FABIO EVANGELHO DE ARAÚJO

SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS DE ÓLEO E GÁS NO BRASIL:

proposta para um programa de estado

Trabalho de Conclusão de Curso - Monografia apresentada ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do diploma do Curso de Altos Estudos de Política e Estratégia.

Orientador: Cel R/1 Mauro Barbosa Ferreira Esteves

Rio de Janeiro

2016

Fabio Evangelho de Araújo

Biblioteca General Cordeiro de Farias

Evangelho, Fabio.
Segurança da Infraestrutura Crítica de Óleo e Gás no Brasil: proposta para um programa de estado / Fabio Evangelho de Araújo. - Rio de Janeiro : ESG, 2016.

38 f.

Orientador: Cel R/1 Mauro Barbosa Ferreira Esteves.
Trabalho de Conclusão de Curso – Monografia apresentada ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do diploma do Curso de Altos Estudos de Política e Estratégia (CAEPE), 2016.

1. Infraestrutura Crítica. 2. Segurança. 3. Gabinete de Segurança Institucional. I. Título.

RESUMO

Esta monografia aborda a proteção de infraestruturas críticas, o histórico de como vem sendo tratada no mundo após ganhar importância com as novas ameaças de terrorismo. Traz então o tema para a realidade brasileira, discorrendo sobre os marcos legais e as iniciativas que foram conduzidas pelo Gabinete de Segurança Institucional, dentro do escopo das instalações terrestres do setor de óleo e gás. Foi realizada uma pesquisa documental com a revisão bibliográfica do tema e o resgate do histórico de participação da Petrobras no levantamento de infraestruturas críticas. Tomando como referência o aparato estatal dos Estados Unidos da América, propõe-se um modelo para incrementar de maneira compulsória a segurança dessas instalações estratégicas no Brasil, porém com incentivos que envolvem desoneração tributária (similar a outros programas locais existentes) e financiamento por meio de linhas de créditos tanto para os provedores de bens e serviços de segurança, quanto para os contratantes, operadores das instalações. O estudo conclui ser necessário definir uma estrutura governamental que estabeleça estratégias, mas que também atue em questões operacionais para controlar a implementação das contramedidas de segurança e buscar garantir a efetividade do programa.

Palavras-chave: Infraestrutura Crítica. Segurança. Petrobras. Gabinete de Segurança Institucional.

ABSTRACT

The current paper deals with critical infrastructure protection, its background and some countries approaches considering the new threats of terrorism. In the Brazilian case, it highlights the legal framework and initiatives conducted by Gabinete de Segurança Institucional *for onshore facilities of oil & gas industry. A documentary research was carried out by a bibliographical revision, including Petrobras' participation timeline in the survey of critical infrastructures. Taking as reference the state apparatus of the United States of America, a model is proposed in order to increase mandatorily the security of strategic facilities in Brazil, but with benefits such as tax relief (similar to other existing local programs) and low interest rate loans for both: providers of security goods and services and contractors (plant operators). In sum, the present study concludes that it is necessary to establish a government structure not only to define strategies, but also to act on operational issues to monitor the implementation of security countermeasures and to ensure the program effectiveness.*

Keywords*: Critical Infrastructure. Protection.* Gabinete de Segurança Institucional*.*

LISTA DE ABREVIATURAS E SIGLAS

ABIN	Agência Brasileira de Inteligência
Anatel	Agência Nacional de Telecomunicações
ANEEL	Agência Nacional de Energia Elétrica
ANP	Agência Nacional do Petróleo, Gás Natural e Biocombustíveis
BNDES	Banco Nacional de Desenvolvimento Econômico e Social
BP	British Petroleum
CCOTI	Centro de Coordenação de Operações Terrestres Interagências
CDN	Conselho de Defesa Nacional
CF	Constituição Federal
CFTV	Circuito fechado de televisão
Cofins	Contribuição para Financiamento da Seguridade Social
CREDEN	Câmara de Relações Exteriores e Defesa Nacional
DHS	*U.S. Departament of Homeland Security* (Departamento Norte-americano de Segurança Nacional)
ECEME	Escola de Comando e Estado-Maior do Exército
Embrapa	Empresa Brasileira de Pesquisa Agropecuária
END	Estratégia Nacional de Defesa
EUA	Estados Unidos da América
GSI	Gabinete de Segurança Institucional
GTSIC	Grupo Técnico de Segurança das Infraestruturas Críticas
IEC	Infraestrutura crítica
IP	*Office of Infrastructure Protection* (Escritório de Proteção de Infraestrutura)
IPI	Imposto sobre Produtos Industrializados
MAB	Movimento dos Atingidos por Barragem
MME	Ministério das Minas e Energia
NIPP	*National Infrastructure Protection Plan* (Plano de Proteção da Infraestrutura Nacional)
O&G	Óleo e gás
PCC	Primeiro Comando da Capital
PEE	Projeto Estratégico do Exército
Petrobras	Petróleo Brasileiro S.A.
PIS	Programas de Integração Social

PR	Presidente da República
SGTSIC-PEGANCOR	Subgrupo Técnico de Segurança de Infraestruturas Críticas de Petróleo, Gás Natural e Combustíveis Renováveis
SIPRON	Sistema de Proteção ao Programa Nuclear Brasileiro
SISCOT	Sistema de Coordenação de Operações Terrestres Interagências
VPR	Vice-Presidente da Republica

SUMÁRIO

1 INTRODUÇÃO

Com a intensificação da ameaça do terrorismo nas últimas décadas, alguns países começaram a desenvolver programas de proteção de suas infraestruturas críticas (IEC). No Brasil, houve algumas iniciativas neste sentido, mas permanecem ainda incipientes, sem aplicação efetiva. E apesar dos grandes eventos internacionais que sediamos recentemente, percebe-se que o País ainda não está preparado para fazer frente a atos intencionais contra as instalações definidas como estratégicas.

Apesar de o terrorismo não representar uma ameaça tão presente aqui quanto em outros países, a atividade de segurança de IEC revela-se muito importante, pois trata de operações que caso sejam interrompidas causam grandes impactos. Significa dizer que quando uma instalação industrial tem sua proteção preparada contra atos intencionais como sabotagem e vandalismo, atende-se a uma necessidade cotidiana de se evitar práticas criminosas comuns de roubo ou furto de materiais.

Essas práticas podem ser muito danosas, como por exemplo, um simples furto de cabo de cobre pode acarretar uma parada de produção que gera prejuízo de milhões de reais e chegar a provocar desabastecimento de determinado mercado como no caso de gasodutos.

Seguindo nesta corrente virtuosa de proteção, quando se mira nos atos intencionais, acaba-se preservando a vida e a continuidade operacional para ações não intencionais, como evitar o acesso inadvertido de animais ou pessoas não autorizadas a um local que ofereça risco de morte, por exemplo.

Tomando-se como modelo o setor de geração de energia petrolífera, no qual a Petróleo Brasileiro S.A. (Petrobras) é a principal empresa no Brasil, é relevante para a Segurança Nacional a proposição de linhas gerais de um programa de Estado que busque alcançar melhores patamares de proteção das estruturas estratégicas para preservação da nossa soberania.

Pretende-se que tal programa defina obrigações para a Petrobras e outras operadoras, mas que também contemple o compromisso da União em viabilizar financeiramente o incremento dos níveis de segurança requeridos pela importância destas instalações e a manutenção dos controles existentes ou a serem implementados.

No âmbito do programa, tornar-se-á necessário definir um órgão de controle

responsável por fiscalizar a correta aplicação dos recursos, além de testar a eficácia dos planos de segurança locais.

O estudo visa ser específico sobre a segurança física de instalações terrestres do setor de óleo e gás (O&G) para buscar formular um modelo legal que responsabilize proprietários, concessionários e operadores destas instalações pela manutenção e aprimoramento dos controles.

A questão que se espera responder ao final deste trabalho é: em que medida as melhores práticas dos programas de proteção das IEC na indústria petrolífera em outros países podem ser adotadas de forma legal, compulsória e sustentável no Brasil.

Para tanto, este ensaio examinará as iniciativas sobre proteção de IEC conduzidas pelo Gabinete de Segurança Institucional (GSI) da Presidência da República e, no âmbito do Projeto PROTEGER, pelo Exército Brasileiro; desenvolverá uma revisão bibliográfica do tema e resgatará o histórico de participação da Petrobras neste processo; analisará as melhores práticas de segurança física para instalações do setor de O&G e como são sustentadas as implantações dos projetos ao longo do tempo; e irá propor linhas mestras para um programa nacional de proteção de IEC para o setor compatível com a realidade brasileira.

O estudo pretende abordar o modelo de proteção de infraestrutura desenvolvido pelos Estados Unidos da América (EUA) como referência, por ter uma postura de envolvimento em relação às empresas operadoras e pela transparência na divulgação dos seus programas, o que torna a informação acessível.

Como um exercício de proposição das diretrizes de um programa de proteção, a monografia ficará restrita à segurança física das instalações terrestres críticas do setor de O&G. Logo, não serão considerados os setores de transporte, de provisão de água, de alimentos, de saúde pública, de redes de telecomunicações (segurança cibernética), sistemas bancários, cadeias de suprimento etc.

Nem serão abordadas, por exemplo, as ameaças cibernéticas direcionadas às infraestruturas críticas que surgiram nos últimos anos, demonstrando a necessidade de desenvolvimento de técnicas de defesa, no intuito da manutenção da segurança nacional (CARVALHO, 2014).

Depois, comparar esses dados com a referência americana via documentos públicos e, por fim, propor linhas gerais de um programa de Estado que fomente a proteção física de instalações de O&G no Brasil.

A abordagem específica para a segurança física de instalações terrestres do

setor de O&G (refinarias, terminais, oleodutos, gasodutos etc.) buscará propor um modelo legal que responsabilize proprietários, concessionários e operadores destas instalações pela manutenção e implantação dos controles (procedimentos e equipamentos) estabelecidos em seus planos de segurança – aprovados por órgão competente, ainda a ser definido.

Em contrapartida, quando classificadas como críticas para o País, as instalações contariam com incentivos fiscais e/ou investimentos públicos dentro de um programa de Estado perene.

Quantos aos fins, a pesquisa será do tipo aplicada, com o objetivo prático de apresentar propostas reais para um programa de proteção das infraestruturas críticas na indústria do petróleo no Brasil.

Quanto aos meios de investigação, a pesquisa será principalmente documental, com base em anais de simpósios, registros dos projetos citados, planos de proteção, formulários e padrões norte-americanos pertinentes ao tema.

2 INFRAESTRUTURA CRÍTICA

É papel do Estado garantir a segurança, o bem-estar, o desenvolvimento e a justiça na sociedade, o que torna relevante a segurança das infraestruturas críticas (IEC) existentes.

A afirmação encontra respaldo no preâmbulo da Constituição Federal (CF) brasileira (BRASIL, 1988), nos seus artigos 5° e 6º, que define a segurança como um dos direitos sociais; e no artigo 91, ao descrever que “o Conselho de Defesa Nacional (CDN) é órgão de consulta do Presidente da República nos assuntos relacionados com a soberania nacional e a defesa do Estado democrático [...]”. E ao Conselho de Defesa Nacional, de acordo com o § 1º, inciso III, da mesma CF, compete:

> Propor os critérios e condições de utilização de áreas indispensáveis à segurança do território nacional e opinar sobre seu efetivo uso, especialmente na faixa de fronteira e nas relacionadas com a preservação e a exploração dos recursos naturais de qualquer tipo.

Ainda vale mencionar o artigo 144 da CF, que estabelece que “a segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio”.

2.1 CONCEITO

Como definido na Portaria Nº 02, do Gabinete de Segurança Institucional da Presidência da República, de 8 de fevereiro de 2008, “consideram-se IEC as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional” (BRASIL, 2008).

Infraestruturas críticas também são definidas como os ativos que se afetados por fenômenos da natureza, como terremotos, inundações ou por ações de terrorismo, causam grandes impactos em toda uma nação e sua sociedade. São definidas também como os subconjuntos de ativos que afetam a continuidade da missão do Estado e a segurança da sociedade (MANDARINO, 2010). São exemplos de

infraestruturas críticas: os sistemas de telecomunicações, os sistemas de transporte, os de distribuição de água e as geradoras e distribuidoras de energia.

As IEC exercem significativa influência na vida de qualquer pessoa e na operação de setores importantes para o desenvolvimento e manutenção do País, como é o caso do setor industrial. Elas são importantes pelas facilidades e utilidades que fornecem à sociedade e, principalmente, por subsidiarem, na forma de recurso ou serviço, outras IEC, mais complexas ou não.

Ao passar dos anos, a interdependências verticais das infraestruturas críticas, caracterizadas por um baixo acoplamento entre elas, deu lugar às interdependências horizontais altamente acopladas, com muitos pontos de interação em suas dimensões (BAGHERY, 2007). Como exemplo, as indústrias de energia exercem um papel fundamental no funcionamento dos sistemas de abastecimento de água e de transportes (CARVALHO, 2014). Na prática, com a ausência da operação apropriada de uma IEC, as funções de outras poderiam ser interrompidas (BRASIL, 2010).

Contudo, nem toda usina hidrelétrica ou qualquer aeroporto são críticos, mas sim aqueles que realmente causem impactos (social, ambiental, econômico, político ou à segurança) e que possam vir a ter uma repercussão nacional. O reflexo internacional também está inserido na definição porque existem infraestruturas que têm extrema relevância econômica para o País, como os cabos submarinos de telecomunicações, que fazem a ligação com os EUA, Argentina e Espanha, assim como a exportação de petróleo para os diversos países (DEMETERCO, 2011).

As áreas prioritárias das infraestruturas críticas, sem prejuízo de outras que porventura vierem a ser definidas, são expressas nos incisos de I a V do art. 3º da mesma Portaria Nº 02, do GSI e compreendem: Energia, Transporte, Água, Telecomunicações e Finanças. A Portaria instituiu ainda os Grupos Técnicos de Segurança das Infraestruturas Críticas (GTSIC), com a finalidade de propor a implementação de medidas e ações relacionadas com a segurança destas.

Após estudos dos GTSIC, concluiu-se que não existem, em diversos órgãos públicos e em algumas instituições privadas, redundâncias (de energia, de telecomunicações, de água, os quais são insumos básicos para qualquer infraestrutura crítica), bem como planos de contingência, de segurança e de recuperação (DEMETERCO, 2011).

Tendo em vista a importância das instituições devido à área de atuação que compõem as infraestruturas críticas de um país para a segurança nacional, devem ser

adotadas e implementadas estratégias efetivas para evitar, minimizar e mitigar os riscos oriundos das ameaças existentes.

2.2 HISTÓRICO

O tema proteção de infraestrutura crítica vem recebendo atenção crescente em diversos países da América do Norte, Europa, Ásia e Oceania a ponto de alguns terem criado órgãos governamentais específicos para tratar do assunto. Embora as estratégias adotadas por tais países sejam distintas, o objetivo final, entretanto, é sempre o mesmo, qual seja: proteger as infraestruturas críticas e seus elementos-chave contra atividades terroristas e/ou espionagem, desastres naturais e situações de emergência.

O emprego do termo Proteção de Infraestruturas Críticas é utilizado por vários países, mas o Brasil preferiu adotar a palavra Segurança por considerar esta mais abrangente, incluindo nela a gestão de continuidade dos negócios (DEMETERCO, 2011).

Cada país busca minimizar os principais riscos, com base em diferentes necessidades e utilizando abordagens distintas, incluindo posição estratégica e interesses nacionais dentro do cenário mundial. Vários deles tratam o tema para todas as suas infraestruturas consideradas críticas: telecomunicações, energia, água, monumentos históricos, defesa nacional etc. Em grande parte a maior preocupação é com o terrorismo, principalmente após os ataques de 11 de setembro de 2001, ocorridos nos EUA.

Percebe-se que há poucas informações a respeito do tema Proteção da Infraestrutura Crítica disponíveis em fontes públicas, pois a grande maioria dos países trata a questão como segurança nacional, aspecto que reforça a necessidade de estabelecimento de acordos de cooperação multilaterais entre países, objetivando o intercâmbio de informações e a atuação colaborativa (DEMETERCO, 2011).

O primeiro país a tratar de uma forma mais organizada a questão das novas vulnerabilidades em suas infraestruturas críticas foram os EUA, que possuem 16 áreas consideradas IEC, dentre elas os ícones que afetam diretamente o moral da sociedade estadunidense, como os setores financeiro, de energia e de sua base

industrial de defesa.

Já a China e a Coréia do Sul possuem oito áreas; o Reino Unido, dez (EUROPA, 2006); Canadá, dez; e a Austrália em conjunto com a Nova Zelândia, nove áreas (AUSTRÁLIA-NOVA ZELÂNDIA, 2015).

Fica evidente que as ações terroristas foram, inicialmente, as principais causas que levaram os diversos países a reconhecerem a importância das infraestruturas críticas.

O tema segurança de infraestruturas críticas começou a ser tratado no Brasil pelo GSI no segundo semestre de 2006.

Segundo Demeterco (2011), dos países que compõem o denominado “BRICS”, o Brasil é o único que ainda não implementou completamente a proteção das infraestruturas críticas. A África do Sul realizou por uma necessidade de se preparar para a Copa do Mundo de 2010.

Os EUA tinham, até 1995, o ataque terrorista em Oklahoma como o principal incidente, com 168 mortos e mais de 500 feridos e que era considerado, até o marco histórico de 11 de setembro de 2001, como o pior ocorrido em solo americano.

Atualmente, além da proteção contra as ações terroristas, o Departamento Norte-americano de Segurança Nacional, conhecido no original em inglês como *U.S. Departament of Homeland Security* (DHS) realiza, dentre outras ações, o monitoramento dos desastres naturais e ministra curso de proteção de infraestruturas críticas, graças à atuação de diversos agentes que orientam os procedimentos que devem ser observados quanto à gestão de riscos.

Desde sua criação, logo após o 11 de setembro de 2001, o DHS vem crescendo continuamente e hoje conta com mais de 240.000 empregados, representando o terceiro maior departamento do governo norte-americano, somente atrás dos Departamentos de Defesa e dos Veteranos; que refletem o orçamento hegemônico em forças armadas, maior do que a soma de todos os outros países.

Incidentes e acidentes também catalisaram outros países a desenvolverem estruturas de proteção das IEC. Por exemplo, na Rússia, em 2009, ocorreu um incidente com a sexta maior usina hidrelétrica do mundo, a Sayano–Shushenskaya, que gerava um quarto de toda a energia consumida pela Rússia, supria 10% da energia da Sibéria e 70% das fábricas de alumínio. A Rússia possui a maior indústria produtora de alumínio do mundo, a United Company Rusal (DEMETERCO, 2011).

Esse fato serve bem para ilustrar a segurança que se deve ter com as

infraestruturas críticas, principalmente aquelas que tenham grande impacto social e econômico a um país.

Outro exemplo de acidente em uma infraestrutura crítica foi a explosão da plataforma petrolífera no Golfo do México, em 2010, da Transocean (uma das maiores empresas de perfuração do mundo) em campanha de exploração no Campo de Macondo para a British Petroleum (BP).

Segundo inquérito interno da BP, a explosão ocorreu porque a tampa do poço teria falhado devido a uma bolha de metano que escapou do poço foi lançada pela coluna de perfuração e se expandiu rapidamente, rompendo várias barreiras de segurança e lacres de cimento até explodir. Tudo isso teria ocorrido ao longo da cimentação.

O relatório final da comissão, criada pelo presidente dos EUA, concluiu que a explosão da plataforma de exploração de petróleo Deep Horizon, no Golfo do México, foi resultado de várias falhas individuais e erros cometidos pela BP e suas prestadoras de serviço, Halliburton e Transocean, que poderiam ter sido evitados.

Estima-se que cinco milhões de barris de petróleo tenham sido despejados no mar, causando um dos maiores acidentes ambientais da nossa história. A britânica BP foi processada em bilhões de dólares pelo governo dos Estados Unidos; e 11 pessoas desapareceram e 17 ficaram feridas, segundo o *Deepwater Horizon Study Group*, grupo de estudo criado para apurar o acidente (DHSG, 2011).

No Brasil, a invasão em maio de 2007 da usina de Tucuruí, no Pará, pelo Movimento dos Atingidos por Barragem (MAB) foi um exemplo típico de como a gestão de risco é extremamente importante para as infraestruturas críticas. O incidente ocorreu porque o MAB conhecia as vulnerabilidades da usina, cujos detalhes foram obtidos durante visitações turísticas àquela usina hidrelétrica, ocasião em que se permitia o acesso de pessoas a locais que deveriam ser negados a visitantes devido à sensibilidade.

Só após o incidente foi realizada uma análise de risco, com ênfase nas ameaças, sendo levantadas as principais vulnerabilidades para mitigar os riscos verificados e, atualmente, a usina tem um plano de contingência e seu sistema de segurança patrimonial e operacional foi reformulado (DEMETERCO, 2011).

3 SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS NO BRASIL

No Brasil, até o ano de 2006, não existia órgão governamental encarregado de discutir aspectos relacionados à segurança de infraestruturas críticas (IEC). Decorrente de uma visita de integrantes do governo federal ao estado de São Paulo, onde a facção criminosa Primeiro Comando da Capital (PCC) atuava violentamente contra as autoridades de segurança do Estado, o então presidente Lula demandou ao Ministro do GSI, General Félix, a realização de um trabalho para identificar as instituições que deveriam ter sua segurança priorizadas (DEMETERCO, 2011).

Em agosto de 2006, o GSI reuniu todas as agências reguladoras para discutir aspectos relacionados à segurança de IEC. Nessa ocasião, foi realizada uma apresentação por um representante do governo norte-americano que repassou a experiência do *Department of Homeland Security* (DHS), órgão criado a partir dos atentados terroristas em 2001 para coordenar e articular as ações na proteção de IEC nos EUA.

O começo da discussão sobre o tema segurança de infraestruturas críticas no Brasil ocorreu com realização dos jogos Pan Americanos, em julho de 2007, com a participação, dentre outras, da Agência Brasileira de Inteligência (ABIN), Agência Nacional de Telecomunicações (Anatel) e Agência Nacional de Energia Elétrica (ANEEL).

3.1 BASE LEGAL

A Resolução do GSI Nº 002, de 24 de outubro de 2007, aprovada pelos ministros que integram a Câmara de Relações Exteriores e Defesa Nacional (CREDEN) e dos comandantes militares de cada Força Singular, propôs ao Presidente da República incluir o tema Segurança de Infraestrutura Crítica em área de sua competência e instituir o Grupo Técnico de Segurança de Infraestrutura Crítica, visando implementar medidas e ações relacionadas à questão, iniciando pelos setores de energia, transporte, água e telecomunicações.

O Decreto nº 6.371, de 12 de fevereiro de 2008, atendeu à sugestão da

CREDEN, ao incluir o inciso IX (ao artigo 1° do antigo Decreto nº 4.801, de 6 de agosto de 2003) com a atribuição para conduzir “ações cujo escopo ultrapasse a competência de um único Ministério” pertinentes à “segurança para as infraestruturas críticas, incluindo serviços”.

3.1.1 Política Nacional de Segurança de IEC

A Política Nacional de Segurança de Infraestruturas Críticas tem por finalidade orientar as ações necessárias para assegurar a prestação de serviços indispensáveis ao Estado e à sociedade brasileira.

Os pressupostos da Política Nacional de Segurança de Infraestruturas Críticas são:

I - Obediência à Constituição Federal e às leis;

II - Esforço conjunto de Estado, sociedade e cidadão;

III - Caráter permanente;

IV - Ação prioritariamente preventiva; e

V - Abrangência de todos os setores da vida nacional.

Os objetivos da Política Nacional de Segurança de Infraestruturas Críticas são:

I - cartório da 2ª vara cível Identificação das infraestruturas críticas do País;

II - Identificação de ameaças e fatores de riscos;

III - Redução dos impactos resultantes;

IV - Pronto restabelecimento dos serviços e sistemas;

V - Desenvolvimento de mentalidade de Segurança de Infraestruturas Críticas;

VI - Capacitação de recursos humanos; e

VII - Conscientização da sociedade para a Segurança de Infraestruturas Críticas.

3.1.2 Implementação de Medidas e Ações

A CREDEN, através de resoluções (de 2007 a 2010), instituiu o Grupo Técnico de Segurança de Infraestruturas Críticas (GTSIC) para estudar e propor a implementação de medidas e de ações relacionadas com a segurança das infraestruturas críticas, iniciando pelas seguintes áreas:

- Energia
- Telecomunicações
- Transportes
- Água
- Finanças

Foram criados grupos técnicos no âmbito do Gabinete de Segurança Institucional da Presidência da República (GSI), para discutir a proteção das infraestruturas críticas, nas linhas temáticas acima citadas, com as seguintes ações a realizar:

- Levantar as infraestruturas críticas;
- Identificar as suas vulnerabilidades;
- Avaliar os riscos que possam comprometer a continuidade dos serviços;
- Definir medidas de proteção;
- Implementar GCN – Gestão por Continuidade do Negócio e;
- Verificar reflexos de uma Infraestrutura Crítica em outras (interdependências).

Destaca-se que tais ações conduzidas por cada GTSIC tiveram um caráter analítico de levantamento de dados como um diagnóstico apenas, sem avanços consideráveis no que tange à efetiva implementação de medidas de proteção. Ou seja, após os trabalhos dos grupos passou-se a conhecer o “problema”, mas quase nada foi feito para “agir e resolver o problema”.

3.1.3 Estratégia Nacional de Defesa

Outro marco legal é a Estratégia Nacional de Defesa (END), que descreve a ação estratégica de “contribuir para o incremento do nível de segurança nacional”, as atribuições aos Ministérios da Defesa, Minas e Energia, Transportes, Integração Nacional e das Comunicações com a missão de adotarem medidas para a segurança das infraestruturas críticas nas áreas de energia, transporte, água e telecomunicações.

Ressalta-se que, nessa ação estratégica, coube ao GSI a atribuição de coordenação, avaliação, monitoramento e redução de risco e que as ações decorrentes desses quatro verbos demandam tempo, gestor e recursos, principalmente por envolver diversas instituições que têm interesses distintos para cada área.

Em resumo, a base legal para a articulação do GSI junto aos demais órgãos restringe-se ao Decreto nº 6.371, de 12 de fevereiro de 2008, e a Estratégia Nacional de Defesa.

3.2 PROTEGER – SISTEMA INTEGRADO DE PROTEÇÃO DE ESTRUTURAS ESTRATÉGICAS TERRESTRES

Hidrelétricas, redes de transmissão de energia, refinarias, portos e aeroportos são instalações essenciais ao desenvolvimento de um país. Para garantir a segurança dessas estruturas, foi criado em 2012 o Projeto Estratégico PROTEGER, sob responsabilidade do Comando do Exército Brasileiro.

Em seu escopo, o projeto priorizou a necessidade de proteção de 664 Estruturas Estratégicas Terrestres, termo usado para fazer referência às instalações, aos bens e serviços e aos sistemas que, se forem interrompidos ou destruídos, provocarão impacto severo no Estado e na sociedade. Ou seja, um novo termo, mas muito similar ao entendimento que se tem para Infraestruturas Críticas (IEC).

O Projeto Estratégico do Exército (PEE) denominado como Sistema Integrado de Proteção da Sociedade – PEE PROTEGER é um sistema complexo que visa

ampliar a capacidade do Exército Brasileiro de coordenar operações na proteção da sociedade, destacando-se a proteção de Estruturas Estratégicas Terrestres em situação de crise, apoio a defesa civil em caso de calamidades naturais ou provocadas, coordenação de segurança em grandes eventos, realização de operações de garantia da lei e da ordem, de garantia da votação e da apuração, de contraterror, de defesa química, biológica, nuclear e radiológica, de proteção ao meio ambiente e outras operações subsidiárias (BRASIL, 2016).

Destaca-se no escopo do PEE PROTEGER, o Sistema de Coordenação de Operações Terrestres Interagências (SISCOTI), que permitirá a coordenação de eventos de toda ordem contando com a parceria das Forças Armadas, outros órgãos e agências governamentais federais e estaduais e, ainda, empresas e instituições civis de interesse.

Beneficiado pela capilaridade e presença do Exército Brasileiro e de sua reserva mobilizável em todo território nacional, o PROTEGER, por intermédio do SISCOTI, será integrado aos demais sistemas de segurança existentes no País, e sob a supervisão do Ministério da Defesa, terá como órgão executivo o Comando de Operações Terrestres.

Entre as estruturas priorizadas estão instalações responsáveis pela geração de 56% da energia elétrica no País, com mais de 100 mil quilômetros de linhas de transmissão.

“Estruturas como essas já contam com sua própria segurança, mas, caso ela falhe, o Exército deve estar preparado para agir”, afirmou o General de Divisão William José Soares, gerente do projeto em abril de 2015 (DIÁLOGO, 2015).

“O PROTEGER visa também equipar e capacitar melhor o Exército para a proteção da sociedade em casos de calamidades, como enchentes, desabamentos e seca. Nesses casos, atuamos de maneira complementar aos órgãos públicos”, completa o General de Divisão Soares.

Ao longo do ano de 2012, ocorreram as principais ações do projeto com:

– a aquisição de equipamento de comunicações, materiais de saúde, viaturas administrativas, viaturas operacionais não blindadas, ferramentais para manutenção de viaturas, materiais e equipamentos individuais e coletivos, materiais de engenharia, mobiliários e equipamentos gerais;

– a adequação de organizações militares para atender às demandas do projeto; e

– a construção de instalações em diferentes guarnições militares.

Tanto em sua atuação em casos de calamidades quanto na defesa das estruturas estratégicas, a intenção do Exército é trabalhar em equipe, permitindo a soma da expertise dos diversos organismos de segurança brasileiros, como a Polícia Federal e a Defesa Civil.

Por isso, as autoridades de segurança criaram o SISCOTI, que será formado por 19 unidades, chamadas de Centro de Coordenação de Operações Terrestres Interagências (CCOTI), e terá sua estrutura principal construída na capital, Brasília. Já os outros centros funcionarão juntos às unidades militares espalhadas pelo Brasil.

Segundo o General de Divisão Soares “o CCOTI de Brasília vai abrigar uma unidade de Comando e Controle mais moderna, além de contar com espaço para as equipes das agências envolvidas na solução de uma determinada situação” (DIÁLOGO, 2015).

Em 2015, o Projeto PROTEGER planejava lançar um pedido de oferta às empresas interessadas em apresentar soluções para a implementação do SISCOTI, começando pela unidade de Brasília, mas restrições orçamentárias impediram de se seguir adiante. Espera-se que as empresas ofereçam sugestões em relação à construção das instalações físicas, dos equipamentos necessários, do preparo de pessoal para uso desses equipamentos, ou seja, proposta de uma solução global integrada para o SISCOTI.

O lançamento desse pedido de oferta dependerá da disponibilidade de recursos, que segundo as autoridades deverá ser necessário cerca de R$ 1 bilhão para financiar o projeto. Além da estrutura física, o SISCOTI prevê o desenvolvimento de software pelo Departamento de Ciência e Tecnologia do Exército, apelidado de "Protetor", que permitirá a integração das informações disponíveis nos bancos de dados dos órgãos e agências de segurança brasileiros.

Com essa nova ferramenta, o PROTEGER buscará alcançar uma maior capacidade de prevenir eventos indesejados. A ideia é fazer um monitoramento contínuo das regiões priorizadas, utilizando principalmente o software integrador.

A distribuição e a instalação dos CCOTI são decididas conforme a localização das estruturas estratégicas que o projeto visa a assegurar. As unidades militares que receberão prioritariamente um CCOTI serão aquelas com mais estruturas estratégicas sob sua responsabilidade, por esse motivo, os centros deverão ser dotados de duas qualidades básicas: mobilidade e flexibilidade.

A mobilidade para facilitar o rápido deslocamento em direção aos pontos necessitados, e a flexibilidade para adaptar o contingente a ser mobilizado em virtude do tamanho dos problemas.

Em relação à capacidade de deslocamento, o PROTEGER planeja equipar cada CCOTI com pelo menos 13 tipos diferentes de viaturas. Embora os centros ainda não tenham sido construídos, o projeto já deu início ao fornecimento de equipamentos para os oito Comandos Militares de Área do Exército.

O primeiro foi o Comando Militar do Sul, do qual faz parte a 15ª Brigada de Infantaria Mecanizada, escolhida para receber o projeto-piloto do PROTEGER, pois está localizada em Cascavel, no estado do Paraná, a cerca de 120 km da Usina Hidrelétrica de Itaipu – uma das maiores produtoras de energia elétrica do mundo, responsável pelo fornecimento de 17% da energia consumida no Brasil.

Em 2012, foram liberados R$ 79 milhões para a instalação do projeto-piloto em Cascavel. O montante foi usado na aquisição de viaturas, equipamentos individuais para os militares, equipamentos de comunicação e melhoria das instalações físicas do local (DIÁLOGO, 2015).

Em 2013, foram compradas em torno de 2 mil viaturas de emprego geral. Os veículos foram entregues a outras brigadas e estão sendo usados tanto em atividades militares quanto administrativas das unidades. Também no mesmo ano, foram adquiridas 13 viaturas de Comando e Controle, das quais duas foram equipadas com tecnologia de transmissão de dados via satélite e usadas durante a Copa do Mundo, em 2014, quando o Exército colaborou nas ações de segurança do evento.

3.3 GABINETE DE SEGURANÇA INSTITUCIONAL

O Gabinete de Segurança Institucional experimentou recentemente, em um curto intervalo de tempo, sua extinção em outubro de 2015 e recriação em maio de 2016.

O GSI tem como área de competência assuntos ligados à assistência direta e imediata ao Presidente da República (PR) no desempenho de suas atribuições; à prevenção da ocorrência e articulação do gerenciamento de crises, em caso de grave e iminente ameaça à estabilidade institucional; ao assessoramento pessoal em

assuntos militares e de segurança; à coordenação das atividades de inteligência de Estado e da informação; à segurança pessoal do Chefe de Estado, do Vice-Presidente da República (VPR) e dos respectivos familiares, dos titulares dos órgãos essenciais da Presidência da República e de outras autoridades ou personalidades quando determinado pelo Presidente da República, assegurado o exercício do poder de polícia; e à segurança dos palácios presidenciais e das residências do PR e do VPR, assegurado o exercício do poder de polícia.

Compete, ainda, ao GSI: executar, permanentemente, as atividades técnicas e de apoio administrativo, necessárias ao exercício da competência do Conselho de Defesa Nacional (CDN), de conformidade com o disposto na Lei nº 8.183, de 11 de abril de 1991; exercer as atividades de Secretaria Executiva da Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo, de conformidade com regulamentação específica; e exercer as atividades de Órgão Central do Sistema de Proteção ao Programa Nuclear Brasileiro (SIPRON).

Desde maio de 2016, a estrutura organizacional do GSI está em processo de atualização, mas segue atuando de maneira muito próxima àquela até outubro de 2015, quando foi provisoriamente extinto. Contudo, hoje não há menção no site do GSI às atividades de segurança de IEC, atribuição até aquela data da Secretaria de Acompanhamento e Articulação Institucional, que compreendia: monitorar e coordenar a atividade de segurança de infraestruturas críticas; coordenar e supervisionar a realização de estudos relacionados com a prevenção da ocorrência e articulação do gerenciamento de crises; realizar estudos estratégicos, especialmente sobre temas relacionados com a segurança institucional.

Recentemente, foi sancionada a Lei Nº 13.341 (29/09/2016) que dispõe sobre a organização da Presidência da República e dos Ministérios. Esta lei mantém o prestígio do Ministro de Estado Chefe do GSI como secretário-executivo do CDN e como presidente da CREDEN. No entanto, permanece a indefinição de qual órgão cuidará das atividades de segurança de IEC, como já dito, antiga atribuição da extinta Coordenadoria de Estruturas Estratégicas, dentro da Secretaria de Acompanhamento e Articulação Institucional, que não foram retomadas no atual organograma.

O estabelecimento de uma estrutura formal responsável pela promoção de ações para a segurança das IEC é, obviamente, fundamental para se desenvolver um programa de Estado com este fim, como pretende propor este estudo.

3.4 INFRAESTRUTURAS CRÍTICAS DE ÓLEO E GÁS

O petróleo é um recurso natural abundante, porém sua pesquisa, além de ser complexa, envolve elevados custos. Já foi causa de muitas guerras e é a maior fonte de renda de muitos países, sobretudo no Oriente Médio. É também a principal fonte de energia não renovável, servindo como base para fabricação dos mais variados produtos, dentre os quais destacam-se benzinas, óleo diesel, gasolina, alcatrão, polímeros plásticos e medicamentos.

O Brasil é o 12º produtor mundial de petróleo e o 7º maior consumidor e está entre as 20 maiores reservas do mundo.

Quanto ao pré-sal, a área que tem recebido destaque pelas recentes descobertas da Petrobras, encontra-se no subsolo do Oceano Atlântico e estende-se do Norte da Bacia de Campos ao Sul da Bacia de Santos.

Destacam-se como infraestruturas, que merecem atenção por ter influência na área social, econômica e internacional, as grandes bacias existentes, como o pré-sal, as plataformas marítimas (*offshore*), os dutos e refinarias de petróleo.

Mas quais são realmente as infraestruturas críticas? Quais são aquelas que necessitam de um “olhar mais crítico” do Estado? Estas perguntas têm que ser respondidas com base em uma metodologia que possa dar respaldo científico a um trabalho que venha a melhorar as infraestruturas do Brasil, e não de forma empírica.

Para tanto, em 16 de junho de 2008, pela Portaria Nº 11 - GSIPR/CH, foi instituído o Subgrupo Técnico de Segurança de Infraestruturas Críticas de Petróleo, Gás Natural e Combustíveis Renováveis (SGTSIC-PEGANCOR), com a atribuição maior de propor a implementação de medidas e ações relacionadas com a segurança das Infraestruturas Críticas (IEC) na área de Petróleo, Gás Natural e Combustíveis Renováveis, que possam afetar, de forma direta ou indireta, a operação do setor.

O SGTSIC-PEGANCOR era composto pelos seguintes membros:

I. Gabinete de Segurança Institucional da Presidência da República, na função de coordenação;
II. Ministério das Minas e Energia (MME);
III. Ministério da Agricultura, Pecuária e Abastecimento;
IV. Empresa Brasileira de Pesquisa Agropecuária (Embrapa);

V. Embrapa - Monitoramento por Satélite;
VI. Agência Nacional do Petróleo, Gás Natural e Biocombustíveis (ANP);
VII. Petróleo Brasileiro S.A. (Petrobras); e
VIII. Órgãos e especialistas convidados pelo GSI.

Já se previa que o subgrupo técnico poderia interagir com outros órgãos para consulta e adoção de providências necessárias à complementação dos trabalhos atribuídos pela portaria.

Estabelecia ainda que as medidas e ações necessárias seriam relatadas à Câmara de Relações Exteriores e Defesa Nacional (CREDEN), por intermédio de seu coordenador.

As atribuições do SGTSIC-PEGANCOR constantes na Portaria eram:

I. pesquisar e propor um método de identificação de IEC;
II. identificar as IEC;
III. levantar e avaliar as vulnerabilidades das IEC identificadas e sua interdependência;
IV. selecionar as causas e avaliar os riscos que possam afetar a segurança das IEC;
V. propor, articular e acompanhar medidas necessárias à segurança das IEC; e
VI. estudar, propor e implementar um sistema de informações que conterá dados atualizados de IEC para apoio a decisões.

Todavia, desde a publicação da portaria em junho de 2008, que formalizava a divisão em subgrupos, o SGTSIC-PEGANCOR efetivamente alcançou apenas as duas primeiras atribuições. Foram realizadas quatro reuniões ao longo de 2008 (entre julho e novembro) com os representantes designados, somente uma em 2009 (novembro) e a derradeira ocorreu em maio de 2010.

Após isto, representantes do GSI visitaram algumas instalações da Petrobras para conhecer suas vulnerabilidades e riscos associados e buscar compreender a interdependência entre as IEC, mas infelizmente o trabalho foi descontinuado com a troca de comando do GSI, no início de 2011.

O último registro que se tem sobre a discussão do tema foi o X Ciclo de Estudos Estratégicos: Proteção das Infraestruturas Críticas, promovido pela Escola de Comando e Estado-Maior do Exército (ECEME) em maio de 2011, no entanto, nenhuma outra iniciativa foi proposta pelo GSI, nem a Petrobras voltou a ser

contatada.

Assim, percebe-se que nada foi desenvolvido sobre a adoção de medidas efetivas de segurança, tampouco no incremento de um sistema de informações de IEC integrado; conforme constavam na Portaria Nº 11 - GSIPR/CH, de 16 de junho de 2008.

4 PROTEÇÃO DE INFRAESTRUTURA CRÍTICA NOS EUA

Em maio de 1998, foi estabelecido pela primeira vez um programa nacional para garantir a segurança das infraestruturas vulneráveis e interligadas dos Estados Unidos, denominado *Critical Infrastructure Protection*, em tradução livre: Proteção da Infraestrutura Crítica.

Por meio de uma diretriz presidencial, *Presidential Decision Directive*-63 (PDD-63), o então mandatário Bill Clinton reconheceu determinadas partes da infraestrutura nacional, como críticas para a segurança nacional e econômica dos Estados Unidos da América e para o bem-estar dos seus cidadãos, e as etapas necessárias a serem tomadas para protegê-las (FAS, 2016).

Essa diretriz foi atualizada em dezembro de 2003, pelo então presidente Bush na *Homeland Security Presidential Directive* (HSPD-7), com o título traduzido como Identificação, Priorização e Proteção de Infraestrutura Crítica. A nova diretriz descreve, em tradução livre, que os EUA têm algumas infraestruturas críticas que são “tão vitais para os Estados Unidos da América que a incapacidade ou a destruição de tais sistemas e ativos teriam um impacto debilitante sobre a segurança, a segurança econômica nacional, a saúde ou a segurança pública nacional” (EUA, 2015).

O Plano Proteção da Infraestrutura Nacional (NIPP, da sigla em inglês) mais recente foi rotulado como, em tradução livre, “NIPP 2013: Parcerias para a Segurança e Resiliência da Infraestrutura Crítica” e visa descrever o modo como o governo e os participantes do setor privado podem atuar em conjunto para gerenciar riscos e alcançar os resultados esperados de segurança e resiliência e reconhece que o bem-estar da nação norte-americana depende de infraestruturas críticas seguras e resistentes, pois são esses ativos, sistemas e redes que sustentam a sociedade americana (EUA, 2013).

4.1 *DEPARTMENT OF HOMELAND SECURITY*

O Departamento de Segurança Interna dos EUA (DHS, da sigla em inglês) combina 22 diferentes departamentos e agências federais em uma entidade de

gabinete unificado e integrado, desde sua criação em 2002.

O movimento para criação do DHS começou onze dias após os ataques terroristas de 11 de setembro de 2001, quando Tom Ridge, governador da Pensilvânia à época, foi nomeado como o primeiro diretor do Escritório de Segurança Nacional na Casa Branca.

O escritório supervisionou e coordenou uma estratégia nacional abrangente para proteger aquele país contra o terrorismo e responder a quaisquer futuros ataques.

Com a aprovação da Lei de Segurança Interna pelo congresso norte-americano em novembro de 2002, o DHS transformou-se oficialmente em um departamento autônomo e passou a coordenar e unificar esforços nacionais de segurança interna, iniciando seus trabalhos em 1º de março de 2003 (EUA, 2013).

As atribuições do DHS incluem o serviço aduaneiro, o controle de fronteiras e a fiscalização de imigração; a resposta de emergência a catástrofes naturais e provocadas pelo homem; o trabalho antiterrorismo; e a segurança cibernética.

4.2 *OFFICE OF INFRASTRUCTURE PROTECTION*

O Escritório de Proteção de Infraestrutura (IP, da sigla em inglês) lidera e coordena programas e políticas sobre segurança da infraestrutura crítica e ao longo do tempo conseguiu estabelecer fortes parcerias em todas as esferas de governo e no setor privado.

O IP conduz e facilita as avaliações de vulnerabilidade e impacto para ajudar proprietários e operadores de IEC e órgãos estatais até o nível local a entender e contemplar os riscos pertinentes, justamente, às infraestruturas críticas.

Além disso, o IP fornece informações sobre as ameaças emergentes, de modo que se possam tomar medidas preventivas apropriadas e também oferece ferramentas e treinamento para parceiros para ajudá-los a gerir os riscos de seus ativos, sistemas e redes (EUA, 2013).

Percebe-se que para o desenvolvimento de um plano nacional de proteção das IEC há extrema necessidade de sinergia entre os diversos órgãos de governo, mas, principalmente, do envolvimento do setor privado nas discussões e proposições.

Caso o plano fosse elaborado somente por servidores do Estado, ele seria desconectado da realidade e não contaria com a adesão voluntária que se pretende conseguir. Enfatiza-se muito a “parceria” necessária entre o governo e os participantes do setor privado na comunidade de IEC, para trabalharem juntos na gestão dos riscos e no incremento dos níveis de segurança e de resiliência (EUA, 2013).

Obviamente, a algumas IEC são impostas medidas de segurança e exigidas que desenvolvam planos de segurança locais, porém todas as empresas, tanto as voluntárias, quanto as acionadas compulsoriamente, são elegíveis para participarem de programas subvencionados pelo Estado, bastando apresentar um projeto nas diversas linhas de financiamento não reembolsável. Existe um site que aglutina todos os tipos de subvenções (www.grants.gov).

4.3 *NATIONAL INFRASTRUCTURE PROTECTION PLAN*

O plano nacional norte-americano de proteção de IEC (EUA, 2013) mais recente foi lançado em 2013, comumente chamado de NIPP 2013, que representa uma evolução de conceitos introduzidos na versão original do NIPP lançado em 2006 e revisto em 2009.

O plano é simplificado e adaptável aos atuais ambientes de risco, político e estratégico e fornece a base para uma abordagem integrada e colaborativa para alcançar a visão de uma nação, onde a IEC física e cibernética permanecem seguras e resistentes, com vulnerabilidades reduzidas, consequências minimizadas, ameaças identificadas e interrompidas, e resposta e recuperação acelerada quando necessária.

O plano de 2013 foi desenvolvido através de um processo colaborativo envolvendo as partes interessadas, contando com os 16 setores de infraestrutura crítica, todos os 50 estados, e de todos os níveis de governo e da indústria e fomenta ações para alavancar parcerias, inovar para gestão de riscos, e foco em resultados.

Dessa maneira, o plano contém as linhas gerais para que a respectiva agência desenvolva e implemente o plano de cada setor, o qual deve detalhar a aplicação dos conceitos do NIPP segundo as especificidades, características e condições únicas de seu setor e sua atualização segue o lançamento de uma nova versão do NIPP.

5 PROPOSTA DE MODELO PARA O BRASIL

Como principal objetivo deste trabalho, pretende-se propor um modelo para o Brasil (baseado no norte-americano) que alavanque a segurança física das IEC como um programa de Estado, que conscientize a sociedade civil como um todo sobre sua importância, para assim perdurar independente das mudanças de governos.

Apesar do escopo se ater às instalações terrestres do setor de O&G, de antemão, vislumbra-se que a proposta poderia ser extrapolada para outros segmentos.

Adota-se como premissa que proprietários, concessionários e operadores das IEC serão compelidos a implementar medidas mínimas de segurança no que tange ao cercamento periférico e à de segregação de áreas internas, ao controle de acesso (procedimentos, sistema de identificação, portões e catracas), à iluminação, ao monitoramento de câmeras e às medidas de reação.

5.1 ADOÇÃO COMPULSÓRIA

Um bom exemplo vigente em nosso País de adoção compulsória é o do código internacional para segurança de navios e instalações portuárias, em inglês, *International Ship and Port Facility Code (ISPS Code)*, que se aplica àqueles que desejam transacionar globalmente.

O procedimento surgiu pela notoriedade de que portos e navios sempre foram meios e vetores de diversos ilícitos, o que desencadeou uma pressão comercial dos países mais desenvolvidos de que os demais que quisessem continuar transacionando com eles deveriam aderir ao código, assim, o Brasil passou a ser signatário e o internalizou na forma do Decreto Nº 6.869[1], de 4 de junho de 2009.

Já no caso das IEC, o maior interessado é o nosso próprio País, pois a sociedade estará diretamente afetada. Por isso, parece razoável que seja importante

[1] Dispõe sobre a coordenação e articulação dos órgãos federais, os níveis de proteção dos navios e das instalações portuárias, da adoção de medidas de proteção aos navios e instalações portuárias, e institui a Rede de Alarme e Controle dos Níveis de Proteção de Navios e Instalações Portuárias.

para o Estado brasileiro fomentar a segurança das IEC e, portanto, em contrapartida às obrigações que serão impostas às organizações que gerenciam as IEC, sejam ofertadas desonerações tributárias e linhas de financiamento reembolsáveis ou não.

5.2 DESONERAÇÃO TRIBUTÁRIA

Para financiar seus gastos, os governos utilizam-se da arrecadação compulsória de recursos – que em termos técnicos caracteriza a tributação de um país. O conjunto de normas que definem e delimitam o processo de arrecadação compõe o sistema tributário legal.

Em geral, os sistemas tributários não possuem outro objetivo, que não o de gerar recursos para a administração e o dispêndio de tais recursos é feito por fora do sistema tributário, por meio de orçamentos aprovados pelos representantes da população.

No entanto, o sistema tributário é permeado por desonerações, que são caracterizadas por todas e quaisquer situações que promovam: presunções creditícias, isenções, anistias, reduções de alíquotas, deduções, abatimentos e diferimentos de obrigações de natureza tributária.

As desonerações, em sentido amplo, podem servir para diversos fins, como promover a equidade; compensar ações complementares às funções típicas de estado desenvolvidas por entidades civis; incentivar determinado setor da economia etc., passando a compor o que se convencionou denominar “gastos tributários”.

Tem-se como exemplo de gasto tributário para promoção do setor de produtos e sistemas de defesa, o Regime Especial Tributário para a Indústria de Defesa (RETID), instituído pela Lei Nº 12.598, de 21 de março de 2012.

Propõe-se que, analogamente, sejam beneficiadas com desonerações tributárias as empresas que proveem os produtos e sistemas de segurança para IEC, beneficiando em última instância a empresa gestora da IEC.

Assim, a empresa teria o benefício fiscal de não incidência do Imposto sobre Produtos Industrializados (IPI[2]) na aquisição no mercado interno, IPI vinculado na

[2] IPI é um imposto federal, ou seja, somente a União pode instituí-lo ou modificá-lo, sobre produtos industrializados nacionais e estrangeiros. Está previsto no art. 153, IV, da CF. Suas disposições estão

importação, suspensão de Programas de Integração Social (PIS) e Cofins[3] sobre a venda no mercado interno ou importação de partes, peças, ferramentas, componentes, equipamentos, sistemas, subsistemas, insumos, matérias-primas, serviços de tecnologia industrial básica, desenvolvimento e inovação tecnológica, assistência técnica e transferência de tecnologia a serem empregados na manutenção, conservação, modernização, reparo, revisão, conversão, industrialização de bens de segurança, quando a aquisição for efetuada por pessoa jurídica cuja a instalação é classificada como IEC. A suspensão também se aplicaria à receita na modalidade de aluguel de máquinas, aparelhos, instrumentos e equipamentos.

Como exemplo prático do nosso caso, uma empresa de equipamentos e sistemas eletrônicos de circuito fechado de televisão (CFTV) teria os benefícios fiscais ao prover para uma refinaria classificada como IEC, o que tornaria mais econômica a aquisição para a Petrobras.

5.3 FINANCIAMENTO

Além da desoneração tributária, seriam criadas pelo Banco Nacional de Desenvolvimento Econômico e Social (BNDES) linhas de crédito reembolsáveis para as empresas de bens e serviços de segurança com taxas de juros especiais e prazos longos e não reembolsáveis para as empresas operadoras das IEC, notadamente a Petrobras.

Numa análise superficial e imediata, pareceria óbvio que a situação econômica atual inviabilizaria o programa proposto, contudo, a ideia é defensável pelos mesmos argumentos iniciais de que a interrupção de determinadas IEC pode gerar impacto econômico e social ainda mais grave para o País.

Nessa modalidade proposta, os gestores das IEC podem obter melhores níveis de segurança operacional; maior competitividade para o País; gerar mais

descritas no Decreto nº 7.212, de 15 de junho de 2010, que regulamenta sua cobrança, fiscalização, arrecadação e administração.

[3] PIS e Cofins são dois tributos previstos pela CF nos artigos 195 e 239.
Em suas definições temos: PIS (Programas de Integração Social e de Formação do Patrimônio do Servidor Público – PIS/PASEP) instituído pela Lei Complementar 07/1970 e Cofins (Contribuição para Financiamento da Seguridade Social, instituída pela Lei Complementar 70 de 30/12/1991.

emprego no mercado de segurança patrimonial, que se encontra estagnado; e impedir práticas criminosas que envolvem quadrilhas como no caso de desvio de derivados em dutos, por exemplo.

Vale ressaltar que por envolver renúncia fiscal, a proposta de programa só poderá entrar em vigor após aprovação de lei no âmbito do legislativo federal, estadual ou municipal, conforme a natureza do tributo, o que garante uma ampla discussão e amadurecimento dos mecanismos propostos.

Em um primeiro momento só se vislumbrou o compromisso da União, mas seria muito valiosa a adesão dos estados da federação, principalmente, na desoneração do ICMS.

5.4 AUDITORIA E CONTROLE

Outro aspecto relevante a ser definido por lei para garantir a perenidade e efetividade do programa se refere às responsabilidades pela fiscalização do uso dos produtos e serviços abrangidos. Há duas especialidades a serem consideradas: a de conhecimento técnico de segurança patrimonial e a de contabilidade.

Os conhecimentos técnicos de segurança devem abarcar a capacidade de criticar os estudos de análises de riscos, os planos de segurança locais, os requisitos funcionais dos equipamentos físicos e eletrônicos e, num nível mais complexo, especificações técnicas.

Já o conhecimento contábil serve para verificar se as previsões de desoneração tributária foram respeitadas sem exageros ou se os financiamentos foram aplicados adequadamente.

Parece natural que o Gabinete de Segurança Institucional (GSI) avoque para si, como órgão central de um sistema, as atribuições de implementar e manter a segurança das infraestruturas críticas do País.

Para isso, o GSI deve dar seguimento ao trabalho interrompido com as outras agências e ministérios pertinentes a cada setor, designando uma estrutura formal com dedicação exclusiva para desenvolver e implementar o sistema de informações que conterá toda a gama de dados atualizados de IEC (ameaças, vulnerabilidades, interdependência, redundância, impactos, catálogo de contramedidas, status de

implementação dos projetos etc.).

Também necessita ser capaz de aprovar os estudos e projetos de segurança em cada passagem de fase, em prazos compatíveis com a dinâmica do mercado; de se preparar tecnicamente para fiscalizar e aprovar a implementação *in loco* das contramedidas e procedimentos definidos e, principalmente, deve auditar de tempos em tempos a manutenção dos planos aprovados.

6 CONCLUSÃO

Nos últimos dez anos, houve iniciativas no âmbito do Gabinete de Segurança Institucional (GSI), visando desenvolver planos para segurança das infraestruturas críticas do Brasil.

Os trabalhos desenvolvidos pelo subgrupo técnico da área de Óleo & Gás (SGTSIC-PEGANCOR) atingiram tão somente o nível de identificação da IEC, iniciaram a verificação da interdependência entre IEC e de avaliação de vulnerabilidades e riscos associados, mas não avançaram sobre a adoção de medidas efetivas de segurança, tampouco no desenvolvimento de um sistema de informações de IEC integrado.

Dessa experiência, foi positiva a interação entre ministérios, agências e empresas, demonstrando que é profícuo dar representatividade para cada instituição interessada e as resoluções coletivas serão mais aderentes à realidade de quem opera as instalações classificadas como críticas.

Mesmo após sancionada a Lei Nº 13.341 (29/09/2016) que dispõe sobre a organização da Presidência da República e dos Ministérios, permanece a lacuna de qual órgão conduzirá o tema de segurança de IEC. Como já comentado, esta lei mantém o prestígio do Ministro de Estado Chefe do GSI como secretário-executivo do CDN e como presidente da CREDEN. Porém, não recupera a atribuição da extinta Coordenadoria de Estruturas Estratégicas, dentro da Secretaria de Acompanhamento e Articulação Institucional.

Segundo troca de correios eletrônicos com a Assessoria de Comunicação do GSI, eles reconhecem que segue indefinida a responsabilidade, mas afirmam que: “permanecemos na expectativa da inclusão do acompanhamento das infraestruturas críticas no rol das competências deste Gabinete”.

Dada a importância do tema, entende-se que o País precisa retomar a discussão, de forma definitiva e deveria ser criada uma estrutura formal dentro do GSI dedicada exclusivamente para capitanear as ações relativas à proteção de IEC, convocando novamente os subgrupos técnicos para definir os patamares mínimos de segurança a serem implantados, definir metas para os operadores das instalações, fiscalizar o cumprimento destas metas.

Este estudo propôs a criação de um modelo com o GSI tendo atribuições nos

níveis estratégico, tático e operacional, quando cabível, assumindo o papel de órgão central de Estado para a segurança de IEC e trabalhando em cooperação com outras agências, com regras – algumas já vigentes – que regulem as atividades e atribuam poderes para exigir o incremento e a manutenção da segurança nas IEC.

Como contrapartida das exigências que recairão sobre os operadores das IEC do setor petrolífero, serão ofertadas subvenções governamentais para a aquisição de bens e serviços de segurança com desoneração tributária e com linhas de créditos vantajosas para o setor.

A implantação de um programa robusto e bem gerenciado, auditado regularmente, fará com que o Brasil atinja um patamar de estabilidade na indústria de O&G, servindo como incentivo para novos investimentos de companhias nacionais e estrangeiras.

Indubitavelmente, trata-se de um tema estratégico de Estado e todas as nações, até mesmo as de orientação mais liberal, atuam ativamente para garantir e exigir que companhias privadas ou estatais estejam preparadas contra ameaças e apliquem os recursos necessários para incrementar a proteção física das instalações críticas. Logo, a discussão sobre o tema, por si só, já é salutar para o Desenvolvimento Nacional.

Para futuros estudos, tornar-se-á interessante analisar se as renúncias fiscais geraram realmente os ganhos coletivos esperados, se este tipo de programa permanece compensatório no longo prazo, se beneficia indevidamente atividades empresariais muito rentáveis ou se gerou acomodação e os modelos de negócios sucumbiriam sem os incentivos.

REFERÊNCIAS

AUSTRÁLIA-NOVA ZELÂNDIA. **The National Guidelines for the Protection of Critical Infrastructure (CI) from Terrorism**. 2015. Disponível em: <https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-guidelines-protection-critical-infrastructure-from-terrorism.pdf>. Acesso em: 06 mai. 2016.

BAGHERY, E. et al. **The State of the Art in Critical Infrastructure Protection: a Framework for Convergence**. Faculty of Computer Science, University of New Brunswick, Fredericton, N.B. Canada, 2007. Disponível em <http://ebagheri.athabascau.ca/papers/CIPFramework.pdf>. Acesso em: 17 ago. 2016.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**: promulgada em 5 de outubro de 1988: atualizada até a Emenda Constitucional nº 91, de 18-02-2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 06 mai. 2016.

BRASIL. Conselho de Defesa Nacional. **Portaria Nº 34, de 5 de agosto de 2009**. Conselho de Defesa Nacional, Secretaria Executiva. Institui Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação, no âmbito do Comitê Gestor de Segurança da Informação - CGSI. Brasília, DF, 2009.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Guia de Segurança de infraestruturas críticas da informação**. Brasília, DF, 2010.

_____. **Portaria nº 2 de 08/02/2008 / GSIPR.** Diário Oficial da União, Brasília, DF, 11 fev. 2008.

BRASIL. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército. Escritório de Projetos do Exército. Projetos Estratégicos do Exército. **Proteção das estruturas estratégicas terrestres do Brasil para garantia do bem-estar da sociedade**. Disponível em: <http://www.epex.eb.mil.br/index.php/proteger>. Acesso em: 06 mai. 2016.

CARVALHO, Regis de Souza de. **Proposta de arquitetura para coleta de ataques cibernéticos às infraestruturas críticas**. Rio de Janeiro: Instituto Militar de Engenharia, 2014.

DEMETERCO, Fernando Antônio. **A Proteção de Infraestruturas Críticas no Âmbito do Governo Federal**. Anais do X Ciclo de Estudos Estratégicos: Proteção das Infraestruturas Críticas. Escola de Comando e Estado-Maior do Exército. Rio de Janeiro, 2011. Disponível em: <https://www.eceme.ensino.eb.br/meiramattos/index.php/RMM/article/view/197/166>. Acesso em: 06 mai. 2016.

DIÁLOGO. **Projeto PROTEGER garante mais segurança à infraestrutura estratégica do Brasil**. 2015. Disponível em: <https://dialogo-

americas.com/pt/articles/projeto-proteger-garante-mais-seguranca-infraestrutura-estrategica-do-brasil>. Acesso em: 06 mai. 2016.

EUA. Departament of Homeland Security. **Energy Sector-Specific Plan - 2015**. 2015. Disponível em: <https://www.dhs.gov/publication/nipp-ssp-energy-2015#>. Acesso em: 06 mai. 2016.

_____. **National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience**. 2013. Disponível em: <https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience>. Acesso em: 06 mai. 2016.

EUROPA. **European Programme for Critical Infrastructure Protection**. 2006. Disponível em: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l33260>. Acesso em: 06 mai. 2016.

FAS - Federation of American Scientists. **Presidential Decision Directive/NSC-63**. Disponível em: <http://fas.org/irp/offdocs/pdd/pdd-63.htm>. Acesso em: 17 ago. 2016.

MANDARINO JR, Raphael. **Segurança e Defesa do Espaço Cibernético Brasileiro**. Brasília, p. 37 - 38, 2010.

DHSG - Deepwater Horizon Study Group. **Final Report on the Investigation of the Macondo Well Blowout.** 2011. Disponível em: <http://ccrm.berkeley.edu/pdfs_papers/bea_pdfs/dhsgfinalreport-march2011-tag.pdf>. Acesso em: 17 ago. 2016.