ROBERTO FERRAZ EBOLI

A IMPORTÂNCIA DO CREDENCIAMENTO DE SEGURANÇA DAS ENTIDADES PRIVADAS VINCULADAS AO COMANDO DA AERONÁUTICA

Trabalho de Conclusão de Curso - Ensaio apresentado ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do diploma do Curso Superior de Inteligência Estratégica.

Orientador: Carlos Eduardo Malafaia Silva.

Rio de Janeiro
2020

C2020ESG

_____

ROBERTO FERRAZ EBOLI

Dados Internacionais de Catalogação na Publicação (CIP)

E16i Eboli, Roberto Ferraz

A importância do credenciamento de segurança de entidades privadas vinculadas ao Comando da Aeronáutica / Roberto Ferraz Eboli. - Rio de Janeiro: ESG, 2020.
28 f.

Orientador: CMG FN (RM1) Carlos Eduardo Malafaia Silva
Trabalho de Conclusão de Curso - Monografia apresentada ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do diploma do Curso Superior de Inteligência Estratégica (CSIE), 2020.

1. Segurança nacional - Brasil. 2. Espionagem industrial. 3. Base Industrial de Defesa (BID). 4. Inteligência competitiva (Administração). I. Título.

CDD – 330.981

Elaborada pelo bibliotecário Antonio Rocha Freire Milhomens – CRB-7/5917

AGRADECIMENTO

Primeiramente a Deus por permitir que mais uma vez conseguisse vencer os desafios dessa nobre carreira que me preparaste.

À minha família que mesmo nesse momento de dificuldade, consequência da pandemia que o mundo está enfrentando, demonstraram compreensão pelo meu momento de dedicação aos estudos na ESG e me incentivaram a buscar o crescimento profissional e pessoal.

À Força Aérea Brasileira por me confiar esta oportunidade de aprimoramento dos meus conhecimentos profissionais.

Aos colegas estagiários da Turma do CSIE-2020, Turma "Confidere", pelo convívio, que apesar de curto, foi harmonioso e enriquecedor.

Ao Corpo Permanente da ESG pelos ensinamentos, orientações, e principalmente pela dedicação demosnstrada ao conduzir o curso de forma tão profissional diante te tantas adversidades ocorridas no período.

Por fim, ao meu orientador, por aceitar-me como orientado, e por sua dedicação e serenidade transmitida, o que contribuiu sobremaneira para atingir todos os objetivos propostos.

RESUMO

A falta de cultura de segurança na sociedade brasileira tem se mostrado um fator preocupante para a comunidade de Inteligência no Brasil. Inclusive as empresas de defesa, que compõem a Base Industrial de Defesa, enfrentam as consequências do descaso com os investimentos em segurança. O fenômeno da globalização é desleal, impõe competição, gera oportunidades e ameaças. Nesse contexto, a Inteligência adversa aproveita-se do conceito de Inteligência Competitiva, muito comum no mundo corporativo, e ultrapassa os limites da legalidade, ao utilizar de ações como a espionagem industrial, sabotagem e ataques cibernéticos para obter vantagens nesse ambiente de disputa comercial, econômica e de defesa. Atentos a esse cenário, após a entrada em vigor da Lei de Acesso a Informação, em 2012, diversas legislações surgiram com a finalidade de orientar e normatizar o tratamento de informações classificadas nesse ambiente de ameaças. Dessa forma, este ensaio tem como objetivo demonstrar a importância da aplicação dessas legislações, por parte do Comando da Aeronáutica, não apenas como um simples cumprimento da lei vigente, mas como uma atividade fundamental de manutenção da mentalidade de segurança nessas empresas, e alinhamento aos interesses nacionais. Após uma pesquisa bibliográfica e documental, foram analisados dados e relatórios que confirmaram a hipótese apresentada ao revelar que as entidades privadas, ao serem submetidas ao processo de habilitação de segurança, de um modo geral, têm fortalecido sua cultura de segurança, através da adoção de práticas cada vez mais eficazes de salvaguarda do conhecimento sensível, que se apresenta como o principal patrimônio e recurso estratégico dessas organizações.

Palavras-chave: Mentalidade de segurança. Base Industrial de defesa. Inteligência Competitiva. Espionagem Industrial. Conhecimento sensível.

ABSTRACT

The lack of safety culture in Brazilian society is a worrying factor for the Intelligence community in Brazil. Including defense companies, which make up the Industrial Defense Basis, face the consequences of neglect with investments in security. The globalization phenomenon is unfair, imposes competition, creates opportunities and threats. In this context, adverse Intelligence takes advantage of the concept of Competitive Intelligence, very common in the corporate world, and goes beyond the limits of what is legal, when using actions such as industrial espionage, sabotage and cyber attacks to obtain advantages in this environment of commercial, economic and defense dispute. Aware of this scenario, after the Access to Information Law went into effect in 2012, several laws have emerged in order to guide and standardize the treatment of classified information in this threat environment. Thus, this essay aims to demonstrate the importance of the application of these laws, by the Air Force Command, not only as a simple compliance of the current law, but as a fundamental activity of maintaining the safety mentality in these companies, and alignment to the national interests. After a bibliographic and documentary research, data and reports were analyzed that confirmed the hypothesis presented when revealing that private entities, when submitted to the security clearance process, in general, have strengthened their security culture, through the use of increasingly effective practices to safeguard sensitive knowledge, which is presented as the main asset and strategic resource of these organizations.
Keywords: *Security mentality. Industrial Defense Basis. Competitive intelligence. Industrial espionage. Sensitive knowledge.*

SUMÁRIO

1 INTRODUÇÃO

No Brasil a mentalidade de segurança das pessoas, no que diz respeito principalmente à percepção de ameaças, é muita baixa. Esse fato se reflete diretamente nas medidas de segurança de muitas empresas do território nacional. À exceção de experientes multinacionais e determinados órgãos estatais que mantêm equipes próprias e/ou contratam regularmente serviços especializados em medidas de Contrainteligência[1] (CI), normalmente encontra-se um território livre para os mais diversos tipos de ataques ao patrimônio intangível.

Ocorre ainda que muitas vezes as medidas de segurança não são levadas em conta, pois "custa caro", como dizem alguns. Ou "Qual o retorno sobre o investimento?", questionam outros. Porém, para os especialistas, uma atitude proativa, centrada na antecipação, que somente um sistema de Contrainteligência pode proporcionar, é de valor inestimável.

Nesse contexto, os gestores de segurança de muitas entidades privadas, enfrentam diversas dificuldades para adequar as empresas aos requisitos necessários para serem habilitadas ao tratamento de informações classificadas. A falta de profissionais especializados, bem como o contexto cultural em que estão inseridos, dificultam a percepção das ameaças e análise correta dos riscos.

Diante dessas dificuldades, e por envolver informações estratégicas e sigilosas, a entidade privada a qual mantenha vínculo de qualquer natureza com o Comando da Aeronáutica (COMAER) e que necessite tratar informação classificada em qualquer grau de sigilo deverá ser submetida ao processo de credenciamento de segurança prevista no Decreto nº 7.845, de 14 de novembro de 2012 (BRASIL, 2012b), e na Norma Complementar nº 1 da Instrução normativa nº 2/NSC/GSI/PR, 27 de junho de 2013 (BRASIL, 2013).

Compete ao Centro de Inteligência da Aeronáutica (CIAER) estabelecer os procedimentos para concessão de credencial de segurança[2] às pessoas naturais e habilitação[3] às pessoas jurídicas, vinculadas ao COMAER e que necessitem, por força

---

[1] Atividade que objetiva prevenir, detectar, obstruir e neutralizar a Inteligência adversa e as ações que constituam ameaça à salvaguarda de dados, conhecimentos, pessoas, áreas e instalações de interesse da sociedade e do Estado" (BRASIL, 2016, p. 1).

[2] Certificado que autoriza pessoa para o tratamento de informação classificada, contudo, não exime o credenciado das responsabilidades administrativas, cíveis e penais quanto à manutenção da segurança dos ativos de informação classificados (BRASIL, 2013, p. 2).

[3] Habilitação: condição atribuída a um órgão ou entidade pública ou privada, que lhe confere a aptidão para o tratamento da informação classificada em determinado grau de sigilo (BRASIL, 2013, p. 2);

de suas atribuições, ter acesso a informações classificadas em qualquer grau de sigilo (BRASIL, 2017, p. 11).

Assim, considerando a parcela de tempo e investimentos desprendidos nas inspeções de segurança, bem como toda a assessoria envolvida no processo, torna-se fundamental demonstrar a importância dessa atividade especializada, não apenas como um simples cumprimento da lei vigente, mas como uma atividade fundamental de manutenção da mentalidade de segurança, que contribui com a preservação do conhecimento a nível estratégico e consequentemente os interesses nacionais, a partir de uma análise do cenário de ameaças que estão inseridas essas empresas, responsáveis pela produção parcial ou integral de materiais e equipamentos de Defesa.

A metodologia aplicada se baseia em pesquisa bibliográfica e documental, com o propósito de se desvelar o cenário em que a indústria de defesa está inserida, bem como analisar a hipótese de que o processo de credenciamento de entidades privadas, além de simplesmente cumprir com o estabelecido nas leis vigentes, contribui substancialmente com o aumento da mentalidade de segurança e a percepção das ameaças dessas empresas.

Prosseguir-se-á examinando-se as leis, decretos, instruções normativas e outros documentos que contribuem com a implementação de medidas eficazes de prevenção à espionagem industrial, sabotagem, e ataques cibernéticos, diferenciando essas ações adversas da atividade de Inteligência Competitiva (IC) que, ao contrário dessas ameaças, oferece um viez assertivo, ético e voltado aos objetivos institucionais da empresa.

Na penúltima seção, serão analisadas as principais dificuldades das entidades privadas durante o processo de credenciamento, o funcionamento do serviço do COMAER, que concentra os pedidos e processos de credenciamento de pessoas naturais, bem como será apresentado a análise dos dados obtidos com a pesquisa documental realizada pelo Sistema de Credenciamento da Aeronáutica (SISCRED) no período indicado.

Por fim, serão expostos os comentários a respeito de todo o conteúdo exposto, com o objetivo de confirmar ou refutar a hipótese proposta.

2 BASE INDUSTRIAL DE DEFESA

A análise desenvolvida neste artigo exige, previamente, a delimitação do conceito de Base Industrial de Defesa (BID). O Livro Branco de Defesa Nacional[4] (BRASIL, 2012d, p. 212) traz o seguinte conceito:

> Base Industrial de Defesa é um conjunto de indústrias e empresas organizadas em conformidade com a legislação brasileira, que participam de uma ou mais das etapas da pesquisa, desenvolvimento, produção, distribuição e manutenção de produtos de defesa[5]. Uma indústria de defesa competitiva e consolidada gera empregos qualificados e incentiva o desenvolvimento tecnológico com encadeamentos produtivos para outros setores da indústria.

A Estratégia Nacional de Defesa (END) estabelece diretrizes para a adequada preparação e capacitação das Forças Armadas Brasileiras, enfatizando a necessidade do fortalecimento dos setores estratégicos na busca do desenvolvimento nacional. Dentre outras diretrizes, merece destaque a necessidade do desenvolvimento do potencial de mobilização militar e nacional para assegurar a capacidade dissuasória e operacional das Forças Armadas (BRASIL, 2019a).

Com isso, percebe-se que defesa e desenvolvimento sempre caminham juntos, considerando ainda, que os investimentos na capacitação das Forças Armadas criam oportunidades que favorecem a inovação e o crescimento econômico.

O Ministério da Defesa (MD) trabalha na implementação de políticas e iniciativas que busquem associar a recomposição da capacidade operativa da Marinha, do Exército e da Aeronáutica à busca de autonomia tecnológica e ao fortalecimento da BID.

No início da década de 80, período mais áureo da indústria de defesa do país, o Brasil já teve a quinta maior indústria de defesa do mundo, com faturamento de mais de US$ 2 bilhões por ano em carros de combate, aviões, mísseis e armas leves. Em 2008 atingiu seu patamar mais baixo, com redução de aproximadamente 90%, praticamente apenas com a venda de armas leves e munições, produtos com menor valor agregado (Mawakdiye, 2006, apud Dellagnezze, 2008, p. 38).

Passado esse período de encolhimento e estagnação, a BID vivencia hoje renovada expectativa quanto ao seu crescimento, tendo como pano de fundo uma

---

[4] Publicação oficial do governo brasileiro criado pela Lei Complementar nº 136, de 25 de agosto de 2010, e lançado em 2012. Trata de assuntos referentes a defesa nacional e de competências do Ministério da Defesa, sobre os objetivos, avanços e desafios da sociedade brasileira em sua correlação no mundo em matéria de defesa nacional (BRASIL, 2012c).

[5] É todo bem, serviço, obra ou informação, inclusive armamentos, munições, meios de transporte e de comunicações, fardamentos e materiais de uso individual e coletivo utilizados nas atividades finalísticas de defesa, exceto de uso administrativo (BRASIL, 2012c, p. 214).

maior influência do país no cenário internacional. Trata-se de um “novo protagonismo com papel mais destacado das Forças Armadas, com o objetivo de melhor capacitá-las a cumprirem seus objetivos de defesa dos interesses nacionais e de garantia da segurança nacional” (ANDRADE, I. O. *et al*, 2016, p. 7).

Além de ser fundamental para a garantia da soberania do país, a BID também desempenha importante papel econômico e científico-tecnológico. Tanto quanto manter indústrias, parques de produção e empregos, os esforços empreendidos visam fazer com que o país, a partir desse setor, possa desenvolver novos modos de incorporar ciência, tecnologia e inovação nos bens e serviços produzidos.

2.1 EMPRESAS DE DEFESA E ESTRATÉGICAS DE DEFESA

É fundamental a obtenção das capacidades militares de defesa por meio do desenvolvimento da base industrial, científico-tecnológica e logística do País, bem como o seu conhecimento. Torna-se, portanto, essencial contar com empresas envolvidas com pesquisa, desenvolvimento, produção e serviços para atendimento das necessidades da Defesa Nacional.

Empresas de Defesa (ED) são “todas as pessoas jurídicas, cadastradas em conformidade com as normas, que produzam sistemas ou produtos de defesa no território nacional ou que integre as cadeias produtivas da indústria de defesa” (BRASIL, 2019a, p. 7).

De acordo com a Lei nº 12.598 (BRASIL, 2012c) entende-se por Empresa Estratégica de Defesa (EED) toda empresa de defesa credenciada pelo Ministério da Defesa mediante o atendimento cumulativo das seguintes condições:

> a) ter como finalidade, em seu objeto social, a realização ou condução de atividades de pesquisa, projeto, desenvolvimento, industrialização, prestação dos serviços, produção, conservação, revisão, conversão, modernização ou manutenção de produtos estratégicos de defesa (PED)[6] [...];
> b) ter no País a sede, a sua administração e o estabelecimento industrial, equiparado a industrial ou prestador de serviço;
> c) dispor, no País, de comprovado conhecimento científico ou tecnológico próprio [...];
> d) assegurar, em seus atos constitutivos ou nos atos de seu controlador direto ou indireto, que o conjunto de sócios ou acionistas e grupos de sócios ou acionistas estrangeiros não possam exercer em cada assembleia geral número de votos superior a 2/3 (dois terços) do total de votos [...]; e
> e) assegurar a continuidade produtiva no País;

[6] PED é todo bem (recursos bélicos navais, terrestres e aeroespaciais), serviço (técnicos especializados na área de projetos, pesquisas e desenvolvimento científico e tecnológico), obra ou informação (inclusive armamentos, munições, meios de transporte e de comunicações, fardamentos e materiais de uso individual e coletivo) de interesse estratégico para a Defesa Nacional, tanto pelo conteúdo tecnológico quanto pela dificuldade de obtenção ou imprescindibilidade (BRASIL, 2019a).

2.2 ED E EED VINCULADAS AO COMAER

A estrutura da END tem como um dos seus eixos o fortalecimento da BID, que assegura o atendimento às necessidades de produtos de defesa tecnologicamente avançados e de profissionais altamente capacitados com o intuito de reduzir a dependência externa e manter os requisitos operacionais das Forças Armadas Brasileiras (BRASIL, 2019b, p. 4).

A Secretaria de Produtos de Defesa do MD promove a relação entre as empresas e as Forças Armadas, para o desenvolvimento dessas tecnologias, a industrialização de novos produtos e o seu uso dual (civil e militar) na sociedade brasileira (BRASIL, 2019b, p. 4).

As parcerias com as ED e EED alavancam os projetos estratégicos das Forças Armadas que se apresentam em três setores destacados para Defesa Nacional: o nuclear, o cibernético e o espacial. O domínio e a salvaguarda de novas tecnologias e o aumento da produtividade e da diversidade na indústria brasileira asseguram a capacidade operacional das Forças.

Considerado um dos principais setores com capacidade para impulsionar o conhecimento tecnológico, aumentar a exportação de produtos com maior valor agregado e trazer benefícios à economia brasileira, os investimentos em defesa, ao efetuar aquisições de equipamentos militares, devem adotar medidas para se tornar cada vez mais competitivo, com acordos de cooperação que possibilitem amplo crescimento tecnológico (BRASIL, 2019b, p. 32).

Nessa linha de raciocínio, no âmbito da Força Aérea Brasileira (FAB), surgiu o projeto F-39 Gripen E/F a partir da necessidade de reequipar a FAB com aviões de caça de última geração, e incorporar avanços tecnológicos importantes na Base Industrial de Defesa brasileira através do programa de transferência de tecnologia.

Outro projeto vinculado a FAB e muito importante para o desnvolvimento da BID brasileira é o KC-390. Trata-se da maior aeronave militar já produzida no Brasil, e representa um marco na excelência de gerenciamento de projetos da Força.

Além da Embraer Defesa e Segurança, mais de 50 empresas brasileiras participam do projeto, e conta ainda com a colaboração da Argentina, de Portugal e da República Tcheca. Trata-se de um projeto que introduziu o Brasil em um nicho de mercado até então dominado apenas por grandes empresas internacionais.

A Tabela 1 traz informações sobre as empresas vinculadas diretamente a esses e outros projetos sob responsabilidade do COMAER, e que são responsáveis pela produção parcial ou total de diversos produtos estratégicos de defesa:

Tabela 1 – Entidades Privadas vinculadas ao COMAER.

Entidade Privada	Tipo	Localização	Principais PED
EMBRAER Defesa & Segurança	EED	Gavião Peixoto-SP	Aeronaves militares e soluções integradas de Comando e Controle (C4I)[7], radares, ISR[8] e espaço.
AKAER Engenharia	EED	São José dos Campos-SP	Soluções tecnológicas em diferentes áreas: aeroespacial, defesa e espaço.
AVIBRAS Indústria Aeroespacial	EED	São José dos Campos-SP	Tecnologias críticas nas áreas aeronáutica, espacial, eletrônica, veicular e de defesa.
AEL Sistemas	ED	Porto Alegre-RS	Sistemas eletrônicos militares e espaciais.
ATMOS Sistemas[9]	EED	São Paulo-SP	Equipamentos eletrônicos, como radares climáticos e serviços de manutenção e suporte para defesa.
MECTROM-COMM	ED	Porto Alegre-RS	Sistemas de comunicação segura para plataformas aéreas, marítimas e terrestres.
KRYPTUS	EED	Campinas-SP	Defesa Cibernética.
IACIT Soluções Tecnológicas	EED	São José dos Campos-SP	Produtos e sistemas aplicados ao auxílio e ao controle do tráfego aéreo e marítimo (CNS/ATM); meteorologia radar; comunicação; e defesa.
SAAB Aeronautica Montagens	ED	São Bernardo dos Campos-SP	Produção em território nacional alguns segmentos aeroestruturais da aeronave F-39 Gripen E/F.

Fonte: Guia de Empresas e Produtos de Defesa (BRASIL, 2019a).

Considerando as condições listadas na Lei nº 12.598 (BRASIL, 2012c), que diferem ED e EED, observa-se que não são consideradas EED, a empresa suéca SAAB Aeronautica Montagens (SAM), e as empresas AEL Sistemas e Mectron-Comm que são subsidiárias da empresa israelita Elbit Systems.

A necessidade humana por informações sobre o inimigo ou nesse caso, os concorrentes, remonta à antiguidade, e a produção de informações estratégicas iniciaram na Segunda Guerra Mundial (PLATT, 1967, p. 20). Como veremos a seguir, os métodos e técnicas destinadas a obter essas informações, aprimoradas durante o período da Guerra Fria, no mundo atual deixaram de ser privilégio dos estados nacionais, e foram introduzidos no mundo corporativo.

[7] Comando, controle, computadores, comunicação e inteligência, todas interligadas entre si, fazendo com que toda a operação seja coordenada, e minimize as perdas.
[8] Inteligência, vigilância, aquisição de alvos e reconhecimento é a atividade de equipar as forças armadas com informações e inteligência para auxiliar nas funções de combate e outras tarefas operacionais.
[9] A empresa suéca SAAB firmou um contrato para adquirir a empresa brasileira de defesa ATMOS Sistemas Ltda em 06 de abril de 2020. O nome legal da empresa mudará de ATMOS Sistemas para *SAAB Sensors and Services Brazil* e permanecerá como uma entidade legal separada, integrada aos serviços e suporte da área de negócios da SAAB no Brasil.

3 INTELIGÊNCIA COMPETITIVA

O planeta globalizado muitas vezes é desleal, impõe competição, gera oportunidades e ameaças. Para competir, ganhar, ou mesmo sobreviver, é preciso agir atento às oportunidades. A informação permanece como a chave para o sucesso. Para buscar o diferencial nesse sistema informacional competitivo também é necessário se preocupar com a negação do acesso ao seu patrimônio de conhecimentos. Nesse ambiente competitivo, o alvo é o conhecimento que, invariavelmente, representa tempo e dinheiro para as empresas.

Para Medeiros (2013, p. 15) a globalização contribuiu para que as empresas, em geral, adotassem uma metodologia chamada de Inteligência Competitiva.

Ainda segundo Medeiros (2013, p. 148), não se pode esquecer que competitividade também significa proteção dos bens tangíveis, como o patrimônio físico, e principalmente os bens intangíveis, como os conhecimentos acumulados, as experiências adquiridas, os projetos, as tecnologias empregadas na confecção dos produtos expostos e os segredos institucionais (estratégias de negócio).

No mundo atual, no qual a pressa tornou-se um requisito essencial para o sucesso, há duas fórmulas distintas para as organizações atingirem seus objetivos, considerando que o ambiente de mercado está cada vez mais globalizado e competitivo: investir em pesquisa e trabalhar ou contratar um profissional para simplesmente furtar as informações dos concorrentes.

Alvin e Heidi Toffler (1994), no capítulo intitulado “O Futuro do Espião” do livro Guerra e Antiguerra, profetizaram que o mundo estava se tornando agressivamente competitivo e acabaria por transformar as organizações em verdadeiros “ninhos de espiões”. Provavelmente já identificavam um dos efeitos perversos da competitividade e, também, que a informação iria se transformar em bem estratégico a ser adquirido e preservado.

Esse cenário de incessante internacionalização dos negócios e de disputas por interesses, indica que as empresas devem se empenhar, cada vez mais, na utilização de processos de Inteligência que lhes dêem melhores condições de enfrentar os novos desafios a partir de um novo paradigma no mundo atual, qual seja o de Inteligência Competitiva, ou melhor, Inteligência para competir.

Na literatura são encontrados vários conceitos de Inteligência Competitiva, que caracterizam essa atividade como um processo de análise dos concorrentes, principalmente em relação às tendências gerais do ambiente econômico, social,

tecnológico, científico e mercadológico. Por exemplo, segundo KAHHANER (2004 apud MEDEIROS, 2013, p. 6), IC é um:

> Programa institucional e sistemático para garantir e analisar informação sobre as atividades da concorrência e as tendências do setor específico e do mercado em geral, com o propósito de levar a organização a atingir seus objetivos e metas.

Os autores Fitzpatrick e Burke (2003) e Medeiros (2013, p. 27), concordam que a Inteligência Competitiva é caracterizada pela aquisição de informações relevantes, pautadas por uma conduta legal e ética sobre o ambiente corporativo.

Segundo Medeiros (2013, p. 150), diariamente, as organizações e empresas sofrem com ações adversas. As empresas apresentadas na seção 2.2, por se destacarem nas áreas estratégicas, apresentam vantagens competitivas no cenário internacional, e com isso se tornam alvos de ações hostis como a espionagem; a sabotagem; e ataques cibernéticos.

3.1 ESPIONAGEM INDUSTRIAL

No mundo empresarial existe a preocupação quanto aos limites da Inteligência Competitiva e suas semelhanças com a espionagem industrial. Considerando os conceitos apresentados acima, percebe-se que a IC está voltada para analisar e estudar o mercado de forma legal e ética, enquanto na literatura, a espionagem usaria meios ilegais e sujos para obter informações privilegiadas.

Basicamente à espionagem industrial utiliza de meios ilegais e não éticos para se chegar aos mesmos resultados da IC, porém, cortando caminho e corrompendo pessoas para obter delas informações privilegiadas sobre uma determinada corporação. Nesse processo, pode-se utilizar várias técnicas de espionagem, como escuta ambiental, telefônica, ciberataques e furtos de documentos com dados sensíveis, além de um possível recrutamento[10] de um funcionário de confiança ou até membro da direção ou pesquisador do projeto.

O *NATIONAL COUNTERINTELLIGENCE CENTER* (1999, p. 2. Tradução nossa)[11],define espionagem industrial como:

---

[10] Recrutamento: consiste em fazer alguém dentro de uma organização, trabalhar em proveito de uma ação de espionagem (MORAES, 2020, pg. 27).

[11] Industrial espionage is defined as activity conducted by a foreign government or by a foreign company with direct assistance of a foreign government against a private US company for the purpose of obtaining commercial secrets. This definition does not extend to activity of private entities conducted without foreign government involvement, nor does it pertain to lawful efforts to obtain commercially useful information, such as information available on the Internet

> Atividade conduzida por um governo estrangeiro ou por uma empresa estrangeira com assistência direta de um governo estrangeiro contra uma empresa privada dos EUA com o objetivo de obter segredos comerciais. Essa definição não se estende à atividade de entidades privadas conduzidas sem o envolvimento de governos estrangeiros, nem se refere a esforços legais para obter informações comercialmente úteis, como informações disponíveis na Internet.

De acordo com Oliveira (2012, p. 76), “estados ou empresas buscarão adquirir o conhecimento de que necessitam onde quer que ele seja produzido, comprando-o ou roubando-o”. Para Cepik (2013, p. 7), “espionagem industrial e comercial é algo praticado ordinariamente pelos países mais poderosos contra seus inimigos, competidores e mesmo aliados”. Ainda segundo Cepik (2013), nessa competição, os Estados menos desenvolvidos sempre estarão em uma desvantagem natural.

Segundo Woloszyn (2013, p. 53), os órgãos de inteligência governamentais adversos fazem um levantamento de futuras ameaças à soberania de seus países, avaliam o potencial bélico dessas nações, e simultaneamente, direcionam ações de espionagem industrial e tecnológica na busca pelos segredos no desenvolvimento de armas.

3.2 SABOTAGEM

De acordo com Medeiros (2009, p. 10), um ato de sabotagem pode variar desde uma pequena ação individual até uma de grande porte, integrando um plano de caráter estratégico. Os planos de sabotagem normalmente valem-se do recrutamento de agentes para serem efetivados, que podem ser executados por elementos orgânicos ou não. Procura-se sempre um disfarce de intenção com intuito de apresentar características de um acidente.

Nesse tipo de atividade, a ação deliberada é provocada intencionalmente contra instalações, processos organizacionais, documentos, materiais, *software* ou *hardware*, em qualquer fase do projeto, sobretudo nos testes, ensaios e apresentações finais dos produtos, com intuito de paralisar, contaminar, desestruturar e desorganizar as atividades desenvolvidas pela empresa, objetivando destruir idéias e/ou a reputação da instituição perante o mercado em disputa.

3.3 ATAQUES CIBERNÉTICOS

A maioria das ameaças tradicionais encontram correspondente no espaço cibernético. Os prejuízos advindos de crimes cibernéticos tornaram o assunto relevante e preocupante (AGÊNCIA BRASILEIRA DE INTELIGÊNCIA, 2016, p. 64).

Essas ações deliberadas que visam interromper, penetrar, adulterar ou destruir redes utilizadas por setores públicos e privados, essenciais à sociedade e ao Estado, trazem muitos prejuízos que vão além das ações no espaço cibernético e do comprometimento de recursos da tecnologia da informação (TI) e comunicações. Decorrem, também, da manipulação de opiniões, mediante ações de propaganda ou de desinformação (BRASIL, 2016, p. 5).

A natureza desses ataques tem origens distintas, tanto por órgãos extrangeiros com interesses comerciais, como também por grupos e organizações criminosas, simpatizantes de causas específicas, ou mesmo por nacionais que apoiem ações antagônicas aos interesses de seus países.

São vários os exemplos de atuações de grupos que dirigiram ataques a sites e bases de dados governamentais e privados. Talvez o ataque cibernético, promovido pelo vírus de computador *Stuxnet*, contra instalações nucleares iranianas em 2010 seja o mais famoso entre eles (AGÊNCIA BRASILEIRA DE INTELIGÊNCIA, 2016, p. 64). Em 2013, o caso Snowden[12], trouxe à tona o programa secreto de vigilância global da internet promovido *National Security Agency* (NSA), conhecido como *Prism*, que monitora governos e empresas estrangeiras. Não menos importante, em 2017, o vírus de computador *WannaCry* atacou computadores em mais de 150 países, afetando milhares de pessoas, incluindo estruturas críticas tais como hospitais do Sistema Nacional de Saúde da Inglaterra e 85% da empresa de telecomunicações Telefônica, da Espanha (SANTOS, 2017, p. 3).

Para Medeiros (2013, p. 160), um processo seletivo rigoroso, composto de investigação social, prova de capacitação, entrevista e avaliação psicológica, dificultariam as ações de espionagem, sabotagem. A divulgação e conhecimento das legislações que criminalizam o vazamento de informações e a difusão de boatos, quando apresentadas ao candidato, também servem como inibidor de ações adversas. Esse procedimento também contribui com segurança no campo cibernético ao inibir a ação adversa de um colaborador responsável pelos meios de TI.

Para compreender a preocupação do governo com essas ameaças no âmbito das empresas que fazem parte da BID, no próximo capítulo será apresentado as legislações que regulam as atividades voltadas à salvaguarda do conhecimento sensível a nível estratégico, mais especificamente, com o tratamento da informação classificada por ED e EED.

---

[12] Edward Joseph Snowden, funcionário terceirizado da NSA que, em 2013, vazou informações sobre a atividade de monitoramento mundial realizado pelo do governo estadunidense.

4 LEGISLAÇÕES VIGENTES

Sobre o tema proposto, o Decreto nº 8.793 (BRASIL, 2016, p, 1), de 29 de junho de 2016, fixa a Política Nacional de Inteligência (PNI), documento que tem por finalidade “definir os parâmetros e os limites de atuação da atividade de inteligência e de seus executores no âmbito do Sistema Brasileiro de Inteligência (SISBIN)”. Trata-se de um documento norteador que define melhor como o conhecimento sensível se associa ao valor estratégico, econômico, de potencial, sendo produto de entes brasileiros públicos e privados. Proteger esse tipo de conhecimento se revela uma necessidade regular do Estado, sendo devida a sua aplicação e ampliação:

> É necessário, ainda, ampliar o desenvolvimento de ações de proteção dos conhecimentos sensíveis e da infraestrutura crítica nacional, bem como contrapor-se ao surgimento de ameaças representadas tanto por serviços de Inteligência, quanto por grupos de interesse, organizações ou indivíduos que atuem de forma adversa aos interesses estratégicos nacionais. (BRASIL, 2016, p.4)

O PNI oferece importantes diretrizes ao SISBIN e ao Programa Nacional de Proteção do Conhecimento Sensível (PNPC)[13], sendo citadas as principais ameaças para o conhecimento sensível como a espionagem, a sabotagem, os ataques cibernéticos, e outros.

Os objetivos nacionais de Inteligência visam contribuir para a promoção da segurança e dos interesses do Estado e da sociedade brasileira, por meio de atividades de Inteligência que possibilitem, dentre outras, neutralizar ações da Inteligência adversa; e proteger áreas e instalações, sistemas, tecnologias e conhecimentos sensíveis, bem como os detentores desses conhecimentos. Dentre as diretrizes contidas no PNI (BRASIL, 2016, p. 7), três devem ser prioritariamente consideradas ao assunto:

- Prevenir ações de espionagem: segredos militares, industriais (inovação e tecnologia) e de política externa são alvos preferenciais da espionagem estrangeira.
- Prevenir ações de sabotagem: é necessário mapear os alvos potenciais para atos de sabotagem, com o intuito de detectar o planejamento de ações dessa natureza em seus estágios iniciais.

[13] O PNPC é um instrumento preventivo para a proteção e a salvaguarda de conhecimentos sensíveis de interesse da sociedade e do Estado brasileiro. O programa foi instituído pela ABIN com a finalidade de exercer sua atribuição institucional de proteger as informações e conhecimentos sensíveis do país.

- Fortalecer a cultura de proteção de conhecimentos: o acesso não autorizado aos conhecimentos sensíveis empresariais, pode comprometer a consecução dos objetivos nacionais e resultar em prejuízos expressivos no campo socioeconômico. Os importantes resultados advindos de pesquisas científicas e tecnológicas requerem contínuo aperfeiçoamento de mecanismos de proteção nos meios acadêmicos e empresariais. A Inteligência deve concorrer para a disseminação da cultura de proteção como forma de evitar ou minimizar prejuízos ao País.

Com o intuito de operacionalizar essas diretrizes e estimular a adoção de procedimentos eficazes que contribuam com o fortalecimento da cultura de segurança, a identificação de ameaças e vulnerabilidades, bem como a implementação de medidas e procedimentos de proteção ao patrimônio intelectual e os conhecimentos sensíveis de defesa, surge o processo de credenciamento de entidades privadas e pessoas naturais vinculadas a esses setores.

4.1 PROCESSO DE CREDENCIAMENTO DE SEGURANÇA

O artigo 37 da Lei nº 12.527 (BRASIL, 2011, p. 11), de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI) instituiu o Núcleo de Segurança e Credenciamento (NSC) no âmbito do Gabinete de Segurança Institucional da Presidência da República (GSI-PR), com o objetivo de promover e propor a regulamentação do credenciamento de segurança de pessoas físicas, empresas, órgãos e entidades para tratamento de informações sigilosas.

O artigo 43 do Decreto nº 7.724 (BRASIL, 2012a, p. 10), de 16 de maio de 2012 estabelece que o acesso à informação classificada seja restrito às pessoas credenciadas segundo as normas fixadas pelo NSC. Estabelece, ainda, que compete ao GSI-PR expedir atos complementares relativos ao credenciamento de pessoas.

O Decreto nº 7.845 (BRASIL, 2012b), de 14 de novembro de 2012, e a Norma Complementar nº 1 da Instrução normativa nº 2/NSC/GSI/PR (BRASIL, 2013), de 27 de junho de 2013, disciplinam o processo de credenciamento de segurança de pessoas naturais, órgãos e entidades públicas e privadas, bem como órgãos de registro[14] e postos de controle[15], para o tratamento de informações classificadas, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal.

[14] Orgão de Registro é o ministério ou órgão de nível equivalente habilitado pelo Núcleo de Segurança e Credenciamento (BRASIL, 2012b);
[15] Posto de controle - unidade de órgão ou entidade pública ou privada, habilitada, responsável pelo armazenamento de informação classificada em qualquer grau de sigilo (BRASIL, 2012b);

Seguindo a ordem cronológica, a Portaria 1.059/GSC/EMCFA-MD (BRASIL, 2015), de 12 de maio de 2015, habilitou o COMAER para o exercício das atribuições inerentes aos Órgãos de Registro Nível 2 (ORN2), tornando-o apto a realizar os procedimentos de inspeção e instrução dos processos de credenciamento de segurança das entidades públicas ou privadas que mantenham vínculo de qualquer natureza, e que necessite tratar informação classificada em qualquer grau de sigilo.

O artigo 11 do Decreto nº 7.845 (BRASIL, 2012b, p. 4), estabelecem os requisitos condicionantes para a habilitação de entidade privada como posto de controle:

> I- regularidade fiscal;
> II- comprovação de qualificação técnica necessária à segurança de informação classificada em qualquer grau de sigilo;
> III- expectativa de assinatura de contrato sigiloso;
> IV- designação de gestor de segurança e credenciamento, e de seu substituto; e
> V- aprovação em inspeção para habilitação de segurança.

A última fase do processo corresponde à inspeção de segurança. Nessa fase, as entidades privadas adotarão providências para que os agentes públicos conheçam as normas e observem os procedimentos de segurança patrimonial e as medidas de segurança voltadas ao tratamento de informação classificada no âmbito da empresa.

A inspeção é finalizada com relatório substanciado, anexado ao processo de habilitação de segurança, no qual constará parecer fundamentado na análise dos autos da inspeção, indicando, em função do nível do risco potencial de quebra de segurança constatado, se a empresa está aprovada ou não. A habilitação de segurança terá validade não superior a dois anos, e deverá ser renovada antes do término do período de validade (BRASIL, 2013, p. 10).

Após a aprovação na habilitação de segurança, o novo posto de controle ativado no âmbito da empresa será responsável por realizar o controle das credenciais de segurança das pessoas que com ele mantenham vínculo de qualquer natureza, bem como garantir a segurança da informação classificada em qualquer grau de sigilo sob sua responsabilidade.

Dessa forma, o CIAER tem realizado uma média de cinco inspeções de segurança por ano, entre habilações e renovações de credenciamento de segurança em entidades privadas, além da expedição de milhares de credenciais de segurança para pessoas naturais. Todos esses dados serão informados e analisados na próxima seção.

5 ANÁLISE DA CULTURA DE SEGURANÇA NAS EMPRESAS

Segundo Gonçalves (2010, p. 14), uma das dificuldades enfrentados pela comunidade de inteligência no Brasil é a convivência com a falta de cultura de segurança e inteligência na sociedade brasileira.

Grande parte dos empresários, embora extremamente competentes nos requisitos técnicos e gerenciais, ainda não contemplam no planejamento das suas empresas os investimentos mínimos e indispensáveis para preservar o precioso patrimônio das suas respectivas entidades, ou seja, as informações sensíveis obtidas ao custo de muito suor e trabalho acabam ficando à mercê de espiões que as capturam com surpreendente facilidade.

Os investimentos em Inteligência, ou melhor em Contrainteligência e segurança normalmente são considerados como gastos, que devem ser desprendidos em valores mínimos, muitas vezes considerando apenas o viés reativo e poucas vezes o lado proativo.

Por esse motivo, preocupados apenas com o bem tangível, ou o simples cuprimento de leis ou normas reguladores para obtenção e manutenção de contratos, essas empresas, muitas vezes sem saber, economizam tostões e acabam tendo prejuízos de milhões. O grande problema é que, conforme descrito no PNI, o acesso indevido a esses conhecimentos sensíveis, pode comprometer a consecução dos objetivos nacionais e resultar em prejuízos expressivos no campo socioeconômico.

Após o vazamento de uma informação estratégica, um incidente gerado por sabotagem, ou um ataque ciberético que resulte o surgimento de um novo concorrente, um contrato cancelado, ações em baixa, ou seja, quando o prejuízo já aconteceu, vem a decisão de gastar: nesse momento o erro se perpetua. As decisões, sem a devida assessoria, invariavelmente recaem sobre mais guardas uniformizados para a portaria, e mais câmeras de segurança para o prédio da empresa.

O despreparo da sociedade brasileira, tanto na iniciativa privada quanto no setor público, é consequência dessa falta de cultura de inteligência no Brasil frente a ameaças reais como a espionagem, a sabotagem, a atuação de organizações criminosas e mesmo de grupos terroristas. Com isso a vulnerabilidade do Brasil diante desse tipo de ameaça é enorme. Outra consequência é a falta de investimento no setor e a ausência de mecanismos legais e institucionais que viabilizem o trabalho do pessoal de inteligência (BRASIL, 2014, p. 88).

5.1 DIFICULDADES DE ADEQUAÇÃO

No processo de proteção do conhecimento sensível cabe à Inteligência, ou melhor, à equipe gestora de segurança da empresa identificar as ameaças[16] e oportunidades no ambiente externo e as vulnerabilidades no ambiente interno da organização

Ao dar início ao processo de habilitação de segurança, as empresas normalmente encontram muitas dificuldades, principalmente por estarem inseridas nessa realidade de baixa mentalidade de segurança e inteligência, que se encontra a grande maioria das empresas brasileiras.

Outro problema é o desconhecimento ou a dificuldade de interpretação das normas e decretos que norteiam o processo. Contribui a isso, o fato de alguns conceitos serem diferentes daqueles empregados no mundo corporativo, e também o fato das determinações mínimas necessárias, contidas no ítem 8.5 da Norma Complementar nº 1 da Instrução normativa nº 2/NSC/GSI/PR (BRASIL, 2013, p. 8), não transmitirem as especificações técnicas relativas ao nível de segurança desejado.

Mesmo não sendo unânime entre as empresas, a falta de profissionais especializados se apresenta como outro fator normalmente presente, principalmente em empresas com números reduzidos de colaboradores. Geralmente essas empresas têm dificuldades para indicar o Gestor de Segurança e Credenciamento (GSC)[17] e seu suplente. Não é incomum, na indicação para essa função, aparecer colaboradores com nenhuma formação específica na área de segurança, diretores de áreas desconexas à atividade ou até mesmo o CEO[18] da empresa.

Após a finalização dos procedimentos de segurança e aquisição dos equipamentos mínimos necessários é realizado o agendamento da inspeção de segurança. Este é ponto mais importante do processo. Nessa fase é possível acompanhar e analisar todas as medidas adotadas pelas ED e EED com vista à proteção do conhecimento sensível e dos ativos fundamentais para a vida segura da organização.

---

[16] Ameaças são atores que realizam ações hostis com a possibilidade de comprometer a segurança dos recursos humanos, das informações, do material e das áreas e instalações por intermédio das vulnerabilidades (MEDEIROS, 2009, p. 6).

[17] GSC é o elo de segurança das empresas com o CIAER e o responsável direto por toda a condução dos processos de credenciamento bem como do tratamento da informação classificada no âmbito da empresa (BRASIL, 2013).

[18] CEO é a sigla inglesa de *Chief Executive Officer*, que significa Diretor Executivo em português. CEO é a pessoa com maior autoridade na hierarquia operacional de uma organização.

5.2 INSPEÇÃO DE SEGURANÇA

A principal finalidade da inspeção de segurança é fiscalizar o cumprimento das normas e procedimentos de credenciamento de segurança e tratamento de informação classificada no âmbito da empresa.

A equipe de inspeção para habilitação de segurança verificará as instalações destinadas para o posto de controle da entidade privada quanto ao atendimento da qualificação técnica mínima necessária ao tratamento de informação classificada, previsto no inciso II do art. 11 do Decreto no 7.845 (BRASIL, 2012b), e no item 8.5 da Norma Complementar nº 1 da Instrução normativa nº 2/NSC/GSI/PR (BRASIL, 2013).

Ao observar os relatórios das inspeções de segurança realizadas pelo CIAER nos últimos 6 anos[19], percebe-se que na maioria das vezes as empresas logram êxito e atingem a qualificação mínima necessária.

Considerando as oito empresas elencadas no item 2.1, duas empresas receberam o parecer negativo durante as inspeções de habilitação de segurança, o que representa uma taxa de 25% de insucesso. Porém, como um dos objetivos é disseminar a cultura de inteligência, após as orientações da equipe do CIAER, contato com o relatório detalhado, e novo prazo para adequação às normas, todas as discrepâncias foram sanadas e as empresas aprovadas.

Nas novas inspeções realizadas nessas duas empresas, foi identificado um avanço enorme nas medidas de proteção ao conhecimento, bem como avanços na cultura de segurança e inteligência, reflexos da conscientização do núcleo diretor e novos investimentos na gestão de segurança com foco no tratamento da informação classificada.

Nas inspeções de segurança referentes ao processo de renovação da habilitação de segurança percebe-se que as empresas, que inicialmente se adequaram apenas para terem êxito no processo, realmente modificaram a visão relativa à proteção da informação, e ampliaram as medidas de segurança da informação a todos os campos da segurança orgânica[20] (corporativa), extendendo as medidas de proteção a toda a empresa e a todos os colaboradores.

---

[19] Considerando a data de publicação da Portaria 1.059/GSC/EMCFA-MD, de 12 de maio de 2015, que habilitou o COMAER para o exercício das atribuições inerentes aos ORN2.

[20] É o segmento da Contrainteligência que preconiza a adoção de medidas e procedi- mentos preventivos destinados à salvaguarda de pessoas, materiais, áreas, instalações e meios de produção, armazenamento e comunicação de conhecimentos e dados, no âmbito do próprio órgão ou instituição (AGÊNCIA BRASILEIRA DE INTELIGÊNCIA,2016, p. 41).

5.3 CREDENCIAMENTO DE PESSOAS NATURAIS

As empresas aprovadas no processo de habilitação de segurança são responsáveis pelas solicitações de credenciamento ao ORN2 para todos os colaboradores que tenham necessidade de conhecer informações classificadas, em qualquer grau de sigilo, conforme estabelecido em normatização interna do órgão ao qual a pessoa a ser credenciada estiver vinculada (BRASIL, 2013, p. 4).

Segundo Mitnick e Simon (2003, p. 3) a empresa pode ter modernas tecnologias de segurança e defesa, pode ter a melhor guarda para proteger as suas instalações, mas mesmo assim ainda poderá estar vulnerável. Isso porque na maioria das vezes, apesar de ser o mais importante, o fator humano é o elo mais fraco da segurança. É preciso criar uma mentalidade de segurança voltada para todos os colaboradores, incorporar a idéia, pois a informação privilegiada possui tanto valor que o seu possuidor se torna um alvo altamente compensador (Medeiros, 2009, p. 8).

Nesse sentido, cabe ao CIAER credenciar os colaboradores das entidades privadas que tenham necessidade de conhecer informações classificadas, em qualquer grau de sigilo, conforme solicitação do GSC das empresas.

A investigação de segurança realizada pelo CIAER tem como objetivo identificar o nível do risco potencial de quebra de segurança ao se permitir que a pessoa indicada acesse informação classificada no grau de sigilo indicado (BRASIL, 2013, p. 5). A investigação é conduzida por um militar de carreira, com competência profissional comprovada para atuar na área de inteligência, que irá avaliar, no mínimo, dados de aspecto pessoal do indicado com o intuito de identificar possíveis envolvimentos com pessoas ou organizações associadas ao crime, terrorismo, tráfico, sabotagem e espionagem, bem como comportamentos que favoreçam um possível recrutamento deste colaborador.

A tabela 2 traz informações sobre as ED e EED credenciadas pelo CIAER. Observa-se que o número de empresas credenciadas cresceu significativamente nos últimos anos, e essa será uma tendência para os próximos anos principalmente devido a nacionalização de muitos componentes dos produtos estratégicos de defesa, e o fortalecimento da BID.

Além disso, observa-se uma maior quantidade de credenciais emitidas para as empresas Embraer, Akaer, Avibras, Ael e Mectrom-Comm devido ao fato dessas empresas possuírem maior número de colaboradores e já estarem na fase de produção. As empresas Atmos, Kryptus, IACIT e SAM apesar de já possuírem ou

estarem na expectativa de assinatura de contrato sigiloso com COMAER, ainda não se encontram em fase de produção.

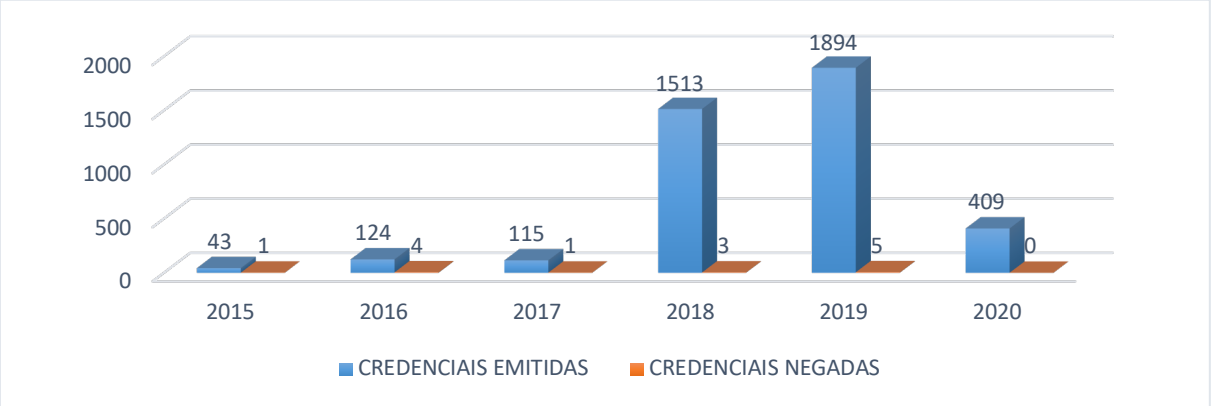
Tabela 2 – Inspeções e Credenciais de segurança por entidade privada [21].

Entidade Privada	Ano da Habilitação	Qtde de Inspeções	Qtde de Credenciais Atuais
EMBRAER Defesa & Segurança	2015	4	2915
AKAER Engenharia	2016	3	130
AVIBRAS Indústria Aeroespacial	2018	2	68
AEL Sistemas	2018	2	8
ATMOS Sistemas	2018	2	2
MECTROM-COMM	2018	2	61
KRYPTUS	2019	1	2
IACIT Soluções Tecnológicas	2019	1	2
SAAB Aeronautica Montagens	2019	1	4

Fonte: SISCRED / CIAER maio 2020.

No gráfico 1 verifica-se um crescimento significativo do número de credenciais emitidas pelo CIAER, principalmente devido a demanda da empresa Embraer e o crescimento do número de empresas credenciadas a partir do ano de 2018. Em 2020 o quantitativo de credenciais emitidas traz informações até o mês de maio.

Gráfico 1 – Credenciais de segurança de pessoas naturais: emitidas e negadas.



Fonte: SISCRED / CIAER maio 2020.

Corroborando com a afirmação de Medeiros (2013) a respeito da importância de um processo seletivo rigoroso, percebe-se uma baixa quantidade de credenciais negadas, principalmente pelo fato dessas empresas serem orientadas a adotarem essa medida durante a seleção dos colaboradores que irão exercer atividades sensíveis. Esse procedimento reduz a quantidade de discrepâncias e, consequentemente, de credenciais negadas pelo CIAER.

Após a apresentação das principais dificuldades enfrentadas pelas empresas, e análise dos dados pesquisados, serão realizadas algumas considerações finais.

[21] Pesquisa documental realizada nos arquivos disponibilizados no banco de dados interno do Sistema de Credenciamento do CIAER (SISCRED). Acesso em: 20 jun. 2020.

6 CONCLUSÃO

“A Atividade de Inteligência visa ao assessoramento de autoridades governamentais, nos respectivos níveis e áreas de atribuição”. O objetivo principal das ações propostas na PNI é a identificação e a avaliação de oportunidades e ameaças que possam comprometer à soberania, defesa e segurança (AGÊNCIA BRASILEIRA DE INTELIGÊNCIA, 2016, p. 67).

Nesse contexto, foram criados decretos e normas com o objetivo de estimular e regular o tratamento de informações classificadas em entidades privadas vinculadas ao Poder Executivo Federal. O cumprimento das determinações dessas legislações, exigiu do CIAER, o preparo de profissionais e diversos gastos públicos com deslocamentos e despesas pessoais das equipes de inspeção. Com isso, surgiu a inquietação no sentido de demonstrar a importância dessa atividade especializada, não apenas como um simples cumprimento da lei vigente, mas também como uma atividade fundamental para a manutenção da cultura de segurança dessas entidades, e consequentemente um alinhamento com os interesses nacionais.

Inicialmente, foi apresentado a constituição da Base Industrial de Defesa, e a relação entre defesa e desenvolvimento. Com um breve histórico da indústria de defesa, foi apresentado o papel econômico e científico-tecnológico do fortalecimento da BID. Com destaque para as ED e EED, essenciais para o desenvolvimento, pesquisa e produção das necessidades de defesa, constatou-se que muitas dessas empresas estão vinculadas diretamente ao COMAER, com a responsabilidade de fornecer produtos de defesa em atendimento às necessidades operacionais da FAB, bem como para atender as peculiariedades dos projetos estratégicos da Força.

Em seguida, foram apresentadas diversas definições de Inteligência Competitiva, enfatizando sua conduta legal e ética sempre com propósito levar a organização a atingir seus objetivos e metas. Pautado nas idéias de Medeiros (2013), foi exposto que essa barreira de licitude da Inteligência Competitiva muitas vezes é rompida e se apresenta como ações adversas que ameçam as empresas de todo o mundo. Os autores Oliveira (2012) e Cepik (2013) deixaram claro que nesse mundo de competitividade, a espionagem industrial deixou de ser excessão e virou regra. De um modo ainda preocupante, Woloszyn (2013) expôs o interesse de órgãos de inteligência adversos em promoverem ações contra a indústria bélica de outras nações. Outras ameaças, como a sabotagem e os ataques cibernéticos ratificaram os prejuízos causados ao mundo corporativo. Resultado de um mundo globalizado e seus avanços tecnológicos, a deslealdade e a competição obrigaram a Inteligência

Competitiva a incorporar os conceitos de proteção dos bens tangíveis e principalmente os intengíveis.

A entrada em vigor do Decreto nº 7.845 (BRASIL, 2012b), somado as orientações de execução normatizadas na NC01/IN02/NSC/GSI/PR (BRASIL, 2013), mesmo que de forma não muito clara para entidades privadas, modificaram a forma do tratamento da informação classificada no âmbito dessas instituições. Mesmo que a adequação a essas normas inicialmente se apresente apenas como um fator condicionante à expectativa de assinatura de um contrato sigiloso, o tempo tem revelado que as ED e EED, de um modo geral, têm fortalecido a cultura de proteção, através da adoção de práticas cada vez mais eficazes de salvaguarda do conhecimento, que se apresenta como o principal patrimônio e recurso estratégico dessas organizações.

Após realizar uma pesquisa documental no SISCRED, no período entre maio de 2015 e maio de 2020, foi possível verificar uma taxa de insucesso de 25% nas inspeções de segurança. A presença dessa expressiva taxa, demonstra o grau de profissionalismo e seriedade ao qual estas inspeções são conduzidas.

Além disso, foram analisadas as credenciais de segurança de pessoas naturais, vinculadas às entidades privadas. Concluiu-se que a demanda de credenciais aumentou significativamente a partir de 2018 devido ao aumento do número de empresas credenciadas e o aumento da produção de PED em território nacional, que de acordo com o Instituto de Pesquisa Economica Aplicada - IPEA (ANDRADE, I. O. *et al,* 2016) é resultado desse “novo protagonismo” destacado as Forças Armadas. Sobre a quantidade de credenciais negadas, concluiu-se que a adoção de um processo seletivo rigoroso defendido por Medeiros (2013, p. 151), por parte das empresas, pode ter sido responsável pela redução de discrepâncias na fase de investigação de segurança.

Os dados estatísticos, bem como a análise das legislações vigentes e o comportamento das empresas, principalmente após as inspeções de segurança permitem confirmar a hipótese que o processo de credenciamento de entidades privadas, além de simplesmente cumprir com o estabelecido nas leis vigentes, contribui substancialmente com aumento da mentalidade de segurança e percepção das ameaças dessas empresas.

Dessa forma, foi possível verificar a importância dessa atividade especializada, tanto para entidades privadas, ao contribuir com a preservação do conhecimento a nível estratégico, quanto para os interesses nacionais.

REFERÊNCIAS

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. **Doutrina Nacional da Atividade de Inteligência:** fundamentos doutrinários. Brasília, DF: ABIN, 2016.

ANDRADE, I.O. *et al.* **O fortalecimento da indústria de defesa no Brasil.** Brasília, DF: IPEA, 2016. (Texto para Discussão, n. 2182). Disponível em: http://repositorio.ipea.gov.br/bitstream/11058/6086/1/td_2182.pdf. Acesso em: 14 maio 2020.

BRASIL. Comando da Aeronáutica. **ICA 200-13**: credenciamento de segurança. Brasília, DF: FAB, 2017.

BRASIL. Decreto nº 7.724 de 16 de maio de 2012a. Regulamenta a Lei no 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição. **Diário Oficial [da] União**: seção 1, Brasília, DF, DF, 17 maio 2012a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7724.htm. Acesso em 26 abr.2020.

BRASIL. Decreto nº 7.845 de 14 de novembro de 2012b, que regula procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento. **Diário Oficial [da] União**: seção 1, Brasília, DF, p. 1, 16 nov. 2012b. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Decreto/D7845.htm. Acesso em: 22 abr 2020.

BRASIL. Decreto nº 8.793 de 29 de junho de 2016, que fixa a Política Nacional de Inteligência. **Diário Oficial [da] União**: seção 1, Brasília, DF, p.5, 30 jun. 2016. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2016/Decreto/D8793.htm. Acesso em: 15 abr. 2020.

BRASIL. Lei nº 12.527 de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências. **Diário Oficial [da] União**: seção 1, Brasília, DF, p. 1, 18 nov. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/2011/l12527.htm. Acesso em: 15 abr. 2020.

BRASIL. Lei nº 12.598 de 21 de março de 2012c, que estabelece normas especiais para as compras, as contratações e o desenvolvimento de estratégica de defesa; altera a Lei no 12.249, de 11 de junho de 2010; e dá outras providências. **Diário Oficial [da] União**: seção 1, Brasília, DF, p.1, 22 mar. 2012c. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12598.htm. Acesso em: 15 abr. 2020.

BRASIL. Ministério da Defesa. **Guia de Empresas e produtos de Defesa.** Brasília, DF: MD, 2019a. Disponível em: https://caslode.defesa.gov.br/site/index.php/guia-produtos-de-defesa-2. Acesso em: 3 maio 2020.

BRASIL. Ministério da Defesa. **Livro Branco de Defesa Nacional.** Brasília, DF: MD, 2012d. Disponível em: https://www.defesa.gov.br/arquivos/estado_e_defesa/livro_ branco/ livrobranco.pdf. Acesso em: 4 maio 2020.

BRASIL. Ministério da Defesa. **Projetos Estratégicos.** Brasília, DF: MD, 2019b. Disponível em: https://www.defesa.gov.br/arquivos/industria_defesa/projetos_ estrategicos/cartilha_laad_final_digital_port.pdf. Acesso em: 3 maio 2020.

BRASIL. Norma Complementar nº 1 da Instrução Normativa nº 2/NSC/GSI/PR, de 27 de junho de 2013,homologada pela Portaria nº 19, de 27 de junho de 2013 do Gabinete de Segurança Institucional do Presidente da República, que disciplina o credenciamento de segurança de pessoas naturais, órgãos e entidades públicas e privadas para o tratamento de informações classificadas. **Diário Oficial [da] União**: seção 1, Brasília, DF, p.1, 27 jun. 2013. Disponível em: http://dsic.planalto.gov.br /legislacao/NC01_IN02_GSI.pdf. Acesso em: 15 abr. 2020.

BRASIL. Portaria nº 1.059/MD de 12 de maio de 2015, que habilita os Comandos da Marinha, do Exército e da Aeronáutica, a Escola Superior de Guerra, o Hospital das Forças Armadas, e Centror Gestor e Operacional do Sistema de Proteção da Amazônia para o exercício das atribuições inerentes aos Orgãos de Registro Nível 2 (ORN2), visando ao credenciamento de segurança e tratamento da informação classificada em qualquer grau de sigilo. **Diário Oficial [da] União**: seção 1, Brasília, DF, p. 11, 13 maio 2015. Disponível em: http://www.lex.com.br/legis_26767259_ PORTARIA_N_1059_DE_12_DE_MAIO_DE_2015.aspx. Acesso em: 15 abr. 2020.

BRASIL. Senado Federal. **Relatório final da CPI da espionagem.** Brasília, DF: Senado Federal, 2014. Disponível em: https://legis.senado.leg.br/sdleggetter/ documento?dm=3857834&ts=1553242070012&disposition=inline. Acesso em: 18 maio 2020.

CEPIK, Marco Aurélio. Espionagem: qual o limite? Entrevista concedida a Alicia Ivanissevich. **Revista Ciência Hoje**, Rio de Janeiro, v.52, n. 308, p. 6-8, out. 2013.

DELLAGNEZZE, R. **200 anos da indústria de defesa no Brasil**. Juiz de Fora: UFJF, 2008. Disponível em: https://ecsbdefesa.com.br/defesa/fts/200ANOS.pdf. Acesso em: 12 maio. 2020.

ESCOLA SUPERIOR DE GUERRA (Brasil). **Fundamentos do poder nacional.** Rio de Janeiro: ESG, 2020. 164 p. Disponível em: https://www.esg.br/publi/FPN2020.pdf. Acesso em: 2 maio 2020.

FITZPATRICK, W. M; BURKE D. R. Competitive Intelligence, Corporate Security and the Virtual Organization. **Advances in Competitiveness Research**, Indiana, v.11, n. 1, 2003.

GONÇALVES, Joanisval Brito. **O que fazer com nossos espiões?**: considerações sobre a atividade de inteligência no Brasil. Brasília, DF: Senado Federal, 2010. Disponível em: https://www12.senado.leg.br/publicacoes/estudos-legislativos/tipos-de-estudos/ outras-publicacoes/agenda-legislativa/capitulo-12-o-que-fazer-com-nossos-espioes-consideracoes-sobre-a-atividade-de-inteligencia-no-brasil. Acesso em: 20 maio 2020.

KENT, Sherman. **Informações estratégicas.** Tradução: Hélio Freire. Rio de Janeiro: Biblioteca do Exército, 1967. v.123.

MEDEIROS, Francisco J. F. **A atividade de inteligência no mundo atual.** [*S.l.: s.n.*], 2009. Disponível em: https://www2.mppa.mp.br/sistemas/gcsubsites/upload/60/a%20atividade%20de%20intelig%C3%83%C2%AAncia%20no%20mundo%20atual.pdf. Acesso em: 15 maio 2020.

MEDEIROS, Francisco J. F. **Os segredos da Inteligência Competitiva.** 1 ed. Rio de Janeiro: Livre Expressão, 2013.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar**. São Paulo: Pearson Education do Brasil, 2003. *E-book*.

MORAES, Marcio Bonifacio. **Inteligência estratégica:** entendendo o mundo secreto da espionagem. [*S.l.*: *s.n.*], 2020.

NATIONAL COUNTERINTELLIGENCE CENTER (UNITED STATES). **Annual Report to Congress on Foreign Economic Collection and Industrial Espionage**. [S.l.]: National Counterintelligence Center, 1999. Disponível em: https://fas.org/irp/ops/ci/docs/fecie_fy00.pdf. Acesso em: 14 de maio 2020.

OLIVEIRA, Hércules Rodrigues. Propriedade Intelectual: uma visão de Contrainteligência. **Revista Brasileira de Inteligência,** Brasília, DF, n. 7, p. 67-78, dez. 2012.

PLATT, Washington. **Produção de Informações estratégicas.** Tradução: Álvaro Galvão Pereira e Heitor Aquino Ferreira. Rio de Janeiro: Biblioteca do Exército; Livraria Agir Editora, 1974. v. 57.

SANTOS, Euripedes Aparecido. **Ataque cibernético autônomo:** análise do ataque do vírus wannacry em 12 de maio de 2017. 2018. Monografia (Curso Superior de Inteligência Estratégica) - Escola Superior de Guerra, Rio de Janeiro, 2018.

TOFFLER, Alvin e Heide. **Guerra e antiguerra.** 2 ed. Rio de Janeiro: Record, 1994.

WOLOSZYN, André Luís. **Guerra nas Sombras:** os bastidores dos serviços secretos internacionais. São Paulo: Contexto, 2013.