala na domácím trhu. Nakonec však tuto technologii nepoužila a vyvinula vlastní. Prakticky to tedy znamená, že Osram je pod hrozbou pokut za vlastní patenty, které na území Jižní Koreje drží společnost LG.

Vozy BMW a Audi přitom tvoří v Koreji nezanedbatelnou část tamních prodejů, vše se navíc ještě posílí po uzavření dohod omezujících překážky v obchodování mezi EU a Jižné Koreou. Celkově však není korejský trh pro obě automobilky nikterak fatálně důležitý, udají zde kolem procenta své produkce.

Spor se týká jen jihokorejského trhu. Ve zbytku světa drží problémové patenty sám Osram a problémy tak nehrozí.[98]

7.7 Špionáž ve vývojovém centru Škoda Auto

V září roku 2011 se na internetu objevily špionážní fotografie, které odhalili novou podobu Škody Octavie III. Ani české firmy, natož takové, které se zabývají vývojem a výrobou automobilů nemohou být nepostiženy průmyslovou špionáží. Škoda Auto obratem, tržbami a počtem zaměstnanců patří k nejdůležitějším článkům českého hospodářství a každý únik informací je velkým rizikem, které se následně projeví v poklesu prodeje nebo snížením konkurenceschopnosti na velmi exponovaném trhu.

Třetí generace Škody Octavia se má podle neoficiálních informací představit až v roce 2012. Na internetu se objevily fotky karoserie kombiverze nafocené přímo ve vývojovém centru Škody, mladoboleslavské Česaně. Špionážní fotky karoserie doposud neznámé škodovky se objevily v diskuzi na serveru autorevue.cz.

Octavia III podle posledních informací podstupuje jízdní zkoušky. Představit by se měla na autosalonu v Paříži na podzim roku 2012.

Podobný únik fotografií z vývojového centra se udál v roce 2007, rok před uvedením druhé generace Škody Superb, autora fotek tehdy odhalili a šel před soud.[99]

---

[98] *Patentová válka míří k automobilům - LG žaluje BMW a Audi* [online]. News.autoroad.cz, 2011 [cit. 2011-12-11]. Dostupné z WWW: <http://news.autoroad.cz/zajimavosti/34951-patentova-valka-miri-k-automobilum-lg-zaluje-bmw-a-audi/>.

[99] *Špionáž ve vývojovém centru Škody: fotky Octavie III* [online]. iDNES.cz, 2011 [cit. 2011-12-11]. Dostupné z WWW: <http://auto.idnes.cz/tiskni.asp?r=ak_aktual&c=A110924_222049_ak_aktual_fdv>.

Zaměstnanec lakovny byl tím, kdo tentokrát stiskl spoušť a poskytl médiím fotografie karosérie chystané Škody Octavia třetí generace. Informoval o tom týdeník Škodovácký odborář. „Velmi nás mrzí, že se jednalo o našeho zaměstnance z lakovny," potvrdil časopisu člen představenstva odpovědný za personalistiku Bohdan Wojnar na zasedání Podnikové rady odborů KOVO. „Tento zaměstnanec ve firmě Škoda ihned skončil," dodal. Škoda podle něho připravuje i další právní kroky související s ochranou firmy v rámci konkurenčního boje.[100]

„Odposlechy, krádeže, ty nástroje, k jakým firmy sahají, jsou hodně pestré," hodnotí tuzemské praktiky čestný prezident České komory detektivních služeb František Brabec. *„Kradení nápadů ale přece jen není až tak běžné, vývojářských center je tu ostatně zatím relativně málo. Nejčastěji jde o pokusy o získání utajovaných ekonomických výsledků či důležitých rozhodnutí managementu, které například ovlivní cenu firemních akcií na burze. Jde často i o to, jakou cenu chce konkurence nabídnout v soutěži o zakázku,"* vypočítává pan Brabec.

Jak se přitom bezpečnostní experti shodují, co se průmyslové špionáže týká, české prostředí ovlivnila v minulosti především mohutná vlna státních privatizací z devadesátých let, kdy se uplácení klíčových lidí na straně státu i zjišťování slabých míst konkurence soupeřící o privatizovaný podnik staly běžnou praxí. *„Ten dnešní stav je díky tomu stále pokřivený. Jde o hrubé prostředí, kde se namísto sofistikovaných špionáží často přistupuje k nátlaku a vydírání. Tu situaci se roky nedaří zlepšovat,"* říká prezident Asociace soukromých bezpečnostních agentur Jiří Kameník, jehož firma Cenzus se mimo jiné specializuje právě na odhalování zaměstnanců vynášejících citlivé informace.

Soud o „hrubém prostředí" je ovšem třeba doplnit o názory expertů, kteří například již roky upozorňují na neexistující zákon, který by tady upravoval činnost nejrůznějších detektivních agentur. Jak říká sám Kameník: *„Marně po něm voláme. Všichni se vlastně pohybujeme na okraji zákona a právě tohle způsobuje, že se mezi agenturami vyskytuje velké množství kriminálníků a mafiánů."*

Kvůli chybějícím paragrafům pro bezpečnostní sektor Česko již několikrát kritizoval Brusel, vášnivé debaty se kvůli té věci v současnosti aktuálně vedou i ve vládě. Diskuse nemá zdaleka jen „firemní rozměr", mimo jiné tu jde o minulost agentury ABL patřící donedávna ministru dopravy Vítu Bártovi (VV), která podle MF

[100] *Škodě Mladá Boleslav unikly fotografie 3. generace vozu Octavia* [online]. Aktuálně.cz, 2011 [cit. 2012-03-19]. Dostupné z WWW: <http://auto.aktualne.centrum.cz/clanek.phtml?id=718342>.

Dnes v minulosti sledovala vybrané politiky ODS v Praze. Nic jako nájemné sledování či to, zda jde o přijatelnou praktiku, nebo kriminální čin, dosud česká legislativa neřeší. Licenci pro „detektivní služby“ má přitom v zemi zhruba patnáct set firem a po vyplnění jednoduché žádosti ji úřady udělují každému.

„Věc je potřeba urychleně řešit, přijetí zákona je ostatně součástí koaliční smlouvy,“ řekl v roce 2011 Radek John (VV). Na konkrétní podobě, autorovi novely ani na datu jejího vypracování se však koalice zatím nedokáže shodnout.[101]

[101] *Špioni v továrnách* [online]. Probin.cz, 2011 [cit. 2011-11-02]. Dostupné z WWW: <http://www.probin.cz/cz/37.spioni-v-tovarnach>.

ZÁVĚR

Práce analyzuje nejen historii průmyslové špionáže, ale v porovnání s případy ze současnosti ji aktuálně prezentuje v období po přechodu ze studené války na současné vysoce konkurenční prostředí. Popisuje příčiny vzniku průmyslové špionáže, řadu příkladů, postupný vývoj a možné způsoby boje, ochrany a prevence k eliminaci rizik před napadením průmyslovou špionáží.

Obchody kolem celého světa jsou pod tlakem hospodářského poklesu a nejistoty další tendence hospodářského vývoje vedou ke zvýšené poptávce po informacích a tedy i k větším rizikům úniku duševního vlastnictví. Dnešní nejrychleji rostoucí ekonomika, Čína, hladoví po technologiích a často nechápe západní pojem autorských práv a duševního vlastnictví.

Hlavním cílem bakalářské práce bylo analyzovat historii průmyslové špionáže a poukázat na projevy současných špionážních praktik v období po přechodu ze studené války na současné vysoce konkurenční prostředí. Škody způsobené ztrátou dat dosáhly v celosvětovém měřítku výše 1 bilionu dolarů. Firmy z Brazílie, Číny a Indie utrácejí za zabezpečení duševního vlastnictví více peněz než ty z Německa, Velké Británie, USA a Japonska. 79 % respondentů z Číny a 68 % z Indie uvedlo, že jejich firmy investovaly do zabezpečení svého duševního vlastnictví, aby tak získaly konkurenční výhodu. Duševní vlastnictví je stále oblíbenějším cílem i kybernetických podvodníků. 39 % respondentů pokládá ochranu duševního vlastnictví před zloději z vnějšku organizace za největší problém vůbec. Stále větší množství zaměstnanců přistupuje k firemním datům s cílem ukrást klíčové informace a obohatit se. 42 % respondentů pokládá za největší hrozbu pro své klíčové informace právě odcházející zaměstnance. Hrozby pro duševní vlastnictví jsou rozdílné ze zeměpisného pohledu. Firmy zúčastněné v průzkumu pokládají (z různých legislativních, kulturních a ekonomických důvodů) za problematické země především Čínu, Pákistán a Rusko. V Číně se firmy často domnívají, že hrozby jejich duševnímu vlastnictví mají původ v USA nebo na Tchaj-wanu, indické firmy mají obavy z Pákistánu. Americké firmy se obávají především úniku dat do Ruska či Číny. Naopak například indické firmy se uchovávat citlivá data v Číně obávají mnohem méně. I řada čínských firem se ale snaží citlivá data ukládat raději mimo svoji zemi. Od toho se odvíjí i podíl firem, které na zabezpečení informací věnují 20 % nebo více z celkových výdajů na IT (35 % Indie, 33 % Čína, 27 % Brazílie, 20 % Německo, 19 % USA, 10 % Japonsko, 4 % Velká Británie).

Průměrná roční ztráta, vyplývající z narušení duševního vlastnictví, byla v rámci průzkumu stanovena na 4,6 milionu dolarů. Přitom ve Velké Británii to bylo v průměru „jen“ 375 tisíc dolarů ve srovnání se 7,2 miliony dolarů v Číně. Za největší rizika pro firemní data je považován vnitřní nepřítel - 68 %, následuje softwarová zranitelnost – 51 %, kybernetický terorismus - 38 % a průmyslová špionáž - 36 %.

Průmyslová špionáž je v současných podmínkách velmi obtížně identifikovatelná, kontrolovatelná, s vysokým indexem hospodářské škodlivosti a bezpečnostního rizika pro společnost. Odborníci se shodují, že se Čína stane před rokem 2030 největší světovou ekonomikou. Na nejvyšší úrovni můžeme pozorovat, jak se nejen ČR, ale i EU vytrvale podbízejí Číně. Z druhé strany, v případě současné nelehké ekonomické situace Evropské unie, má samozřejmě i Čína eminentní zájem, aby se Evropské unii dařilo, neboť je to její klíčový obchodní partner. Z dlouhodobé praxe a odbornosti autora pracujícího více než dvacet let v oddělení vývoje komponentů pro automobilový průmysl jedné nejmenované firmy, může autor práce pozorovat tendence a tlaky nejvyššího zahraničního managementu nejen na rychlé přesuny výroby, kolikrát i samotných oddělení zabývající se vývojem a předvývojem výrobků s vysokým technologickým know-how, ale mnohdy i přesun nedostatečně patentově chráněného know-how. Vlastní ochrana tohoto duševního vlastnictví je pak již téměř nemožná.

Podle názoru autora je základní problém ten, že zatímco většina obyvatel Západu na spolupráci s Čínou prodělává, ekonomika firem je na tom opačně. Přesun výroby do Číny a dalších zemí s levnou pracovní silou - „*low cost country*“ je v zájmu výrobců šetřících náklady, nikoliv obyvatel států, které samotný průmysl opouští.

Je důležité si uvědomit, že se přístup k ochraně „životně“ důležitých informací duševního vlastnictví ze zeměpisného pohledu liší, a že je důležité, aby si každý subjekt, kterému záleží na informacích, jež mají pro jeho fungování a podnikatelský úspěch velký význam, tyto informace velmi dobře chránil.

Základní druhy ochrany, podle hrozby napadení, je nejvhodnější odlišit na vnitřní a vnější. Při vnitřní ochraně (ochrana proti interním útokům) lze nastavit zvláštní interní režim, při kterém je důležité se zaměřit na lidský faktor interních zaměstnanců, rozdělení vnitřních prostorů organizace na bezpečnostní zóny s definovanými právy vstupu prostřednictvím čipových karet, bezpečnostní služby, ochranu počítačové sítě, zálohování dat a informací, bezpečnost práce s datovými nosiči, a jiné. Vnější ochrana (proti útokům zvenčí) by měla využívat technologické aktivní ochrany (kontroly vstupu,

monitorovací a kamerové systémy, biometrické systémy, apod.) a pasivní ochrany dat a sítí (firewally, stínění datových a komunikačních spojů, asymetrické kryptografie, kvalifikované certifikáty, apod.).

Metody obrany lze třídit podle oblastí, kterých by se měla konkrétní ochrana týkat. Zaměstnanci by měli mít v počítačové síti vytvořeny uživatelské účty a vyřešena přístupová práva. Pro ochranu informací je žádoucí klasifikovat informace na stupně utajení a vytvořit speciální metodiku k aplikaci přístupů k jednotlivým třídám informací.

Průmyslová špionáž často využívá nedostatků v ochraně počítačové bezpečnosti daných firem. Vznikají bezpečnostní agentury, které se specializují na ochranu proti konkrétním druhům hrozeb. Průmyslová špionáž je trend, který se do značné míry pojí s konkurenceschopností firem, ale většina informací, o jednotlivých konkrétních metodách či druzích napadení, není veřejně prezentována, což má za následek celkově malé znalosti o tomto druhu špionážní činnosti.

Jako další způsob ochrany know-how je na místě chránit obchodní tajemství, důvěrné informace již v okamžiku jejich vzniku, ve fázi myšlenky a nikoliv až poté, kdy dojde k jejich neúmyslnému prozrazení. K tomuto účelu je vhodné investovat do nepřetržité práce v podobě pravidelného podávání patentových přihlášek.

SEZNAM POUŽITÝCH ZDROJŮ

Literární zdroje

1. BRABEC, F. *Ochrana bezpečnosti podniku.* Praha : EUROUNION s.r.o., 1996. 206 s. ISBN 80-85858-29-0.
2. BERGIER, J. *Průmyslová špionáž.* 1. vyd. Praha : Orbis, 1974. 192 s. ISBN 605-22-826.
3. DUŠEK, J., PROTIVA, V. *Veřejná ekonomika.* České Budějovice : Vysoká škola evropských a regionálních studií, 2007. 240 s. ISBN 978-80-86708-43-0.
4. FALIGOT, R., KROP, P. *"Bazén" : francouzská tajná služba (1944-1984)* Praha : Themis, 1998. 435 s. ISBN 80-85821-53-2.
5. GIFFORD, C. *Svět špionáže.* Havlíčkův Brod : Nakladatelství Fragment, s.r.o., 2006. 64 s. ISBN 80-253-0227-X.
6. ICT Unie a ÚPV podepsaly memorandum. *Technik.* 2012, č. 2/2012, s. III. ISSN 1214-9802.
7. JIRÁSEK, J. *Agenda příštích let.* Praha : Professional Publishing, 2006. 189 s. ISBN 80-86946-04-5.
8. JIRÁSEK, J. *Benchmarking a konkurenční zpravodajství.* Praha : Profess Consulting, s.r.o., 2007. 120 s. ISBN 978-80-7259-051-3.
9. JIRÁSEK, J. *Souboj mozků v řízení.* Praha : Alfa Publishing, s.r.o., 2004. 176 s. ISBN 80-86851-01-X.
10. NENADÁL, J., VYKYDAL, D., HALFAROVÁ, P. *Benchmarking : mýty a skutečnost : model efektivního učení se a zlepšování.* 1. vyd. Praha : Management Press, 2011. 265 s. ISBN 978-80-7261-224-6.
11. Ochrana soukromí před odposlechy. *Technik.* 2012, č. 4/2012, s. III. ISSN 1214-9802.
12. PACNER, K. *Atomoví vyzvědači studené války.* 1. vyd. Praha : Epocha, 2009. 501 s. ISBN 978-80-7425-001-9.
13. PACNER, K. *Československo ve zvláštních službách : pohledy do historie československých výzvědných služeb 1914-1989. Díl IV., 1961-1989.* 1. vyd. Praha : Themis, 2002. 692 s. ISBN 80-7312-013-5.
14. PACNER, K. *Kosmičtí špioni.* 1. vyd. Praha : Albatros, 2005. 283 s. ISBN 80-00-01686-9.

15. PIEKALKIEWICZ, J. *Historie špionáže : agenti, systémy, akce.* Praha : Naše vojsko, 2004. 567 s. ISBN 80-206-0738-2.
16. Před 75 lety získal DuPont patent na nylon. *Technik.* 2012, č. 6/2012, s. IV. ISSN 1214-9802.
17. REITZ, M. *Špioni, kteří měnili svět : od faraonů po Matu Hari.* 1. vyd. Praha : Víkend, 2008. 238 s. ISBN 978-80-86891-80-4.
18. *SiFo-Studie 2009/10 : Know-how-Schutz in Baden-Württemberg.* 1. vyd. Stuttgart : Steinbeis Edition, 2010. 102 s. ISBN 978-3-941417-20-5.
19. SOBEK, V. *Pomohli jsme sestřelit Powerse : tajemství Vědeckotechnické rozvědky ČSSR.* Praha : Futura, 2011. 162 s. ISBN 978-80-86844-67-1.
20. SMITH, M. *Britské tajné služby.* 1. vyd. Praha : Ivo Železný, 1998. 323 s. ISBN 80-237-3556-X.
21. ULFKOTTE, U. *Válka v temnotách : skutečná moc tajných služeb.* Praha : Ikar, 2007. 472 s. ISBN 978-80-249-0959-2.
22. VOLKMAN, E. *Dějiny špionáže : tajný svět špionů, vyzvědačů a rozvědčíků od starověku až do doby po 11. září.* 1. vyd. Praha : Fortuna Libri, 2008. 223 s. ISBN 978-80-7321-387-9.

Elektronické zdroje

1. *Americká špionáž náprava selhání* [online]. Computerworld.cz, 2000 [cit. 2011-11-10]. Dostupné z WWW: <http://computerworld.cz/archiv/americka-spionaz-naprava-selhani-17263>.
2. BAUER, J. *Tajnosti tajných služeb* [online]. 21 století.cz, 2003 [cit. 2011-08-11]. ISSN 0040-1064. Dostupné z WWW: <http://www.21stoleti.cz/view.php?cisloclanku=2003091828>.
3. *BMW a Audi hrozí v Koreji zákaz prodeje. Kvůli LED světlům* [online]. iDNES.cz, 2011 [cit. 2012-03-04]. Dostupné z WWW: <http://auto.idnes.cz/bmw-a-audi-hrozi-v-koreji-zakaz-prodeje-kvuli-led-svetlum-pem-/automoto.aspx?c=A111008_165249_automoto_vok>.
4. *Ceník služeb* [online]. PatentCentrum, 2010 [cit. 2011-11-16]. Dostupné z WWW: <http://patentcentrum.cz/prehled-sluzeb/cenik-sluzeb/>.

5. *Český hojivý vynález chrání patenty v Evropě i Americe. Má vydělat miliony* [online]. iDNES.cz, 2011 [cit. 2011-12-16]. Dostupné z WWW: <http://finance.idnes.cz/cesky-hojivy-vynalez-chrani-patenty-v-evrope-i-americe-ma-vydelat-miliony-1rh-/podnikani.aspx?c=A111207_111611_podnikani_sov>.
6. *Evropská unie varuje před anglosaským odposlouchávacím systémem, který prověřuje provoz na internetu* [online]. Britskelisty, 2001 [cit. 2011-08-11]. Dostupné z WWW: <http://www.britskelisty.cz/0105/20010528d.html>.
7. *Firmy mohou sledovat emaily pracovníků* [online]. Lidovky.cz, 2009 [cit. 2011-11-30]. Dostupné z WWW: <http://byznys.lidovky.cz/tiskni.asp?r=moje-penize&c=A090304_221230_ln_ekonomika_abc>.
8. *Investice Čína vs Západ, 3:0* [online]. Zadluzení.cz, 2010 [cit. 2011-11-04]. Dostupné z WWW: <http://www.zadluzeni.cz/2010/01/investice-cina-vs-zapad-30.html>.
9. JANSA, L. *Ochrana obchodního tajemství, důvěrných informací a know-how v podnikání* [online]. Právo IT, 2007 [cit. 2012-01-12]. Dostupné z WWW: <http://www.pravoit.cz/article/ochrana-obchodniho-tajemstvi-duvernych-informaci-a-know-how-v-podnikani>.
10. JOSHUA, P. *Informační válka, kybernetické útoky a rostoucí hrozba insiderů* [online]. Velká Epocha, 2010 [cit. 2011-10-26]. Dostupné z WWW: <http://www.velkaepocha.sk/2010122115706/Informacni-valka-kyberneticke-utoky-a-rostouci-hrozba-insideru.html>.
11. KŘEPELKOVÁ, H. *Marketing nebo průmyslová špionáž?* [online]. Ictsecurity.cz, 2011 [cit. 2011-7-01]. Dostupné z WWW: <http://ictsecurity.cz/sk/pdf/serial-o-informacnej-bezpecnosti/marketing-nebo-prumyslova-spionaz-serial-o-informacni-bezpecnosti-ze-vsech-uhlu.pdf>.
12. *KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV)* [online]. 2003. Praha : Národní knihovna České republiky, 2003 [cit. 2012-02-22]. Dostupný z WWW: <http://aleph.nkp.cz/F/?func=direct&doc_number=000000438&local_base=KTD>.
13. MAREK, J. *Využitelnost veřejně poskytovaných informací od firem* [online]. Risk-Management.cz, 2011 [cit. 2011-7-01]. Dostupné z WWW: <http://www.risk-management.cz/clanky/Vyuzitelnost-verejne-poskytovanych-informaci-od-firem.pdf>.

14. *McAffee - Firmy by neměly spoléhat na pomoc ze strany vlád nebo legislativy* [online]. Ictsecurity.cz, 2010 [cit. 2011-12-12]. Dostupné z WWW: <http://ictsecurity.cz/10/06/1-prumyslova-spionaz/mcaffee-firmy-by-nemely-spolehat-na-pomoc-ze-strany-vlad-nebo-legislativy.html>.
15. *McAfee Unsecured Economies Report* [online]. Resources.mcafee.com, 2009 [cit. 2011-10-12]. Dostupné z WWW: <http://resources.mcafee.com/content/NAUnsecuredEconomiesReport>.
16. *Metody špionáže: Průmyslová špionáž* [online]. Specialista.info, 2006 [cit. 2011-11-04]. Dostupné z WWW: <http://www.magazin.specialista.info/view.php?cisloclanku=2006013001>.
17. MOLNÁR, Z. *Potřeba, místo a úloha Competitive Intelligence profesionála v organizaci* [online]. Sborník konference systémová integrace 2008, CSSI, 2008 [cit. 2012-02-17]. Dostupné z WWW: <http://si.vse.cz/archive/proceedings/2008/potreba-misto-a-uloha-ci-profesionala-v-organizaci.pdf>.
18. *Patentová válka míří k automobilům - LG žaluje BMW a Audi* [online]. News.autoroad.cz, 2011 [cit. 2011-12-11]. Dostupné z WWW: <http://news.autoroad.cz/zajimavosti/34951-patentova-valka-miri-k-automobilum-lg-zaluje-bmw-a-audi/>.
19. *Patenty a užitné vzory* [online]. PatentCentrum, 2010 [cit. 2011-11-16]. Dostupné z WWW: <http://patentcentrum.cz/prehled-sluzeb/patenty-a-uzitne-vzory/>.
20. *Poplatky* [online]. Úřad průmyslového vlastnictví, 2012 [cit. 2012-03-05]. Dostupné z WWW: <http://www.upv.cz/cs/prumyslova-prava/vynalezy-patenty/poplatky.html>.
21. *Renault: Špionáž mohla být podvod, vyhozené manažery vezmeme zpět* [online]. Byznys.ihned.cz, 2011 [cit. 2011-11-03]. Dostupné z WWW: <http://byznys.ihned.cz/zpravodajstvi-evropa/c1-50925470-renault-spionaz-mohla-byt-podvod-vyhozene-manazery-vezmeme-zpet>.
22. *Schäuble se omluvil Němcům* [online]. iDNES.cz, 2000 [cit. 2011-10-25]. Dostupné z WWW: <http://zpravy.idnes.cz/schauble-se-omluvil-nemcum-d0v-/zahranicni.aspx?c=000118_184350_zahranicni_jpl>.
23. *Stav české legislativy v oblasti ochrany duševního vlastnictví* [online]. BusinessInfo.cz, 2009 [cit. 2012-01-15]. Dostupné z WWW:

<http://www.businessinfo.cz/cz/clanek/podnikatelske-prostredi/stav-ceske-legislativy-duse-vlastnictvi/1000520/51563/>.

24. *Šedá ekonomika v Číně roste rychleji než HDP* [online]. Velká Epocha, 2010 [cit. 2011-11-14]. Dostupné z WWW: <http://www.velkaepocha.sk/2010091614566/Bujici-seda-ekonomika-v-Cine.html>.
25. *Škodě Mladá Boleslav unikly fotografie 3. generace vozu Octavia* [online]. Aktuálně.cz, 2011 [cit. 2012-03-19]. Dostupné z WWW: <http://auto.aktualne.centrum.cz/clanek.phtml?id=718342>.
26. ŠMEJKAL, P. *Role informačního specialisty v procesu competitive intelligence* [online]. ProInflow: Časopis pro informační vědy, 2010 [cit. 2012-20-02]. ISSN 1804-2406. Dostupné z WWW: <http://pro.inflow.cz/sites/default/files/pdfcisla/ProInflow_12010.pdf>.
27. ŠPINDLER, K. *Průmyslová špionáž co o ní víme?* [online]. Technický týdeník, 2006, roč. 54, č. 4 [cit. 2011-10-12]. ISSN 0040-1064. Dostupné z WWW: <http://www.techtydenik.cz/detail.php?action=show&id=907&mark=>.
28. *Špionáž ve vývojovém centru Škody: fotky Octavie III* [online]. iDNES.cz, 2011 [cit. 2011-12-11]. Dostupné z WWW: <http://auto.idnes.cz/tiskni.asp?r=ak_aktual&c=A110924_222049_ak_aktual_fdv>.
29. *Špioni v továrnách* [online]. Probin.cz, 2011 [cit. 2011-11-02]. Dostupné z WWW: <http://www.probin.cz/cz/37.spioni-v-tovarnach>.
30. *Třetí světová válka:* [online]. 1.9.2007 [cit. 2012-01-03]. Dostupné z WWW: <http://www.pravoslav.gts.cz/zn_doby/vres.htm>.
31. VAIDIŠOVÁ, K. *Renault zradili vlastní manažeři* [online]. IHNED.cz, 2011 [cit. 2012-03-04]. Dostupné z WWW: <http://byznys.ihned.cz/c1-49260100-renault-zradili-vlastni-manazeri>.
32. VOLF, T. *Špionáž v Renaultu: Podezřelí manažeři mají v cizině tajná konta s miliony* [online]. IHNED.cz, 2011 [cit. 2011-11-03]. Dostupné z WWW: <http://byznys.ihned.cz/c1-49439160-spionaz-v-renaultu-podezreli-manazeri-maji-v-cizine-tajna-konta-s-miliony>.
33. WEYERSTALL, N. *Schutz vor Folgen der Industriespionage: Informationen auf Abwegen* [online]. Sicherheit.info, 2008 [cit. 2011-08-12]. Dostupné z WWW: <http://www.sicherheit.info/SI/cms.nsf/si.ArticlesByDocID/2101215?Open&SessionID=2559532-140656>.

SEZNAM ZKRATEK

- AIG - American International Group
- CI - Competitive Intelligence (konkurenční zpravodajství)
- CIA - Central Intelligence Agency (Ústřední zpravodajská služba USA)
- CIO - Chief Information Officers
- DGSE - Direction Générale de la Sécurité Extérieure (ekvivalent CIA)
- DST - Direction de la Surveillance du Territoire (Francouzská domácí tajná služba)
- ENISA - European Network and Information Security Agency (Evropská agentura pro bezpečnost sítí a informací)
- EPO - European Patent Office (Evropský patentový úřad)
- GCHQ - Government Communication Headquarters (Centrála pro vládní komunikace)
- GEC - General Electric Company
- GRU - Glavnoje Razvedivatěl'noje Upravlenije (Hlavní správa rozvědky)
- ICE - Intercity express (Rychlovlaky německých drah DB)
- ICT - Information and Communication Technology
- IFIP - International Federation for Information Processing (Mezinárodní federace pro zpracování informací)
- IT - Information Technology
- KGB - Komitet Gosudarstvenoi Bezopasnosti (Ruská tajná státní policie)
- LED - Light-emitting diode
- McAfee - Jedna z největších společností zaměřená na bezpečnostní technologie
- M.I.S - Military Intelligence Service (protišpionážní organizace v Anglii)
- NSA - National Security Agency (Národní bezpečnostní agentura)
- PCT - Patent Cooperation Treaty (Smlouva o patentové spolupráci)
- P.S.I. - Protection des Secrets Industriels (Ochrana průmyslových tajemství)
- RMC - Radio Monte Carlo
- SAEPO - Säkerhetspolisen (švédská zahraniční tajná služba)
- TDKIV - Česká terminologická databáze knihovnictví a informační vědy
- TGV - Train de Grande Vitesse (Rychlovlaky Francouzských železnic)
- ÚPV - Úřad průmyslového vlastnictví

SEZNAM OBRÁZKŮ, TABULEK A GRAFŮ

PŘÍLOHY

PŘÍLOHA Č. 1 – GENEZE SPONZORSKÉ AFÉRY CDU[102]

- 4. listopadu 1999 - Soud v Augsburgu vydává zatykač na Walthera Leislera Kiepa, pokladníka CDU v letech 1971-1992. Je podezřelý, že v roce 1991 přijal částku milion marek, kterou nezdanil.
- 5. listopadu 1999 - Kiep předstoupil před justici. Zatykač je na kauci 500 tisíc marek pozastaven. Jako svědek je předvolán hospodářský expert na účetnictví Horst Weyrauch, který vypovídá, že částka milion marek nebyla vyplacena Kiepovi, ale byla jako stranický dar uložena na konto CDU.
- 6. listopadu 1999 - List Süddeutsche Zeitung sděluje, že obchodník se zbraněmi Karlheinz Schreiber předal v roce 1991 v jednom švýcarském nákupním středisku Weyrauchovi kufřík s milionem marek; Kiep byl této transakci přítomen. Důvodem údajně je, že Kiep pomáhal při obchodech s tanky. Kiep toto obvinění popřel.
- 12. listopadu 1999 - Bývalý generální zmocněnec CDU Uwe Lüthje, kdysi nejbližší Kiepův spolupracovník, sděluje poprvé podrobnější údaje o milionové částce. Podle něj byly tyto peníze v roce 1992 ve formě tří dílčích částek rozděleny mezi různé lidi, kteří je zdanili. On sám dostal 370 tisíc marek.
- 21. listopadu 1999 - V souvislosti s Kiepovou aférou bývalý šéf CDU Helmut Kohl popírá podezření, že při dodávkách tanků do Saúdské Arábie v roce 1991 byly použity úplatky.
- 22. listopadu 1999 - Poslanecké frakce sociálních demokratů (SPD) a Zelených požadují, aby se stranickými dary a obchodem se zbraněmi zabýval zvláštní vyšetřovací výbor.
- 23. listopadu 1999 - Soud v Augsburgu ruší zatykač na Kiepa. Naléhavé podezření z daňového úniku však přetrvává.
- 26. listopadu 1999 - Bývalý generální tajemník CDU Heiner Geissler přiznává, že CDU vedla za Kohlovy éry tajná konta.

---

[102] *Schäuble se omluvil Němcům* [online]. iDNES.cz, 2000 [cit. 2011-10-25]. Dostupné z WWW: <http://zpravy.idnes.cz/schauble-se-omluvil-nemcum-d0v-/zahranicni.aspx?c=000118_184350_zahranicni_jpl>.

- 30. listopadu 1999 - Kohl přebírá politickou odpovědnost za „chyby“, jichž se CDU pod jeho vedením ve finančním resortu dopustila. Po krizovém zasedání předsednictva strany Kohl přiznává, že za jeho funkčního období se vedla oddělená konta. Obvinění, že za jeho působení finance ovlivňovaly politické rozhodování, však popírá.
- 3. prosince 1999 - Hannoverský právní zástupce Matthias Waldraff podává na Kohla trestní oznámení. Státní zastupitelství v Bonnu poté na základě Kohlova prohlášení zkoumá podezření vůči čestnému předsedovi CDU.
- 4. prosince 1999 - CDU sesazuje Hanse Terlindena, vedoucího pracovníka v centrále CDU. Tento blízký Kohlův důvěrník nepředal důležité podklady k peněžní aféře nynějšímu předsedovi CDU Wolfgangu Schäublemu, ale Kohlovi. 16. prosince 1999 - Kohl v jednom televizním rozhovoru přiznává, že v letech 1993-1998 převzal pro CDU sponzorský dar 1,5 až 2 miliony marek, který však nebyl vykázán v žádném oficiálním účetnictví strany. Jména sponzorů odmítl uvést. Poprvé se schází vyšetřovací výbor v čele s poslancem SPD Volkerem Neumannem. Výbor se nemá zabývat jen případnými úplatky při obchodu se zbraněmi, nýbrž také možným vlivem sponzorských darů na plánovaný prodej 114 tisíc železničářských bytů Kohlovou vládou.
- 18. prosince 1999 - Vychází najevo, že chybí důležité doklady k objasnění aféry Leuna. Při privatizaci tohoto východoněmeckého petrochemického kombinátu domněle CDU získala značné provize za prodej firmy francouzskému koncernu Elf Aquitaine.
- 22. prosince 1999 - Další krizové zasedání předsednictva CDU - Kohl se ho neúčastní. Předsednictvo rozhodně vyzve bývalého kancléře, aby zveřejnil jména tajných sponzorů. Generální tajemnice CDU Angela Merkelová požaduje v jednom novinovém článku, aby se strana konečně odpoutala od Kohla. Kromě toho svému pěstounovi vyčetla, že stranu poškodil. Předseda CDU Schäuble přiznal, že v roce 1994 převzal od obchodníka se zbraněmi Karlheinze Schreibera dar v hotovosti přes 100 tisíc marek, který není zanesen do účetnictví strany.
- 29. prosince 1999 - Státní zastupitelství v Bonnu sděluje Spolkovému sněmu své rozhodnutí zavést proti Kohlovi vyšetřování. Zastupitelství dalo osmačtyřicetihodinovou lhůtu ke vznesení námitky proti tomuto kroku. Kohl je vyšetřován pro podezření ze zpronevěry, která měla za následek poškození spolkové CDU.

- 10. ledna 2000 - Šéf CDU Wolfgang Schäuble potvrdil, že v roce 1994 přijal od obchodníka se zbraněmi Karlheinze Schreibera dar v hotovosti přes 100 tisíc marek, které nebyly zaneseny v účetních knihách CDU.

PŘÍLOHA Č. 2 – SAZEBNÍK SPRÁVNÍCH POPLATKŮ[103]

Poplatky

1) SPRÁVNÍ POPLATKY

ZÁKON č. 634/2004 Sb. o správních poplatcích
Sazebník správních poplatků

(poplatky se hradí na účet 3711-21526001/0710)

Variabilní symboly a číslování přihlášek vynálezů a evropských patentů
Číslo přihlášky vynálezu je označeno: **PV**, čtyřmístným rokem podání, pomlčkou a pořadovým číslem
Např.: PV 2000-156, 2008-1298
Variabilní symbol (VS) se skládá z číslice **1 + ročník (čtyři místa) + pořadové číslo přihlášky**
Např. pro PV 2000-156 je VS: 12000156, pro PV 2008-1298 je VS: 120081298.
V případě, kdy je placeno za nově podanou přihlášku a není plátci známé její číslo, lze uhradit poplatek pouze na první číslo variabilního symbolu, tj. 1. V tomto případě musí být název účtu plátce shodný s názvem/jménem přihlašovatele nebo zástupce, aby bylo možné platbu identifikovat.
Číslo evropského patentu je označeno EP + číslo evropského patentu
Např.: EP 1444521
Variabilní symbol pro EP je číslo evropského patentu, např.: 1444521.

Položka 126

	Kč
Vydání stejnopisu, opisu, výpisu z rejstříku, spisů, úředních listin a záznamů za každou i započatou stránku	100
Za každou i započatou stránku, je-li pořizována na kopírovacím stroji nebo na tiskárně počítače	15

Poznámka
Každou započatou stránkou se pro účely tohoto zákona rozumí vydaná stránka formátu A4 a menší.

Položka 127

	Kč
a) Přijetí žádosti	
- o první prodloužení lhůty	200
- o každé další prodloužení lhůty	500
- o prominutí zmeškání lhůty	1 000
b) Přijetí rozkladu proti rozhodnutí Úřadu průmyslového vlastnictví	1 000
c) Přijetí žádosti	
- o vydání osvědčení o právu přednosti (prioritní doklad)	600
- o zápis převodu	600
- o zápis licence	600
- o zápis zástavního práva	600
- o konverzi evropské přihlášky za každý stát, do kterého bude přihláška zaslána	600

[103] *Poplatky* [online]. Úřad průmyslového vlastnictví, 2012 [cit. 2012-03-05]. Dostupné z WWW: <http://www.upv.cz/cs/prumyslova-prava/vynalezy-patenty/poplatky.html>.

Položka 128

	Kč
a) Přijetí přihlášky vynálezu	1 200
- pokud je (jsou) přihlašovatelem (li) výlučně původce (i)	600
b) Přijetí žádosti	
- o zveřejnění před zákonem stanovenou lhůtou	800
- o zpřístupnění překladu nároků evropské patentové přihlášky včetně zpřístupnění oprav překladů	500
c) Přijetí žádosti o provedení úplného průzkumu přihlášky vynálezu	3 000
- za 11. a každý další uplatněný patentový nárok	500
d) Vydání patentové listiny do rozsahu	
- deset stran strojopisu	1 600
- za každou další stranu	100
e) Zveřejnění překladu evropského patentového spisu	2 000
- za zveřejnění oprav překladu	100
f) Předložení překladu evropského patentového spisu v dodatečné lhůtě	3 000

Položka 129

	Kč
a) Přijetí žádosti o určení, zda technické řešení spadá do rozsahu patentu	5 000
b) Přijetí návrhu na zrušení	
- patentu po uplynutí šesti měsíců od nabytí účinnosti patentu	2 000

Variabilní symboly a číslování mezinárodních přihlášek podle Smlouvy o patentové spolupráci (PCT)
Číslo přihlášky je označeno: **PCT/CZ**, čtyřmístným rokem podání, lomítkem, nulami k doplnění celkového pětimístného čísla a pořadovým číslem přihlášky
Např.: PCT/CZ2000/00049, PCT/2008/00001
Variabilní symbol (VS) se skládá z číslice **5 + ročník (čtyři místa) + pořadové číslo přihlášky**
Např. pro PCT/CZ2000/00049 je VS: 5200000049, pro PCT/CZ 2009/00001 je VS: 5200900001.
V případě, kdy je placeno za nově podanou přihlášku a není plátci známé její číslo, lze uhradit poplatek pouze na první číslo variabilního symbolu, tj. **5**. V tomto případě musí být název účtu plátce shodný s názvem/jménem přihlašovatele nebo zástupce, aby bylo možné platbu identifikovat.

Položka 130

	Kč
Úkony Úřadu průmyslového vlastnictví spojené s podáním mezinárodní přihlášky podle Smlouvy o patentové spolupráci	1 500

2) UDRŽOVACÍ POPLATKY

ZÁKON č. 173/2002 Sb. o poplatcích za udržování patentů a dodatkových ochranných osvědčení pro léčiva a pro přípravky na ochranu rostlin a o změně některých zákonů
Sazebník poplatků za udržování patentů v platnosti

(poplatky se hradí na účet 80012-21526001/0710)

Variabilní symboly (VS): Jako variabilní symbol se užívá číslo patentu.
Např.: pro patent 289326 je VS: 289326.

	Kč
a) za první rok ode dne podání přihlášky vynálezu	1 000
b) za druhý rok ode dne podání přihlášky vynálezu	1 000
c) za třetí rok ode dne podání přihlášky vynálezu	1 000
d) za čtvrtý rok ode dne podání přihlášky vynálezu	1 000
e) za pátý rok ode dne podání přihlášky vynálezu	2 000
f) za šestý rok ode dne podání přihlášky vynálezu	2 000
g) za sedmý rok ode dne podání přihlášky vynálezu	2 000
h) za osmý rok ode dne podání přihlášky vynálezu	2 000
i) za devátý rok ode dne podání přihlášky vynálezu	3 000
j) za desátý rok ode dne podání přihlášky vynálezu	4 000
k) za jedenáctý rok ode dne podání přihlášky vynálezu	6 000
l) za dvanáctý rok ode dne podání přihlášky vynálezu	8 000
m) za třináctý rok ode dne podání přihlášky vynálezu	10 000
n) za čtrnáctý rok ode dne podání přihlášky vynálezu	12 000
o) za patnáctý rok ode dne podání přihlášky vynálezu	14 000
p) za šestnáctý rok ode dne podání přihlášky vynálezu	16 000
q) za sedmnáctý rok ode dne podání přihlášky vynálezu	18 000
r) za osmnáctý rok ode dne podání přihlášky vynálezu	20 000
s) za devatenáctý rok ode dne podání přihlášky vynálezu	22 000
t) za dvacátý rok ode dne podání přihlášky vynálezu	24 000

Sazebník poplatků za udržování evropských patentů v platnosti

(poplatky se hradí na účet 35-21526001/0710)

Variabilní symboly (VS): Jako variabilní symbol se užívá číslo evropského patentu.
Např.: pro evropský patent 1328015 je VS: 1328015.

	Kč
a) za první rok ode dne podání evropské patentové přihlášky	1 000
b) za druhý rok ode dne podání evropské patentové přihlášky	1 000
c) za třetí rok ode dne podání evropské patentové přihlášky	1 000
d) za čtvrtý rok ode dne podání evropské patentové přihlášky	1 000
e) za pátý rok ode dne podání evropské patentové přihlášky	2 000
f) za šestý rok ode dne podání evropské patentové přihlášky	2 000
g) za sedmý rok ode dne podání evropské patentové přihlášky	2 000
h) za osmý rok ode dne podání evropské patentové přihlášky	2 000
i) za devátý rok ode dne podání evropské patentové přihlášky	3 000
j) za desátý rok ode dne podání evropské patentové přihlášky	4 000
k) za jedenáctý rok ode dne podání evropské patentové přihlášky	6 000
l) za dvanáctý rok ode dne podání evropské patentové přihlášky	8 000
m) za třináctý rok ode dne podání evropské patentové přihlášky	10 000
n) za čtrnáctý rok ode dne podání evropské patentové přihlášky	12 000
o) za patnáctý rok ode dne podání evropské patentové přihlášky	14 000
p) za šestnáctý rok ode dne podání evropské patentové přihlášky	16 000
q) za sedmnáctý rok ode dne podání evropské patentové přihlášky	18 000
r) za osmnáctý rok ode dne podání evropské patentové přihlášky	20 000
s) za devatenáctý rok ode dne podání evropské patentové přihlášky	22 000
t) za dvacátý rok ode dne podání evropské patentové přihlášky	24 000

PŘÍLOHA Č. 3 – CENÍK SLUŽEB PATENTCENTRUM SEDLÁK & PARTNERS S.R.O.[104]

V tomto ceníku naleznete honoráře za jednotlivé úkony služeb patentového zástupce. Kompletní náklady na registraci patentu, ochranné známky apod. sestávají kromě těchto honorářů i ze správních poplatků a z dalších eventuálních nákladů jako jsou např. překlady apod. Na Vaše konkrétní zadání dotazu Vám připravíme předběžnou kalkulaci či odhad celkových nákladů.

Kromě úkonů patentového zástupce zahrnují náklady na průmyslově – právní ochranu i správní poplatky patentových a známkových úřadů. Správní poplatky Úřadu průmyslového vlastnictví ČR naleznete ZDE.

Ceny uvedeny bez DPH (20%)

Ceník služeb ZDE

Č. pol.	Úkon	Cena
	I. Vynálezy	
1	Podání přihlášky vynálezu v ČR	* 4.400,-
2	Podání žádosti o provedení úplného průzkumu	700,-
3	Informování klienta o zveřejnění PV	700,-
4	Podání žádosti o dřívější zveřejnění PV	600,-
5	Podání žádosti o zápis změny v rejstříku	1.100,-
6	Podání rozkladu nebo odpovědi na rozklad	*2.700,-
7	Podání návrhu na zrušení patentu nebo vyjádření k návrhu na zrušení patentu, podání rozkladu proti rozhodnutí	*2.700,-
8	Podání návrhu na určení, podání rozkladu proti rozhodnutí	*2.200,-
9	Podání vyjádření k návrhu na určení	*2.200,-
10	Zajištění úhrady poplatku za tiskové náklady	700,-
11	Zajištění úhrady poplatku za udržování patentu (za každý jednotlivý rok)	600,-
12	Podání mezinárodní přihlášky vynálezu dle PCT	*8.000,-
13	Podání evropské patentové přihlášky (EP)	*19.000,-
	II. Užitné vzory (UV)	
	zde neuvedené položky jsou obdobné jako v části I. Vynálezy	
14	Podání přihlášky užitného vzoru v ČR	*4.400,-
15	Podání žádosti o prodloužení platnosti užitného vzoru	1.600,-
16	Podání návrhu na výmaz užitného vzoru nebo vyjádření k návrhu na výmaz, podání rozkladu proti rozhodnutí	*2.400,-
17	Podání návrhu na určení nebo vyjádření k návrhu na určení podanému třetí osobou, podání rozkladu	*2.400,-
	* bez věcného zpracování (hodinová sazba č. pol. 55)	
	III. Průmyslové vzory (PVz)	
18	Podání přihlášky průmyslového vzoru v ČR	4.000,-
19	Podání přihlášky hromadného průmyslového vzoru (+ 300,- za každý další průmyslový vzor)	4.000,-
20	Podání žádosti o prodloužení platnosti průmyslového vzoru	2.200,-
21	Podání návrhu na výmaz průmyslového vzoru nebo vyjádření k návrhu na výmaz, podání rozkladu	*2.400,-
22	Podání žádosti o změnu v rejstříku	1.100,-
23	Podání přihlášky komunitárního (evropského) průmyslového vzoru (CD) – prvý prům. vzor	14.400,-
23a	Podání hromadné přihlášky komunitárního (evropského) prům. vzoru (CD) – za druhý a každý další prům. vzor	1.100,-
	IV. Ochranné známky (OZ)	
24	Podání přihlášky OZ (do tří tříd) v ČR, včetně rešerše	5.500,-
25	Podání národní přihlášky OZ v zahraničí (mimo SR)	10.000,-
26	Poplatek za každou další třídu (nad tři třídy)	300,-
27	Nárokování priority	500,-
28	Podání žádosti o obnovu OZ	3.300,-
29	Podání žádosti o obnovu OZ v poshověcí lhůtě	4.400,-
30	Podání žádosti o změnu jména nebo adresy přihlašovatele nebo majitele OZ, zúžení či úpravu seznamu výrobků a služeb, zápis nebo změnu zástupce, zápis licenční smlouvy apod.	1.100,-
31	Informace o zveřejnění OZ, sledování námitkové lhůty, přijetí, kontrola a zaslání osvědčení o zápisu OZ, založení evidenčních souborů pro sledování platnosti OZ	1.100,-
32	Sledování kolizních zveřejněných přihl. OZ (1 známka / měsíc)	150,-
33	Podání návrhu na zrušení či prohlášení neplatnosti OZ, námitky či připomínky proti zápisu OZ, podání vyjádření k návrhům, námitkám, připomínkám	*3.000,-

[104] *Ceník služeb* [online]. PatentCentrum, 2010 [cit. 2011-11-16]. Dostupné z WWW: <http://patentcentrum.cz/prehled-sluzeb/cenik-sluzeb/>.

34	Podání rozkladu proti rozhodnutí Úřadu nebo odpovědi na rozklad ve věci OZ	*3.400,-
35	Provedení rešerše OZ platných na území ČR (CZ, WIPO, CTM) (nikoli jako součást přihlášky OZ) na shodnost i zaměnitelnost, včetně rešeršní zprávy	*2.200,-
36	Podání přihlášky mezinárodní OZ	4.400,-
37	Podání žádosti o územní rozšíření, převod, změnu jména či adresy mezinárodního zápisu	2.200,-
38	Vyjádření proti „Avis de refus“ v zahraničí	*2.200,-
39	Žádost o obnovu platnosti mezinárodní OZ	4.400,-
40	CTM – Podání přihlášky komunitární (evropské) OZ	16.000,-
41	CTM – Podání námitky, návrhu na zrušení nebo prohlášení neplatnosti, rozkladu nebo vyjádření k těmto položkám	*9.000,-
42	CTM – Podání žádosti o zápis změny v rejstříku	3.000,-
42a	CTM – Podání žádosti o vydání Osvědčení	4.000,-

* bez věcného zpracování (hodinová sazba č. pol. 55)

V. Různé obecné úkony

43	Žádost o vystavení prioritního dokladu	1.100,-
44	Podání odpovědi na výměr Úřadu	*1.000,-
45	Dodatečné předložení listin nebo jiných materiálů	700,-
46	Jiná, nespecifikovaná podání Úřadu	1.100,-
47	Překlad z češtiny do cizího jazyka (1 strana – cca 250 slov)	480,-
48	Překlad z češtiny do cizího jazyka (1 strana – cca 250 slov)	420,-
49	Převzetí zastoupení rozpracovaného případu	1.100,-
50	Podání žádosti o prodloužení lhůty	500,-
51	Podání žádosti o navrácení lhůty	800,-
52	Podání žádosti o převod V, UV, PVz, OZ popř. přihlášky	1.600,-
53	Podání žádosti o zápis licence	1.300,-
54	Kontrola a zaslání patentové listiny nebo osvědčení o registraci užitného popř. průmyslového vzoru	600,-
55	Věcné zpracování – odborná práce patentového zástupce (1 hodina dle obtížnosti)	800 – 1.200,-
56	Administrativní práce (1 hodina)	450,-
57	Paušální poplatek na úhradu spojových služeb, telekomunikací a režie	300,-
58	Expresní příplatek (za provedení úkonu do 3 dnů)	30%
59	Podání správní žaloby proti rozhodnutí předsedy Úřadu prům. vlastnictví, podání vyjádření ke správní žalobě	*4.000,-
60	Podání žádosti v přijetí celního opatření. opatření ČOI	*3.500,-
61	Zajištění registrace domény	1.000,-

* bez věcného zpracování (hodinová sazba č. pol. 55)