UNIVERSIDADE FEDERAL DO PARANÁ

LEONARDO SCHMITZ MOSCA

ESPIONAGEM ECONÔMICA-INDUSTRIAL: CARACTERÍSTICAS, MÉTODOS E FORMAS DE MANIFESTAÇÃO

Curitiba

2017

LEONARDO SCHMITZ MOSCA

ESPIONAGEM ECONÔMICA-INDUSTRIAL: CARACTERÍSTICAS, MÉTODOS E FORMAS DE MANIFESTAÇÃO

Trabalho acadêmico apresentado ao departamento de Economia da Universidade Federal do Paraná, como parte dos requisitos para a obtenção do título de bacharel em economia.

Orientador: Prof. Dr. Walter Tadahiro Shima

Curitiba
2017

RESUMO

A prática de atos de espionagem econômica-industrial remonta a tempos antigos, porém a emergência das novas tecnologias da informação aumentou exponencialmente a facilidade para cometer estas ações. Este trabalho apresentará como estes fenômenos se manifestam, quem está por trás deles e quem há de se preocupar com eles. Através de análises de casos que vieram a público, é possível ver uma fração do que ocorre diariamente dentro das maiores companhias e governos do mundo. Em decorrência do caráter dissimulado destas ações, a análise de casos torna-se indispensável para compreender a metodologia deste tipo de espionagem. Através de uma análise baseada nestes exemplos, pode-se descobrir quais são as vulnerabilidades que existem dentro de uma organização. Descobrir as vulnerabilidades é o primeiro dos passos para eliminá-las ou reduzi-las. O caráter estratégico destas ações para os países que abrigam as sedes destas firmas também será apresentado, já que a competição industrial é uma das bases dos conflitos econômicos ao longo da história humana.

Palavras-chave: *espionagem econômica, concorrência, políticas públicas*

ABSTRACT

The practice of either industrial and economic espionage dates back to ancient times. However, the emergency of new information and communication technologies has exponentially increased the ways to commit his actions. This work reports how this phenomenon manifest themselves, what is behind them and who should be concerned about them. Through analyzing cases that were brought to light, it is possible to observe a fraction of what happens daily inside the greatest companies and governments around world. Due to the deceitful nature of this actions, the analysis of the cases becomes of crucial importance to understand the methodologies of this kind of espionage. By analyzing these examples, it is possible to discover the vulnerabilities that exist inside an organization. The first of the step to eliminate or reduce the vulnerabilities is to know how to recognize them within the general framework. The strategic character of this actions in the countries which are headquarters to these companies shall be described and discussed, since industrial competition is one of the cornerstones of the economic conflicts along human history.

Keywords: *economic espionage, competition, public policies*

Sumário

1. Introdução

Este estudo busca compreender como se dão as ações de espionagem econômica-industrial nos dias atuais, assim como a trajetória evolutiva destas ações ao longo do tempo. Esta estratégia de competição pode ser usada como pelo setor público, em forma de políticas públicas, que são ações que o governo julga necessárias em um determinado setor, com o intuito de desenvolver uma atividade que o Estado julga não estar sendo devidamente atendida pelos entes privados.

1.1. Aspectos gerais e justificativa

As ações espúrias de concorrência entre empresas e países são antigas, existindo exemplos análogos às práticas modernas desde os tempos das cidades mercantes da Itália renascentista. No entanto, com o advento da globalização e disseminação das tecnologias da informação, este processo se intensificou de maneira substancial. Compreender o que é feito pelos expoentes destas práticas é uma maneira eficiente de se proteger delas, bem como de formular políticas públicas para detê-las, ou aproveitar-se delas. Levando em consideração estes fatos, evidencia-se a necessidade de um trabalho que abranja as ações dissimuladas cometidas em nome da obtenção de vantagens entre competidores. Sendo a competição entre entes privados ou entre nações, onde a espionagem econômica-industrial pode tomar a forma de política pública.

1.2. Objetivos

Existem dois pontos principais neste estudo. O primeiro é analisar como a espionagem econômica-industrial ocorre nos dias atuais, bem como a metodologia empregada para o sucesso desta iniciativa. O segundo ponto consiste em determinar quais são os ganhos reais desta ação para o perpetrador e, por consequência, quais são as perdas possíveis das vítimas.

1.2.1. Objetivos específicos

Identificar as vulnerabilidades que as empresas modernas têm, para que seja possível elaborar estratégias de contenção de riscos. Definir como as nações transformam estas ações em políticas de Estado.

1.3. Metodologia

Esta pesquisa a respeito da espionagem econômica-industrial segue uma linha descritiva e explicativa, buscando melhor compreensão da forma em que estas ações se manifestam. Graças aos casos documentados e as teorias de concorrência entre empresas é possível analisar os métodos empregados pelas empresas ou países que cometem atos de espionagem, havendo a possibilidade de verificar quais são as diferentes abordagens metodológicas para realizar estas ações. Logo, para a realização deste estudo será empregada uma técnica de coleta de dados consistindo em pesquisas bibliográficas e estudos de casos. A seleção dos autores e dos casos segue o critério da especialização no tema, bem como a relevância destes para o tema desta pesquisa.

Devido ao caráter dissimulado destas ocorrências, há uma escassez de dados numéricos a respeito das perdas das vítimas. Esta escassez de dados foi um empecilho para a realização deste estudo, por muitas vezes, o alvo da ação não tem nem mesmo conhecimento de sua perda não gerando dados disponíveis para análises futuras. Ainda assim, existem órgãos e autores com dados e estimativas críveis disponíveis sobre o tema. Estes dados serão utilizados para realizar uma tentativa de mensuração dos riscos a que uma firma pode estar sujeita, ainda que de forma estimada.

2. Revisão bibliográfica

A revisão bibliográfica consiste em oferecer uma melhor compreensão de como se dá a manifestação dos casos de espionagem industrial, auxiliada por uma apresentação do histórico do objeto de pesquisa. Assim como oferecer uma definição e delimitação do tema abordado que permita uma análise mais precisa.

2.1. Definição

Os conceitos de espionagem industrial e espionagem econômica são distintos. A espionagem industrial é realizada por empresas e conglomerados tendo como foco as suas concorrentes ou qualquer outra entidade possuidora de objetos de interesse. A espionagem econômica, por sua vez, é realizada por países que busquem informações que julguem pertinentes para as necessidades do país. Explicitando a diferença: caso uma empresa de um país “x” se apropriasse de uma máquina ou método de uma empresa de um país “y”, isto seria espionagem industrial. Porém, caso o país “x” fornecesse os meios

de espionagem ou a fizesse por conta própria para a empresa agressora, isto seria espionagem econômica. O Departamento de Justiça Americano define espionagem industrial como: *"uma atividade conduzida por uma companhia estrangeira, com ou sem apoio de um governo estrangeiro, contra uma companhia privada americana, com o único propósito de se adquirir segredos comerciais"*, Nasheri (2005). A definição envolve governos estrangeiros, pois, muitas vezes as grandes companhias de um país estão intrinsecamente ligadas aos seus governos, sendo difícil definir a origem e composição exata da ação de espionagem. A maioria das nações define a espionagem econômica como uma questão de segurança nacional, já que os alvos são tecnologias estratégicas em áreas extremamente intensivas em tecnologia. Uma definição bastante precisa de espionagem econômica é posta pelo Serviço de Segurança e Inteligência Canadense: *"atividade ilegal, clandestina, coercitiva ou dissimulada engajada ou facilitada por um governo estrangeiro designada para ganhar acesso não autorizado à inteligência econômica, como informação ou tecnologia de outros, para vantagens econômicas",* Nasheri (2005).

A definição de espionagem industrial de Fialka (1999) é que a espionagem econômica é sutil e constante, com ganhos muitas vezes imperceptíveis: *"Os vencedores vencem silenciosamente e os perdedores, por muitas vezes, não tem consciência da perda"*. A natureza da espionagem econômico-industrial é a constância destas ações, um limbo perpétuo entre a guerra e a paz. A espionagem de propriedade intelectual alheia é, por definição, um roubo, ainda que feito de nas mais tênues relações legais do comércio internacional. Uma série de legislações, criadas pelos países para combater a aquisição ilícita de informações econômicas, tem como objetivo trazer delimitações das especificidades de cada tipo de ação. Porém, como será relatado, as linhas entre os tipos de ação são tênues e convergentes, com os interesses privados das empresas sendo simbióticos aos do país.

2.2. Origens históricas

A prática de espionagem industrial tem origens remotas. Um exemplo clássico e claro é a antiga república de Veneza, onde constam nas leis da cidade diversos mecanismos de fomento à espionagem. Uma lei de 1474 dava direitos de monopólio, por certa quantidade de anos, para quem trouxesse uma máquina ou equipamento estrangeiro para a cidade. Esta lei tinha como objetivo claro incentivar que venezianos viajassem pelo

mundo buscando novas tecnologias. Este mecanismo institucional fazia com que o aventureiro obtivesse lucros com o monopólio da nova tecnologia e a república mercante adquirisse novos conhecimentos e maquinários. Leis de patentes e proteção intelectual foram sendo desenvolvidas por esta cidade, para tentar reverter o declínio que Veneza se encontrava ao final do século XV, tendo perdido espaço para outras cidades-estado italianas como Florença. Estas instituições de fomento à inovação e à espionagem econômica-industrial primitiva foram gradualmente se espalhando por outras nações europeias, como a França, Inglaterra e Estados membros do Sacro Império Romano, Nasheri (2005).

Dentro da incorporação destas instituições legais, dois caminhos se destacaram: o francês e o britânico, Nasheri (2005). Tratam-se de dois tipos de pensamento filosófico distintos, o método francês era coletivista por natureza, entendendo que era o Estado que deveria distribuir as benesses e monopólios das patentes desenvolvidas, roubadas ou adquiridas. Já os britânicos partiram de uma visão individualista, fundamentalmente baseada nas visões de John Locke, um predecessor dos liberais. Alguns pensadores iluministas subsequentes, como Kant, reforçariam estas noções. Para a corrente liberal, o obtentor da patente deveria ser agraciado com os direitos de seu trabalho. O método britânico acabou por se tornar o "vencedor" sendo seguido pelos Estados Unidos da América, após sua independência em 1776, e pelo restante da Europa ocidental após o advento da revolução francesa. Porém, a importância do Estado dentro da lógica de desenvolvimento e obtenção de tecnologia, mesmo que o obtentor tenha seus direitos individuais, não deixa de ser uma realidade, como os exemplos apresentados demonstrarão.

Bergier (1975) um historiador suíço que tratou das relações econômicas nos tempos medievais, relata os seguintes casos de espionagem industrial: a porcelana e a seda chinesas. O caso da porcelana Ming, cujas técnicas de produção foram trazidas da China para a Europa. Um padre jesuíta francês chamado François Xavier d'Entrecolles fez um estudo sobre o método de produção de porcelana enquanto este se encontrava em na cidade de Jingdezhen. Sua obra detalhada foi capaz de transmitir o *know-how* chinês para a França e da França, para outros países da Europa. Até então a porcelana era um produto, em sua quase totalidade, proveniente da China. Este caso é um forte exemplo dos riscos econômicos que a espionagem industrial pode ter para um país, mesmo com a interferência de apenas um agente privado. Ainda segundo Bergier (1975) a nação chinesa

já havia sido vítima deste tipo de ação no passado. No século V depois de Cristo, uma nobre chinesa foi até a Índia, com bichos da seda escondidos em seu chapéu, a partir deste ponto o segredo da produção de seda escapou da China e se disseminou para outros potenciais concorrentes.

Segundo Harris (1989), durante o século XVIII, a Inglaterra estava diversas etapas à frente de seus vizinhos na criação e ampliação de sua base industrial. Registraram-se neste período intensas tentativas do Estado francês em se apropriar dos métodos e maquinários britânicos. O desnível entre as capacidades industriais de países vizinhos é um grande incentivo para estes tipos de operações ilícitas, oferecendo ganhos reais de curto prazo, bem como "queimar etapas" no desenvolvimento industrial. A queima de etapas é um dos objetivos básicos da espionagem econômico-industrial, desenvolver um *know-how* próprio para um produto pode levar décadas, um tempo que não pode ser perdido entre países vizinhos e concorrentes.

Este tipo de ação foi se popularizando cada vez mais nas estratégias de concorrência globais, especialmente com as duas guerras mundiais no século XX e a subsequente guerra fria entre os Estados Unidos e a extinta União Soviética. Na Primeira Guerra Mundial (1914-1918) os países da Entente (Inglaterra, França e Império Russo) estavam extremamente atrasados no campo da engenharia química, comparativamente ao Império Alemão, e, através de espionagem econômica, foram capazes de adiantar em muitos anos a produção de gás tóxico para fins militares, de acordo com Bergier (1969). O mais notório caso entre as superpotências da guerra fria é o desenvolvimento da bomba nuclear soviética concluída em 1949 graças, em grande parte, à espionagem nas instalações nucleares americanas, Fraumann (1997). Nasheri (2005) afirma que, após o término da guerra fria os antigos membros do pacto de Varsóvia tinham uma quantidade elevada de agentes de espionagem sem uma função, bem como um atraso tecnológico frente aos países membros da OTAN. Esta situação teve como resultado um redirecionamento das atividades de espionagem destes países das atividades internas para a espionagem econômica de países mais desenvolvidos.

2.3. O processo de evolução devido ao progresso tecnológico

Para Nasheri (2005) com o advento da informática e da facilitação das linhas de comunicações, não houve só um aumento nos casos de espionagem industrial, mas também, a facilitação destas ações. Estes novos métodos de espionagem são imunes a

barreiras físicas e concretas, dependendo apenas de habilidade e engenhosidade da parte agressora. Como estas situações ocorrem em diversos países, de maneira simultânea, há conflitos entre as legislações de cada local, impedindo que uma investigação sobre crimes cometidos contra a propriedade intelectual seja realizada de maneira eficiente. Estes problemas jurisdicionais são apenas uma das facilitações trazidas pela propagação do uso da Internet, Nasheri (2005).

As diferenças entre os países não se limitam a diferenças legais. Um país pode deliberadamente ter um conjunto de leis que dificulte os processos de rastreamento das atividades ilegais de seus cidadãos, havendo interesses na realização deste tipo de atividade. O progresso tecnológico se dá em diferentes etapas, muitas vezes é um processo de aprendizado dependente de tentativas e erros. A cada tentativa frustrada, há uma perda de recursos inerentes. As nações menos desenvolvidas, na área em questão, que desejem obter estas novas tecnologias não podem se dar ao luxo de desperdiçar recursos em tentativas de pesquisa fracassadas. Por conseguinte, um país pode ter a intenção deliberada de incentivar atividades ilícitas de espionagem contra alvos de interesse em países mais avançados. Nasheri (2005) argumenta que os conflitos provenientes destas situações são de difícil resolução, dado que há pouca cooperação efetiva no nível internacional. Esta falta de cooperação é decorrente das discrepâncias entre os países desenvolvidos e em desenvolvimento, que possuem interesses dicotômicos neste campo.

Outra facilitação para atividades de espionagem provenientes do progresso tecnológico é a abrangência geográfica do crime. Uma ação voltada a coibir ou eliminar ações de espionagem contra um alvo podem exigir forças-tarefas compostas de um grande número de agentes e departamentos de países variados. As diferenças linguísticas, de estruturação, de fuso-horário e de ordem jurídica são fatores que reduzem, em medidas diferentes, a eficiência da resposta das instituições legais responsáveis contra ameaças. Além da demora de reação da parte agredida há uma outra problemática: nos casos onde é possível identificar o agressor é, em muitos casos, difícil efetuar uma punição condizente com a magnitude do crime. Agentes operando de forma privada podem vender os segredos comerciais e industriais para empresas ou governos. De forma que o agente individual pode ser encontrado e responsabilizado sem que haja uma reparação efetiva, visto que o segredo já foi perdido e os perpetradores necessitam somente arregimentar novos agentes para realizar novas atividades. O combate a crimes cometidos via meios

eletrônicos requer um treinamento diferenciado e custoso, em termos de recursos e tempo, e nem todas as instituições de combate ao crime podem arcar com esta especialização.

Assim como o processo de globalização e universalização das comunicações iniciado no século passado trouxe ganhos e oportunidades gigantescas para os grandes conglomerados e empresas, houve também uma perda de segurança e controle do fluxo de informações entre competidores. Há uma proliferação de casos de espionagem econômica-industrial que transcende as alianças geopolíticas clássicas. Segundo Nasheri (2005), após o colapso do bloco soviético ao final dos anos 1980, houve uma mudança de área de atuação para agentes, tanto dos países membros do finado pacto de Varsóvia, quanto de agentes provenientes da OTAN, que perderam seu principal rival. Esta momentânea ociosidade dos agentes de inteligência permitiu aos países, antes interessados em proteger sua segurança interna e externa, que passassem a usar essa capacidade ociosa de espionagem, para ampliar sua capacidade econômica. O fato desta mudança de foco dos agentes de inteligência ter ocorrido simultaneamente à revolução informática serviu como um efeito catalisador na dimensão que a espionagem econômica-industrial tem no mundo.

No processo de evolução animal, para que caça e caçador não sejam extintos, ambos devem estar constantemente evoluindo para sobreviver. Assim como um guepardo tentando alcançar uma gazela, o nível de complexidade e capacidade de defesa dos sistemas de informática é acompanhado pelo desenvolvimento de técnicas e meios de infiltração cada vez mais complexos por parte dos agressores, como corroborado pelo testemunho de Richard Pethia, diretor do CERT/CC (*Computer Emergency Research Team/Coordenation Center*) em 10 de setembro de 2003, diante do congresso americano, apud Nasheri (2005). Esta lógica de sobrevivência evolutiva torna o componente tecnológico da espionagem muito mais dinâmico que os meios jurídicos de combate. Logo, torna-se evidente que a pesquisa e o desenvolvimento de métodos de defesa são o modo mais eficiente contra as ameaças provenientes desta nova face dos conflitos econômicos.

2.4. As formas de perpetração e combate modernas

Segundo Nasheri (2005), o roubo de segredos industriais e a espionagem econômica acontecem em duas formas clássicas: um empregado insatisfeito utiliza seus conhecimentos internos sobre segredos da firma para seu ganho financeiro pessoal ou

para prejudicar a firma, ou uma concorrente desta firma ou nação estrangeira age para se apropriar das informações que achar vantajosas para seus interesses. King; Bravin (2000) afirmam que há uma gama variada de espiões provenientes de atividades diversas como: vendedores, investigadores, consultores, membros da imprensa, agentes governamentais, entre outros. Segundo King; Bravin (2000), há diversas maneiras de se obter informação, partindo de métodos primitivos como: espionagem em feiras de tecnologia, julgamentos de empresas e terminais de aeroportos ou roubo de equipamentos com dados armazenados, até métodos mais sofisticados como: monitoramento das comunicações do alvo e o uso de softwares para realizar *data mining* (forma de agregar e organizar dados, encontrando padrões, associações e mudanças dentro de um banco de dados). Essas ferramentas são utilizadas para neutralizar a vantagem que o desenvolvedor do objeto de monitoramento teria ao controlá-lo.

Durante os anos da guerra fria, havia uma possibilidade de conflito militar entre dois blocos distintos e bem definidos. Após o fim desta era, a supremacia econômica foi gradualmente se interligando ao conceito de supremacia militar. Este maior foco dos Estados em seu desenvolvimento econômico é um fator determinante para o redirecionamento da espionagem industrial de alvos majoritariamente militares, para alvos civis. Apesar da espionagem militar ainda ser essencial para as grandes potências mundiais, a busca por ganhos de competitividade em conhecimentos e produtos para uso civil é o novo foco dos serviços de inteligência no mundo, segundo Fink (2002). Esta evolução na visão dos países sobre a espionagem é fundamental para se compreender as novas formas de perpetração modernas, cada vez mais partindo de entes privados, ainda que com ajuda ou incentivo estatal, King; Bravin (2000).

As recentes revelações feitas por Edward Snowden, Julian Assange e outros grupos de jornalistas, mostram que há uma rede de monitoramento espalhada pelo mundo. Essa rede de monitoramento não é voltada somente para fins militares, mas, também para adquirir informações econômicas estratégicas. Como se tornou de conhecimento público após os vazamentos do WikiLeaks em 2010 e pelas revelações de Edward Snowden em 2013. Estas revelações envolviam o cometimento, pela agência americana NSA (*National Security Agency*), de atos de espionagem contra governos estrangeiros, incluindo países não hostis aos EUA. Diversos governos como o japonês, o alemão, o brasileiro e outros, foram vítimas deste tipo de ação, com empresas como: Mitsubishi, Siemens e Petrobrás estando, presentes entre os principais alvos do monitoramento americano. Para os Estados

Unidos, o ganho de informações privilegiadas é um objetivo constante de suas agências governamentais, não sendo somente uma estratégia de ganho de competitividade, mas também, como uma forma de defesa contra ações semelhantes de seus rivais.

As novas inovações têm, em sua maioria, uma característica comum em termos de interesse para agentes de espionagem, suas partes tangíveis e intangíveis. A tangibilidade de uma inovação é sua parte real e material, que pode normalmente ser codificada, a codificação de um conhecimento permite que haja um fácil entendimento e aprendizado sobre ele. A parte intangível de uma inovação, por sua vez, é um conhecimento muitas vezes tácito, de difícil reprodução e que requer um *know-how* próprio ao desenvolvedor. Por este motivo, a espionagem industrial moderna busca, sempre que possível, coletar informações sobre as partes intangíveis de um conhecimento, dado que este é imprescindível para certos processos, mercadorias e conhecimentos, tais como patentes e segredos industriais. Segundo Garner (1999), a absorção de um conhecimento intangível para um agente que não tenha desenvolvido o conhecimento em questão é um processo árduo que consome tempo e recursos. Contrariamente, no processo de espionagem, o roubo de conhecimentos tangíveis seria de maior facilidade que o roubo de recursos intangíveis. Ainda assim, há tentativas cada vez mais intensas de se obter conhecimentos intangíveis das empresas via espionagem industrial. Como corroborado pelo testemunho de Hefferman em 1996, que afirmou que os bens intangíveis das empresas norte americanas foram de 38% para 62% de seus respectivos valores de mercado, entre 1982 e 1992, apud Fink (2002). Por conseguinte, tornando-os atraentes para ações de espionagem, ao melhorar seu custo benefício.

Cria-se um dilema com a busca por defender-se das ameaças de espionagem. Se defender significa, em maior ou menor escala, se fechar; se fechar acarreta em perda de competitividade e escala. Por outro lado, manter-se aberto pode acarretar em aumento do risco de sofrer com ações de agentes de espionagem. As empresas modernas buscam encontrar um grau de abertura que as permita funcionar da forma mais segura e eficiente possível, isso implica em encontrar um equilíbrio entre a flexibilidade de procedimentos e comunicações (o grau de abertura da empresa) e seus mecanismos de defesa contra ameaças externas. As abordagens modernas de obtenção de informação por agentes podem usufruir de diversos meios para atingirem seus objetivos. Há diversos tipos de agentes que se configuram como ameaças para a segurança das empresas e países na fase

atual deste processo. Cada um destes agentes tem uma agenda e propósito específico, bem como um nível de ameaça próprio, como ilustrado na Figura 1.

Ameaças à segurança nacional	Agências de inteligência nacional	Vantagens estratégicas Informações para uso econômico e militar
Ameaças mútuas	Terroristas Espionagem industrial Crime organizado	Visibilidade e publicidade Vantagens competitivas Vingança e ganhos financeiros
Ameaças localizadas	Hacker institucional Hacker independente	Ganhos financeiros e prestígio Emoção e desafio

Figura 1, tipos de ameaças
Fonte: adaptado de Nasheri (2005)

O funcionamento destes agentes tem diversos pontos em comum, geralmente questões técnicas de operação. Porém, devido à variabilidade de propósito que cada um tem, há uma necessidade de segurança em áreas distintas da instituição ou empresa. Como se pode observar no quadro acima, boa parte das ameaças aos alvos pode ser definidas como ameaças mútuas, logo, há uma razão que serve de incentivo para que o setor privado colabore com o setor público. Em outros casos, os interesses de um país são simbióticos aos interesses das grandes firmas estabelecidas nele. Uma cooperação entre entes públicos e privados é fundamental para que se haja uma maior eficiência no combate aos agentes agressores. A partir do momento em que há troca de informações entre empresas e instituições estatais, voltadas a coibir estas atividades, se torna mais fácil combatê-las.

Devido ao caráter dissimulado destas ocorrências, há uma escassez de dados numéricos a respeito das perdas das vítimas. Por muitas vezes, o alvo da ação não tem nem mesmo conhecimento de sua perda. Ainda assim, existem órgãos e autores com dados e estimativas críveis disponíveis sobre o tema. Estes dados serão utilizados para

realizar uma tentativa de mensuração dos riscos a que uma firma pode estar sujeita, ainda que de forma estimada.

3. Análises de casos

Apesar da natureza da espionagem econômica-industrial não permitir uma grande exposição de suas ocorrências, devido ao grande número de ações que nunca são detectadas e a constância destas, pode-se ver diversos casos, de cernes distintos. Os fatores a serem analisados nestes casos são: a proveniência dos agentes envolvidos, a forma de condução da atividade de espionagem, as motivações dos agentes, o envolvimento de países, as defesas das empresas e a forma de reação legal dos Estados onde empresas foram vitimadas. Dentro dos casos observados, fica claro que há sempre uma linha tênue entre a espionagem de agentes privados e estatais. Por diversas vezes, há apenas a suspeita de malfeitos por parte de um país, sendo difícil obter provas cabais de envolvimento.

Os casos abaixo são relatos de ações de espionagem contra alvos diversos realizadas por meios diversos. O interesse econômico em novas tecnologias e métodos vai desde exemplos primitivos e relativamente simples, até situações complexas que envolvem a espionagem de pesquisas em andamento. A diversidade de situações que podem ser averiguadas demonstra que não há lugares seguros dentro da lógica de competitividade global. Sempre que há algo de diferente dentro de uma instituição ou empresa, haverá um interesse dos concorrentes em obtê-las ou estudá-las, por meios que podem, ou não, ser lícitos. Os casos 3.2, 3.3, 3.4 e 3.5 são provenientes de Fink (2002), que fez uma longa pesquisa referente a casos de espionagem industrial-econômica.

Para compreender a persecução penal dos envolvidos nos casos abaixo é preciso explicar o EEA (*Economic Espionage Act*), o ato de espionagem econômica foi uma ação legislativa do congresso americano que se tornou efetiva em 11 de outubro de 1996. O ato é uma longa e detalhada tentativa de oferecer proteção a pessoas e empresas que vierem a se tornar vítimas de roubo de sua propriedade intelectual ou outras maneiras de espionagem. A seção que mais gerou persecuções foi a de número 1832, que se refere ao roubo de segredo comercial. Os casos ocorridos anteriormente à realização e efetivação do EEA possuíam dificuldades em obter reparações justas ao dano sofrido.

3.1. Caso AMTORG

Zelchenko (1952), narra sua participação nas ações da companhia comercial soviético/americana AMTORG (*Amerikanskaia Torgovlia*). O caso AMTORG é uma ocorrência com paralelos nos dias atuais, tratando-se de um caso de espionagem sem fins diretamente militares, buscando roubar o conhecimento por trás de tratores, como o Fordson da Ford, e outros manufaturados americanos. A empresa era composta por comunistas americanos, cidadãos russos vivendo nos Estados Unidos e de cidadãos soviéticos. Setenta e cinco engenheiros soviéticos foram aos Estados Unidos na primavera de 1926, e passaram oito anos espionando diretamente centros de produção americanos e enviando os dados coletados para a União Soviética. Com o intuito de construir plantas industriais e produtos semelhantes. A espionagem ocorria com a desculpa de se adquirir os produtos manufaturados americanos. Ao visitar as fábricas americanas, os engenheiros soviéticos adquiriam parte do *know-how* dos engenheiros americanos, em alguns casos roubando diretamente documentos e diagramas, em outros perguntando diretamente sobre processo, sob o pretexto de "averiguar a qualidade".

A espionagem neste caso ocorria de maneira bastante primitiva e direta, mas demonstra claramente uma complexa relação público-privada com interesses estratégicos tanto de partes privadas, as empresas americanas, quanto de partes públicas, o Estado soviético e o Estado americano. Ocorrendo durante os anos de 1920 e 1930 esta situação mostra o descuido que as empresas americanas do início do século XX tinham com suas atividades, bem como uma ingenuidade, ao permitir a presença de potenciais concorrentes dentro de seus complexos industriais. O caráter internacional da espionagem industrial foi ficando cada vez mais evidente ao longo do século passado, com as empresas e países se tornando cada vez mais conscientes da gravidade deste tipo de ameaça. O caso AMTORG é relevante ao ser um prenúncio tanto das situações futuras trazidas pela guerra fria, quanto por ser um vislumbre da espionagem internacional futura com fins civis. A AMTORG em si sobreviveu até 1998, quando foi discretamente desfeita. Dos oito presidentes da empresa ao longo de sua existência, o primeiro morreu em condições suspeitas em Nova York e seus três próximos sucessores foram executados na União Soviética, durante os expurgos da década de 1930, no governo de Stalin, segundo Vaksberg (2011)

3.2. Caso Kodak

A ação de um homem chamado Harold Worden, um engenheiro com quase 30 anos de serviço na Kodak, é uma situação clássica de espionagem industrial, com sérias consequências para a empresa. Worden era diretamente responsável pelo design e projeto da máquina 401. A máquina 401 era um projeto de uma instalação de grande porte que visava acelerar e incrementar a qualidade da produção de filmes para câmeras. Worden era uma figura estratégica deste projeto, um dos poucos engenheiros que tinham conhecimento de todas as etapas de produção dos núcleos individuais e o responsável por decidir quais destas partes seriam patenteadas e quais permaneceriam como segredo industrial. Em 1992, antes do projeto 401 ser completado, Worden saiu da empresa e fundou sua própria consultoria para assuntos relacionados às suas atividades na Kodak. Esta empresa de consultoria acabou por contratar diversos engenheiros aposentados da Kodak, que prestavam serviços para as concorrentes de sua antiga empresa, como a alemã Afga.

O chefe da segurança institucional da Kodak, Pat Watson, um antigo agente do FBI, e o chefe do departamento legal, Brian O'Connor, decidiram conduzir uma investigação privada e só reportar às autoridades em caso de encontrarem evidências concretas. Após armar uma falsa reunião de negócios com Worden, fingindo representarem uma empresa estrangeira, O'Connor e Watson concluíram que segredos industriais estavam em risco e denunciaram ao FBI, com gravações secretas destes encontros. Após uma investigação demorada por parte da polícia federal americana concluiu-se que Worden havia deliberadamente comercializado segredos industriais da Kodak, Worden se declarou culpado e foi condenado a 15 anos de prisão, acrescidos de uma multa de 30.000 dólares, no ano de 1996. Os outros antigos funcionários da Kodak que se associaram a Worden fizeram, em sua maioria, acordos individuais com seu antigo empregador. A Kodak, por sua vez, pode processar as empresas que haviam adquirido os segredos de Worden e seus sócios, como a 3M e uma de suas subsidiárias italianas, a Imaton, pela aquisição fraudulenta de segredos industriais da Kodak.

Percebe-se que este caso foi um exemplo atípico de comportamento por parte da Kodak, com a empresa buscando resolver o problema de forma independente. Porém, é um exemplo clássico da antiga forma de atuação do agente agressor, sendo comum o emprego de antigos funcionários que atuavam em setores estratégicos da empresa para vazar dados confidenciais de suas antigas funções. O fato de Worden ter criado uma consultoria especializada em comercializar segredos industriais para qualquer

interessado, nacional ou estrangeiro, mostra o grau de periculosidade de uma situação envolvendo poucas pessoas. Entre antigos funcionários da Kodak, é difundida a ideia de que este episódio foi um dos grandes, e primeiros, marcos da longa decadência da empresa. É digno de nota que este caso é anterior ao EEA, logo, as dificuldades enfrentadas para trazer os responsáveis à justiça foram ainda maiores e mais custosas do que poderiam ter sido.

3.3. Caso Lucent Technologies

A empresa Lucent Technologies atuava no ramo das telecomunicações fabricando equipamentos para telefones, sendo uma subdivisão da AT&T. No ano de 2001, a Lucent Technologies estava à beira da falência, com suas ações despencando, e acumulando fracassos em série. Porém, a empresa ainda contava com um produto de sucesso, o sistema PathStar™, que havia movimentado US$ 100 milhões em vendas no ano anterior. Contribuindo para a ruína da empresa, o FBI descobriu que os antigos engenheiros chineses da empresa, que haviam desenvolvido o sistema PathStar™, haviam repassado os códigos do sistema para uma estatal de seu país natal. Hai Lin e Kai Chu foram presos por comercializar a tecnologia proveniente da Lucent. Os dois empregados, conjuntamente a um terceiro cúmplice chinês, eram sócios em uma empresa chamada ComTriad Technologies, que atuava em *joint venture* com a empresa chinesa Datang Telecom Technology Co. of Beijing. A Datang, por sua vez, era majoritariamente composta por capital estatal chinês, mas não houve provas conclusivas de que a Datang que estivesse por trás da ação ou que ela soubesse que estava adquirindo sistemas que eram propriedades da Lucent.

Este caso é particularmente semelhante ao ocorrido na Kodak, onde antigos funcionários saem da empresa onde desenvolveram as tecnologias e passam a atuar como uma concorrência desleal ao seu antigo empregador, com o agravante do envolvimento com estatais estrangeiras. A motivação dos agentes neste caso pode ser facilmente explicada pela ganância de se obter um ganho livre de custos. Quando os dois estudantes chineses entraram na Lucent Technologies eles puderam desenvolver um sistema a partir de seus conhecimentos, mas com os custos materiais vindo da sua empregadora. Ao sair de sua antiga empregadora e abrir a própria empresa, os perpetradores puderam usufruir de seus conhecimentos tácitos sem se preocupar com os custos de desenvolvimento de suas ideias. A motivação financeira é um dos principais fatores para que este tipo de ação

seja cometido, nem sempre sendo necessário um agente externo à empresa para a deflagração de ações como esta. Por diversas vezes as empresas interessadas na compra destes segredos podem encontrá-los em um mercado paralelo.

3.4. Caso Bristol-Myers Squibb Taxol (E.U.A. vs. Kai-lo Hsu)

A seção 1835 do EEA permite que a corte judicial tome providências para proteger o segredo de negócio da empresa envolvida. Em 1997, o EEA foi empregado para processar Kai-Lo Hsu por conspiração para roubo de segredos de comércio. O caso envolvendo Hsu se mostra emblemático para a compreensão do EEA e seu funcionamento. Durante o julgamento, a defesa de Hsu argumentou que devia ter acesso aos segredos em questão, invocando o direito do defendente de conhecer as provas contra si. A argumentação consistia em afirmar que o segredo da empresa era uma das provas contra Hsu, já que era o objeto que gerou a acusação. A promotoria argumentou que fornecer a fórmula do Taxol seria uma contradição clara com o EEA, que existe para garantir a integridade dos segredos dos desenvolvedores e mantenedores de um segredo industrial. Apesar de a primeira instância ter aceitado os argumentos da defesa, as cortes superiores rejeitaram esta argumentação, entendendo que revelar o segredo para a defesa seria a negação do que a EEA representa.

Fica clara a importância de mecanismos legais não somente para coibir os crimes, mas para tornar a persecução penal dos envolvidos eficiente. Os casos de espionagem industrial são complexos e arriscados, com o custo-benefício de se empreender as ações ilícitas sendo atrativo para os interessados. Devido a esta situação, a lei precisa ter a flexibilidade necessária para abranger todas as facetas que as ações de espionagem podem apresentar. Porém, esta flexibilidade não deve deixar margem a interpretações erradas, que possam ser prejudiciais às vítimas. O caso de Hsu demonstra que o EEA, neste caso, teve os mecanismos necessários para permitir a aplicação da lei sem comprometimentos para a vítima, mesmo que com tentativas reiteradas da defesa do agente agressor.

3.5. Caso LRI

A LRI (Lerner Research Institute), parte da CCF (Cleveland Clinical Foundation), estava desenvolvendo um medicamento para combater o mal de Alzheimer. Após identificar certas proteínas que ajudavam o corpo a resistir ao avanço da doença, os

pesquisadores começaram a fazer uma análise de DNA para compreender a produção destas proteínas. A pesquisa genética com usos para o mercado farmacêutico apresenta possibilidades de lucro elevadas no mercado atual. Dois pesquisadores japoneses, Takashi Okamoto e Hiroaki Serizawa, foram perpetradores de ações visando a apropriação dos conhecimentos gerados por esta pesquisa. Okamoto participou das pesquisas referentes ao mal de Alzheimer da LRI de janeiro de 1997 a julho de 1999. Serizawa, por sua vez, era ligado ao centro universitário médico da universidade do Kansas. Ligado a estes dois pesquisadores, aparece o instituto japonês Riken (Instituto para pesquisa Física e Química, em japonês). Este instituto recebia 94% de sua verba do governo do Japão, de acordo com o indiciamento subsequente ao caso. O propósito do instituto era promover as ciências químicas, físicas, biológicas e da engenharia. Em 1997, mesmo ano que Okamoto ingressa no LRI, este instituto abriu uma subdivisão que pesquisava a respeito de neurociência e combate ao mal de Alzheimer, segundo o processo judicial *United States vs. Takashi Okamoto and Hiroaki Serizawa* (2001). Okamoto e seus colegas pesquisadores conseguiram alguns progressos na área, mas, em janeiro de 1999 aceitou uma vaga como pesquisador na Riken. Utilizando suas prerrogativas de acesso ao LRI, Okamoto transferiu o conhecimento das pesquisas realizadas, para Serizawa. Houve ainda a destruição dos reagentes obtidos na pesquisa que estavam armazenados nos laboratórios do LRI, para sabotar a capacidade de desenvolvimento deste laboratório. Redirecionando seus colegas a procurar os reagentes no laboratório de Serizawa, Okamoto substitui-os por reagentes falsos e retornou ao Japão com os verdadeiros.

A complexa trama relatada anteriormente terminou com a abertura de inquérito contra ambos os pesquisadores japoneses, enquadrando-os no EEA, nas seções 1831 (espionagem econômica) e 1832 (roubo de segredo comercial). Deve-se ressaltar que a dificuldade teórica de responsabilizar os governos estrangeiros pelas ações de seus agentes se tornou prática neste caso. Há um espaço jurídico muito limitado para que se determine o grau de envolvimento do governo japonês e, consequentemente, persegui-los judicialmente. Este caso demonstra como as ameaças são generalizadas não sendo o alvo uma empresa, mas, uma instituição de pesquisa. Logo, observa-se uma necessidade crescente de ampliar o monitoramento sobre os membros de grupos de pesquisa e identificar as fontes de ameaças potenciais.

3.6. Caso francês

Em artigo de Jehl (1993), são apontadas tentativas do governo americano para frear ações de espionagem de países considerados aliados. O país usado para exemplificar a situação é a França, devido à suposta agressividade no país em suas atividades de captação de informação. O artigo narra o cancelamento da participação americana no show aéreo de Paris, em junho de 1993, devido a ameaça de que as empresas americanas fossem espionadas na ocasião. As potenciais vítimas eram: Boeing, McDonnell Douglas Corporation, The Lockheed Corporation e The General Dynamics Corporation. A suspeita foi reconhecida através de um memorando anônimo entregue à CIA (*Central Intelligence Agency*) que, por sua vez, notificou as empresas e aconselhou-as a não participarem do evento. Em outro caso, relatado em artigo do The New York Times (1991), os franceses são novamente protagonistas de um caso de espionagem. A acusação consistia em afirmar que a Air France inseria agentes do serviço secreto francês dentro de suas aeronaves e grampeava locais onde pessoas de interesse estivessem posicionadas. O ex-diretor do serviço de inteligência francês, Pierre Marion, confirmou em entrevista que a França havia incentivado atos de espionagem contra alvos americanos. Porém, a acusação contra a Air France foi negada por Marion, tendo sido feita por especialistas americanos em inteligência que optaram pelo anonimato. Marion afirmou também que, as ações de inteligência francesa contra os EUA ocorreram entre 1987 e 1989, contra a IBM e Texas Instruments. As duas firmas tinham contribuições importantes no mercado de computação nascente na década de 1980, e a espionagem tinha o intuito de ajudar a estatal francesa Bull. O oficial francês negou que a espionagem econômica tivesse gerado qualquer retorno para a França.

Em ambos os artigos publicados pelo The New York Times, a França é apontada como um competidor extremamente agressivo e ativo em práticas de espionagem. O artigo de Jehl (1993) afirma que a espionagem oriunda de países desenvolvidos é mais perigosa que a de países subdesenvolvidos. Um país desenvolvido já possui a capacidade industrial necessária para traduzir um conhecimento adquirido em lucro. Um país subdesenvolvido, por sua vez, não será um concorrente imediato. Além da França, os Estados Unidos consideram países como Coreia do Sul, Japão e outros membros da OTAN como ameaças à segurança de empresas americanas. Pode-se observar que os interesses nacionais são muitas vezes simbióticos aos de suas grandes empresas. As ações de espionagem econômica-industrial, tanto de defesa quanto de perpetração, são uma

realidade essencial para a competitividade no comércio internacional moderno, como visto nos casos acima.

3.7. Caso Brünnhilde

A operação *Brünnhilde*, nomeada em homenagem à heroína mítica germânica, foi uma operação da STASI (*Ministerium für **Sta**atss**i**cherheit)*, Ministério para a Segurança do Estado) para obter segredos industriais dos países membros da OTAN. A operação fez cerca de 20 incursões documentadas, conseguindo obter diversas informações estratégicas de empresas europeias. O serviço secreto belga tomou conhecimento desta operação através de um cidadão suíço, Dr. Jean Paul Soupert, um membro da operação da Alemanha Oriental e passou a ser um agente duplo. Com a colaboração do agente duplo suíço, os serviços de inteligência da Europa ocidental tomaram conhecimento de certas atividades dessa operação, alega-se que a operação conseguiu roubar o design dos componentes elétricos dos aviões *Concorde*. Segundo Heims (1982) dois funcionários da Kodak foram acusados de vender segredos de sua empresa para espiões da STASI, mas, foram inocentados no julgamento que se seguiu. A Kodak era encarregada de fazer registros dos componentes dos sistemas do *Concorde* e estes funcionários teriam vendido à Jean Paul Soupert parte destes registros. Porém, os funcionários foram absolvidos após o testemunho de Soupert que afirmou que a Kodak, durante a década de 1960, havia pago £5000,00 para incriminar seus funcionários.

Relevando as dúvidas a respeito da culpa do vazamento, pode-se observar que a espionagem industrial neste caso não era uma ação de competição entre empresas, mas sim, uma política de Estado. Elevar táticas desleais de competição à uma política de pública não é um fenômeno novo, como os casos relatados por Bergier (1975) podem mostrar, mas a magnitude e eficiência das ações são imensamente maiores. Durante a Guerra Fria (1945-1989) a informação era a arma mais poderosas dos países, com ambas as superpotências quase sempre empatadas durante a maioria do período qualquer ganho, mesmo que marginal, sobre a outra era buscado. Com a existência deste fator cria-se um mundo onde não há nenhuma área segura, pois, qualquer brecha poderia ser utilizada para alavancar uma das potências. Boa parte do salto nos casos de espionagem contemporâneos se deve às táticas desenvolvidas neste período. A importância do Estado na condução destas políticas mostra o caráter desenvolvimentista destas nações. Buscar ampliar a base industrial de seu país é uma atividade que acarreta em uma busca por

tecnologias, especialmente após o fim da Segunda Guerra Mundial (1939-1945). A operação *Brünnhilde* é um dos mais latentes exemplos da situação que gerou a situação pós-guerra fria nos países que faziam parte do Pacto de Varsóvia, Nasheri (2005). Após o colapso da União Soviética, os agentes de inteligência passaram a usar suas habilidades para continuar a espionar os países da Europa ocidental, incentivados por seus países natais ou empresas de seus países natais.

4. A mensuração do potencial de perda frente às ameaças contra o patrimônio

Ter consciência do quanto está em risco é o principal incentivo para se adotar as medidas de segurança necessárias, no entanto, trata-se de uma tarefa de difícil execução. Estabelecer um valor monetário para os ativos de uma empresa é algo bastante difundido e de extensa bibliografia, não consistindo em um problema para esta tentativa. Por sua vez, estabelecer uma mensuração para a gravidade da ameaça é muito mais complexo. Ao longo deste capítulo buscar-se-á estabelecer uma graduação das vulnerabilidades dentro de uma empresa e adaptá-la para a mensuração do potencial de perda de uma firma.

4.1. A manifestação das ameaças

Para que seja possível mensurar as possíveis vulnerabilidades, é necessário conhecê-las. Existem diversos tipos de ameaças a uma firma e é possível dividi-las em quatro categorias: físicas, operacionais, pessoais e técnicas. Cada uma destas será definida no decorrer desta seção.

A ameaça física é a menos complexa, é a presença de elementos não autorizados e com más intenções nas instalações da empresa, seja para roubar equipamentos e peças ou reproduzir algum objeto de interesse. Este tipo de ação direta era a mais frequente e uma das mais sérias ameaças externas ao patrimônio de uma empresa no passado, como visto em Zelchenko (1952). Com o advento das revoluções tecnológicas no setor de comunicações, métodos mais seguros de espionagem foram se tornando as maiores ameaças. No entanto, isso não significa que este método se tornou obsoleto por completo, ainda é significante, especialmente no setor manufatureiro.

As ameaças operacionais são as que ocorrem durante o funcionamento da empresa, como o monitoramento das comunicações da empresa, a engenharia social e a dispersão de informações durante o trabalho dos empregados. Engenharia social é um

conceito amplo, mas, é possível delimitá-lo neste caso como: *a manipulação deliberada de pessoas com o intuito de obter informações privilegiadas destas,* Winkler (1999). O grau da manipulação e da farsa para atingir os objetivos varia de caso para caso, dependendo do comportamento do alvo frente às tentativas. O método mais fácil de combate à engenharia social é a construção de uma *cultura de vigilância* dentro da empresa, segundo Fink (2002), onde se incentive o cumprimento de protocolos, respeito à hierarquia, autonomia de decisões limitada pelos protocolos e o conhecimento de quais são as informações sensíveis que nunca devem ser reveladas. Essa cultura de vigilância é um instrumento para os empregados se defenderem de ameaças diretas e indiretas, preparando-os a como se comportar no ambiente onde eles estão inseridos.

Segundo Mendell (2003) e Fink (2002), ameaças pessoais são as mais perigosas dentro de uma empresa, empregados insatisfeitos e ex-funcionários mal-intencionados podem causar um dano de grandes proporções à empresa, de uma maneira diretamente proporcional à importância do cargo que exerce ou exercia. É comum na literatura sobre o tema, encontrar exemplos de ex-funcionários montando consultorias para vender informações sigilosas da empresa. Como o caso do engenheiro Harold Worden, ex-funcionários da Kodak, descrito em Fink (2002). A empresa manter relações cordiais com as pessoas que trabalharam anteriormente nela é um mecanismo de defesa eficiente. Ao manter abertas as linhas de comunicações com estas pessoas, é possível continuar informado sobre as atividades destas, identificando potenciais ameaças aos interesses da firma. Outro mecanismo de defesa efetivo é o estabelecimento de contratos de confidencialidade com empregados em posições estratégicas, servindo para desestimulá-los de ofertar essa informação após serem desligados da firma. A segunda parte dos problemas com pessoal se dá com quem está efetivamente ligado à empresa. Encontrar e neutralizar ameaças dentro da própria firma é uma tarefa complexa e delicada, devido a afetar as relações entre membros da firma. O acesso às informações é a questão central dentro desta situação, restringir o acesso à informação para um número menor de pessoas é de vital importância para garantir a segurança. Ao ter um número menor de empregados com acesso a dados importantes, o monitoramento do fluxo de informações se torna menos complexo. No entanto, a restrição a informação pode acarretar em uma queda na produtividade média dos envolvidos. Fink (2002) defende que a firma faça uma análise rigorosa dos históricos de atividade dos empregados da firma na internet, de maneira a identificar possíveis ameaças.

As vulnerabilidades técnicas dizem respeito às fraquezas dos sistemas da empresa, tanto nas partes referentes aos sistemas quanto nas partes terceirizadas. Os sistemas de informação da empresa se tornaram fragilidades dentro da lógica de segurança. A comunicação e transferência de dados pela rede é um fator que gera grandes benesses para as empresas, qualquer limitação nestas áreas é um entrave na produtividade da empresa, Nasheri (2005). Percebe-se então que há um dilema entre a limitação das comunicações, para reduzir riscos inerentes à transferência de informação, e a produtividade média da empresa. Existem diversas medidas que podem ser tomadas para reduzir estes riscos inerentes, como será exposto ao decorrer deste capítulo. A espionagem decorrente de empresas terceirizadas com acesso à informações de sua contratante é uma realidade, como mostrado por Fink (2002) e Hanssen (2008). Para contornar esta situação, é necessário evitar manter empresas terceirizadas próximas de locais sensíveis da empresa ou internalizar o máximo possível de processos, quando possível.

4.2. Como mensurar o grau de vulnerabilidade dos ativos de uma empresa

Efetuar uma medição precisa de quanto do patrimônio de uma empresa está sob ameaça é uma tarefa complexa. Atividades de espionagem são clandestinas, portanto, não deixam registros consistentes de suas ocorrências. Porém a ASIS (*International American Society for Industrial Security*) possui análises referentes as áreas de maior risco dentro de uma empresa. Ao se saber quais são as vulnerabilidades apontadas dentro de uma empresa e seus respectivos "pesos", torna-se possível estimar um grau de vulnerabilidade, como é mostrado na tabela 1.

Tabela 1 - Vulnerabilidades de organizações

Vulnerabilidades físicas	**Contramedidas**	**Peso**
Invasão a áreas restritas	Controle através de obstáculos físicos e protocolos ao acesso destes locais.	7,50%
Vulnerabilidade de armazenamento de informações	Identificar quais informações são relevantes, controlar seu acesso e dispersão.	2,50%
Falsificação de status para obter acesso a áreas restritas	Estabelecer e respeitar protocolos de checagem de pessoal.	2,50%
Vulnerabilidades operacionais	**Contramedidas**	**Peso**
Vulnerabilidade do sistema de comunicações	Controle do pessoal autorizado a lidar com o sistema.	5,00%
Empregados com posse de informações fora da empresa	Evitar a dispersão de conhecimentos ou equipamentos importantes.	2,50%

Engenharia social	Limitar o poder decisório do empregado, estabelecer normas claras e específicas.	12,50%
Espionagem de empregados em convenções e eventos	Instrução sobre o tipo de ameaça que o ambiente pode proporcionar.	2,50%
Vulnerabilidades de pessoal	**Contramedidas**	**Peso**
Cooptação de ex-empregados	Manter contato com ex-empregados. Mecanismos contratuais de proteção.	12,50%
Empregados com problemas financeiros e/ou pessoais	Atenção aos empregados em situação de risco, oferecer ajuda para não incentivar a ameaça	2,50%
Displicência dos empregados com segurança	Treinamento e conscientização dos empregados. Estabelecer uma cultura de vigilância na empresa.	12,50%
Grupos de pesquisa com agentes infiltrados	Checagem de antecedentes. Dividir grupos de pesquisa.	2,50%
Contratação de empregados não confiáveis	Checagem de antecedentes. Não permitir acesso imediato à locais estratégicos.	2,50%
Empregados interessados em prejudicar a empresa	Monitoramento das atividades dos empregados na empresa, especialmente na rede.	5,00%
Vulnerabilidades técnicas	**Contramedidas**	**Peso**
Ataques cibernéticos	Criptografia das informações importantes. Reduzir pontos de acesso à rede.	12,50%
Empresas terceirizadas e fornecedores vendendo informações	Não utilizar mesmos fornecedores para todos os processos. Internalizar o máximo de atividades possíveis.	7,50%
Senhas com baixo nível de segurança	Troca regular de senhas.	2,50%
Falhas previamente conhecidas no sistema da empresa	Reparar falhas com celeridade, de forma a não as acumular.	5,00%

Fonte: Elaboração própria, com dados de Fink (2002).

Os pesos estabelecidos para cada vulnerabilidade não são regras estáticas e inflexíveis, são apenas medidas de grandeza para separar as ameaças de maior porte das de médio e pequeno porte. Para cada setor produtivo haverá uma prioridade específica, firmas de tecnologia e softwares darão muito mais valor a vulnerabilidades técnicas que as físicas, já uma empresa manufatureira não pode se dar ao luxo de negligenciar suas defesas físicas. As se somar as porcentagens designadas chega-se ao total de 100%, esse total representa o quanto da empresa está em risco sem nenhuma contramedida de defesa. Ao se aplicar todas as contramedidas citadas se chega ao valor teórico de 0%, aonde todos os ativos da empresa estão protegidos naquele momento. Para cada medida tomada, subtrai-se a sua porcentagem referente da porcentagem máxima, chegando-se então ao grau de vulnerabilidade dos ativos.

4.3. A mensuração dos ativos em risco da empresa

Ao se encontrar o grau de vulnerabilidade da empresa é necessário saber quais são os ativos em risco. Um ativo tangível é algo físico, como máquinas e equipamentos

pertencentes à firma. Um ativo intangível tem a mesma lógica de algo como uma patente, ou os gastos da firma com pesquisa e desenvolvimento. Explicar como se dá a mensuração do valor destes ativos é o próximo degrau na determinação do potencial de perda da empresa com espionagem.

4.3.1. O valor dos ativos tangíveis

O valor dos ativos tangíveis não será considerado, devido ao fato de que a espionagem industrial não busca este tipo de ativo. As atividades de espionagem têm o objetivo de buscar projetos, documentos ou informações, não sendo considerável, neste contexto, a busca pelo roubo de objetos físicos. Pode-se dizer que a ameaça aos ativos tangíveis é uma ameaça indireta, dependente da ameaça aos ativos intangíveis, que serão abordados a seguir.

4.3.2. O valor das informações possuídas pelas firmas

As informações que uma empresa possui são um alvo frequente de monitoramento das suas rivais. Essas informações dizem respeito aos clientes dessa firma ou sobre as decisões que ela tomará no futuro. Devido ao caráter estratégico dessas informações, pode-se atribuir um valor monetário a elas. Saber o padrão de consumo de um cliente é possível direcionar um tipo de marketing especifico a ele. Nos tempos atuais, isso se torna ainda mais importante devido à internet e as redes sociais. Ataques cibernéticos contra os sistemas de armazenamento das empresas são corriqueiros, como ao Yahoo, Gmail e Hotmail em 2014 ou à Google em 2009, onde aproximadamente um bilhão de contas foram invadidas. Roubar as informações armazenadas pelas empresas representa uma economia em pesquisas de mercado e em investimentos de marketing, o que gera vantagens comparativas sobre as rivais. A questão fundamental a respeito das informações estratégicas é como mensurar seu valor, neste trabalho será utilizada a lógica do perpetrador, onde o valor das informações será igual ao retorno de possuí-las menos o custo de obtê-las, como na seguinte equação:

$$R_E = R_I - C_I$$

Onde, R_E é o retorno esperado da informação, R_I é o retorno da informação e C_I é o custo de se adquirir, legalmente ou não, a informação. Há de se ressaltar que a informação não será considerada um ativo sujeito à depreciação, devido ao caráter de uso imediato.

Quando uma informação é adquirida, de forma legítima ou não, ela será utilizada no mesmo momento para a tomada de decisão da firma no mercado. Caso o custo de se adquirir a informação seja superior ao custo de se roubar a informação, considerar-se-á, neste modelo, que a firma irá optar pelo roubo. O custo de se roubar a informação sempre será especialmente baixo, não sendo necessárias infraestruturas complexas nem contratações custosas para a firma realizar ataques cibernéticos ou outro tipo de atividade de espionagem.

4.3.3. O valor das pesquisas e patentes da firma

Para se determinar o valor dos ativos intangíveis será utilizado o método encontrado em Sandner (2009), que consiste em mensurar o valor das patentes e os gastos em pesquisa e desenvolvimento da firma. A seguinte equação dará o valor da pesquisa e patentes produzidas e mantidas pela empresa:

$$PP_t^{Est} = PP_t^{In} + (1-\delta)\, PP_{t-1}^{Est}$$

Onde, PP_t^{Est} é o valor estocado de pesquisa e patentes no período "t", PP_t^{In} é o valor investido em pesquisa e patentes no período "t", $(1-\delta)$ é a taxa de depreciação destes ativos (na literatura especializada utiliza-se 15%, como em Sandner (2009)), e PP_{t-1}^{Est} é o valor estocado em pesquisa e patentes no período anterior, "t-1". Esse valor resultante, PP_t^{Est}, é o valor dos ativos intangíveis passíveis de espionagem. Quando uma empresa tem um de seus projetos roubados, não se perde somente o projeto em si, mas também, os ganhos de monopólio que ela obteria com a exclusividade da do que foi desenvolvido.

4.4. O potencial de perda da firma

A elaboração da equação de potencial de perda devido a atos de espionagem será elaborada utilizando todos os conceitos que foram levantados neste capítulo. Tanto o valor das informações quanto o valor de patentes e pesquisas serão multiplicados pelo coeficiente de vulnerabilidade, oriundo das porcentagens apresentadas anteriormente. A decisão de separar os ativos de informações dos demais intangíveis provém da vontade de facilitar a identificação de qual é a parte mais estratégica para a empresa ou organização. Ao se identificar a parte de maior importância é possível estabelecer prioridades de ação dentro da firma. A equação utilizada será a seguinte:

$$X_t = (R_E \times vul_{\%}) + (PP_t^{Est} \times vul_{\%})$$

Onde X_t é o potencial de perda no período "t"; R_E é o retorno esperado das informações em posse da firma; $vul_{\%}$ é o grau de vulnerabilidade onde $(0 \leq vul_{\%} \geq 1)$ e PP_t^{Est} é o valor das pesquisa e patentes pertencentes à firma no período "t".

Esta equação tem como objetivo servir como um referencial para se estabelecer prioridades. Ao uma empresa inserir seus dados dentro desta equação, ela pode identificar o quanto de seu patrimônio está ameaçado, bem como, quais são os componentes deste patrimônio ameaçado. Não se deve levar o valor resultante como um fato inquestionável, mas como um apontador de potenciais dificuldades que podem ser encontradas pela firma. Não é necessário utilizá-la de forma generalizada. Caso houver interesse em utilizar uma informação ou um equipamento específico para apenas um projeto, pode-se desmembrá-la da forma que for conveniente.

5. Considerações finais

5.1. Os ganhos obtidos pelos perpetradores

Os ganhos provenientes espionagem da econômico-industrial podem se apresentar de diversas maneiras. Ainda que o objetivo final seja o lucro proveniente do equipamento ou método roubado, há outras questões importantes a se considerar. A aquisição espúria de certa propriedade alheia pode trazer um ganho meramente momentâneo, de modo a apenas acompanhar uma concorrente que se encontre em uma posição mais avançada, sem ter qualquer contrapartida de longo prazo. Porém, há a possibilidade de que a aquisição da propriedade traga vantagens estratégicas de longo prazo. Os dois casos relatados por Bergier (1975) envolvendo a nação chinesa são emblemáticos destes ganhos estratégicos. Tanto a porcelana quanto a seda eram dois produtos de alto valor agregado, que se tornaram passíveis de reprodução por nações europeias, no caso da porcelana, e por principados indianos, no caso da seda. Percebe-se que este ganho de longo prazo ocorreu em um mundo onde havia um comércio internacional ainda bastante limitado, em comparação com os dias atuais. A chance de se perder uma propriedade nos dias atuais é muito maior, e mais ameaçadora, como visto em Fink (2002), no caso Lucent Technologies. Se para os antigos chineses a perda de suas vantagens tecnológicas só se traduziu na decadência de sua civilização séculos depois, no mundo moderno e comercialmente interligado de hoje as empresas perdedoras podem decair em questão de

anos. A questão da perda para as empresas modernas é complexa, por muitas vezes elas não tem consciência da perda, percebendo somente quando já é tarde demais, como dito por Fialka (1999). Para se desenvolver uma inovação, tempo e recursos são consumidos e estes fatores se traduzem como custos para uma firma. Porém, uma empresa que adquira esta inovação de forma espúria não tem nenhum destes custos, como explicitado no caso Kodak. Logo, o produto roubado pode se tornar mais competitivo que o desenvolvido. É digno de nota que este ganho de competitividade só será pleno e sustentável a longo prazo se os métodos por trás da propriedade roubada sejam conhecidos, para que os conhecimentos tácitos e codificados por trás da inovação sejam, pelo menos em parte, absorvidos.

A queima de etapas devido à apropriação maliciosa de certo conhecimento é outro fator fundamental no ganho estratégico que pode vir a ser obtido. Como visto no estudo de Harris (1989), durante o século XVIII, a França e outros países como o Reino da Prússia, Império Russo, Suécia, Dinamarca e Espanha enviaram agentes para espionar as instalações industriais inglesas. Um processo de industrialização orgânico e interno de um país depende da criação de um *know-how* próprio, que pode levar décadas para começar a se desenvolver. Ao se apropriar de métodos estrangeiros para seu desenvolvimento, uma nação pode poupar um tempo vital em seu desenvolvimento econômico. Esta forma de desenvolvimento teve um paralelo histórico recente. Com a queda do bloco soviético, os países do pacto de Varsóvia passaram a utilizar seus agentes de inteligência para obter o *know-how* dos países mais tecnologicamente avançados, o oeste europeu e os Estados Unidos da América. Ainda que os países desenvolvidos sejam alvos atraentes, isso não os torna necessariamente vítimas, como visto nos vazamentos de Edward Snowden e Julian Assange, nesta década, bem como nas ações dos governos japonês e francês, mostradas anteriormente.

As equações apresentadas anteriormente são uma tentativa de quantificar, ainda que de forma aproximada, o que há a se ganhar ou a se perder em uma tentativa bem-sucedida de espionagem. Ainda que existam imprevisões inerentes a qualquer aproximação de um modelo com a realidade, pode-se observar o quanto é possível perder devido a questões triviais. Devido aos fatores apresentados anteriormente, podemos estabelecer que o ganho depende da capacidade do agressor em fazer uso do que obteve. Um agressor que já possua as bases tecnológicas necessárias para a produção do que foi

roubado é extremamente mais perigoso do que o agressor que busca começar sua base, como visto no caso da Air France, relatado por Jehl (1993).

5.2. Perspectivas sobre à manifestação de fenômenos de espionagem econômica-industrial

Quanto mais difundidas são as relações de comércio entre os países, mais ações de espionagem econômica-industrial podem ser esperadas. A velocidade com que as inovações, nos ramos mais dinâmicos dos setores intensivos em capital, são geradas causa um poderoso incentivo para que as empresas busquem economizar recursos em pesquisa e desenvolvimento. Não são somente empresas privadas e estatais que se encontram em risco, as instituições de pesquisa também são alvo. A pesquisa e desenvolvimento, mesmo que feita sem fins lucrativos e em ambientes acadêmicos pode ser extremamente atraente para agentes estrangeiros, como observado previamente no caso LRI.

Devido aos baixos custos relativos da aplicação destas ações, bem como as limitações nas repressões e represálias, pode-se crer que a espionagem econômica-industrial continuará a ocorrer. A lei econômica que afirma que os agentes respondem a incentivos pode ser vista claramente nesta situação, altos retornos com baixos riscos são uma garantia de ver agentes se engajando nestas atividades. Por este ponto de vista, o Estado é responsável por tentar aumentar os riscos para os perpetradores, seja blindando legalmente os obtentores e desenvolvedores de tecnologia ou investindo em contra inteligência para melhor identificar as ameaças. As empresas, por muitas vezes, são relapsas com sua segurança. Como os casos apresentados anteriormente mostram. Ter consciência dos riscos e buscar produzir um ambiente de trabalho hostil a ações de espionagem é um passo crucial para a segurança da empresa e de seus ativos.

Percebe-se que a espionagem econômica-industrial é uma realidade que remonta há centenas de anos atrás, mas intensificou-se com o advento da revolução nas comunicações e na ampliação do comércio internacional. Caso mantenham-se as características da espionagem econômica-industrial moderna (baixo custo, baixo risco de punição, disponibilidade de meios e etc.), a busca por garantir segurança às informações e propriedades, de países e empresas, se intensificará. Essa intensificação se dará como uma corrida evolutiva entre os meios de perpetração e os mecanismos de defesa, como pode ser observado nos exemplos. Ao longo da História, a tecnologia foi uma ferramenta

para ambos os participantes da corrida, em mesmo tempo que surgem ferramentas para agredir, surge a necessidade de novas ferramentas para a defesa.

Não se deve considerar a constante ameaça de se perder uma propriedade intelectual como um desincentivo para o processo de inovação dentro de uma organização. Ainda que seja possível sofrer perdas consideráveis por essas ações, e que qualquer mecanismo de defesa é limitado e passivo de falhas, deixar de investir em inovações ou em informações é uma sentença de morte a qualquer empresa. A geração de conhecimento é e sempre foi a mais valiosa forma de se adquirir ganhos competitivos frente aos adversários. O mero fato de ser um alvo frente aos seus rivais já é um forte sinal da posição superior de uma empresa, ao menos no ramo em questão. A lógica por trás da espionagem industrial é a da manutenção de uma cultura de vigilância, ainda que uma empresa tenha diversos recursos materiais a sua disposição, os mais importantes pontos de defesa são os próprios membros da organização, lembrando uma frase do estadista espartano Licurgo (800-730 a.C.) *"A cidade bem fortificada é aquela que tem uma muralha de homens ao invés de uma de pedras".*

6. Referências

BERGIER, J. **Secret Armies: The Growth of Corporate and Industrial Espionage.** Indianápolis: Bobbs-Merrill, 1975.

FIALKA, J. **War by Other Means: Economic Espionage in America**. New York: Norton & Company, 1999.

FINK, S. **Sticky Fingers: Managing the Global Risk of Economic Espionage**. Chicago: Dearborn Trade, 2002.

GARNER, B. A. **Black's Law Dictionary**. 7th ed. St. Paul: West Group, 1999.

HANSSEN, E. **Industrial Espionage – a Management Perspective**, 2008. University of Wales.

HARRIS, J. R. French Industrial Espionage in Britain in the Late Eighteenth Century. **RSA Journal**, v. Vol. 137, p. 629–634, 1989.

HEIMS, P. A. **Countering Industrial Espionage**. Leatherhead, Surrey: Century Security Education Ltd, 1982.

JEHL, D. U.S. Expanding Its Effort to Halt Spying by Allies. **The New York Times**, 1993. New York.

KING, N.; BRAVIN, J. Call It Mission Impossible, Inc. – Corporate Spying Firms Thrive. **Wall Street Journal**, 2000.

MENDELL, R. L. **The Quiet Threat**. 2nd ed. Springfield, Illinois: Charles C. Thomas, 2003.

NASHERI, H. **Economic Espionage and Industrial Spying**. New York: Cambridge University Press, 2005.

SANDNER, P. **The Valuation of Intangible AssetsGabler**, 2009. Ludwig-Maximilians-Universität.

THE NEW YORK TIMES. Air France Denies Spying on Travelers. **The New York Times**, 1991. New York.

VAKSBERG, A. **Toxic Politics: The secret history of the Kremlin's poison laboratory – from the Special Cabinet to the death of Litvinenko.** Santa Barbara, Calif: Praeger, 2011.

WINKLER, I. S. Case Study of Industrial Espionage Through Social Engineering. **National Computer Security Association**, p. 7, 1999. Disponível em: <https://www.researchgate.net/publication/2237195_Case_Study_Of_Industrial_Espion

age_Through_Social_Engineering>. .

ZELCHENKO, H. L. Stealing America's Know-How. **American Mercury**, p. 75–84, 1952. New York.