A ATIVIDADE DE INTELIGÊNCIA NA SEGURANÇA CIBERNÉTICA ÀS INFRAESTRUTURAS CRÍTICAS NACIONAIS DO SETOR DE ENERGIA ELÉTRICA

LUIS HENRIQUE SANTOS FRANCO[1]

RESUMO

O incremento da automação da informação no gerenciamento das Infraestruturas fundamentais de um país torna-se instigante, uma vez que a humanidade depara-se com o ambiente cibernético, ferramenta cada vez mais presente em conflitos modernos. Nesta direção, o atual gerenciamento operacional de grande parte das Infraestruturas Críticas Nacionais (ICN) do País é realizado de forma eletrônica com dispositivos remotos, por meio do uso maciço de *softwares* e sistemas de controle em tempo real. Parte daí a necessidade de se acompanhar e proteger tais sistemas, garantindo o pleno funcionamento dos serviços essenciais à população. Para a Inteligência, este assunto pode ser revolucionário, na medida em que amplia tanto as possibilidades de busca e coleta de dados, quanto as vulnerabilidades das redes computacionais das ICN. A fim de restringir o escopo desse estudo, a atenção é concentrada no setor de energia elétrica. Destarte, o presente trabalho visa estudar a adequação da Atividade de Inteligência na segurança às ICN, com foco na segurança cibernética do setor de energia elétrica brasileiro. O estudo foi baseado em pesquisas bibliográficas, entrevistas a personalidades governamentais de destacado conhecimento em suas áreas e na remessa de questionários para integrantes do Sistema de Inteligência do Exército (SIEx).

1 INTRODUÇÃO

A automação da informação encontra-se cada vez mais presente em empresas de caráter público ou privado. Nesta direção, o gerenciamento operacional de grande parte das Infraestruturas Críticas Nacionais[2] (ICN) é realizado de forma eletrônica e remota com o operador à distância, às vezes até em outro Estado. Isto só é perfeitamente factível por intermédio do uso maciço de *softwares* e sistemas digitais. Esse incremento na automação de coleta e transmissão de dados implica na necessidade de se proteger digitalmente tais sistemas, garantindo o pleno funcionamento dos serviços essenciais à população.

A dependência inevitável de sistemas computadorizados no controle operacional das infraestruturas de um país oferece uma nova dimensão de estudos de segurança e defesa.

Tais reflexões crescem de importância na medida em que o Brasil foi escolhido para sediar inúmeros eventos de amplitude mundial, a saber: Conferência Mundial Sobre o Meio Ambiente "Rio+20" (2012), Jornada Mundial da Juventude Católica e visita do Papa Bento XVI (2013), Copa das Confederações (2013),

[1] *Oficial (Major) da Arma de Engenharia do Exército Brasileiro, Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN), Mestre em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (EsAO), Mestre em Ciências Militares pela Escola de Comando e Estado-Maior do Exército (ECEME) e Especialista em Inteligência Militar pela Escola de Inteligência Militar do Exército (eSIMEx).*

[2] *ICN é defina pelo Gabinete de Segurança Institucional da Presidência da República (GSI-PR) como sendo o conjunto de instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade (MANDARINO JR, 2009, p. 7). Atualmente o termo está sendo atualizado pelo GSI-PR para Estruturas Estratégicas, englobando as instalações existentes, as em construção e aquelas que ainda estão em estudos. Entretanto, esta terminologia, até o fechamento deste artigo, ainda não estava homologada. Portanto, o termo utilizado por este autor será ICN.*

Copa do Mundo (2014), Olimpíadas e Paralimpíadas (2016).

Nesses eventos de grande envergadura aumenta a responsabilidade do papel do Estado como organizador e principalmente como garantidor da segurança e pleno funcionamento das ICN. Nesse contexto, Canongia e Mandarino Jr. (BRASIL, 2010), organizadores do Livro Verde da Defesa Cibernética, ressaltam que a Segurança Cibernética é um novo desafio deste século e que "vem se destacando como função estratégica de Estado, essencial à manutenção das infraestruturas críticas de um país, tais como Energia, Defesa, Transporte, Telecomunicações, Finanças, da própria Informação, dentre outras".

No Brasil, a Estratégia Nacional de Defesa (END), de 2008, ressalta que a área cibernética é um dos três setores estratégicos prioritários para o Estado Brasileiro. O grande objetivo é capacitar os recursos humanos a fim de constituir uma estrutura eficaz capaz de desenvolver o setor cibernético nos campos industrial e militar (BRASIL, 2008, p. 24). Tal diretriz tem provocado o debate, ainda que em estágio inicial, na sociedade e na comunidade acadêmica, no que se refere ao controle do espaço cibernético, visando sua melhor regulamentação, defesa e segurança.

No âmbito do Ministério da Defesa (MD), a Diretriz Ministerial nº 014/2009, de 09 de novembro de 2009, atribuiu ao Exército Brasileiro (EB) a responsabilidade pela coordenação e integração do Setor Cibernético. Esta tarefa traz impactos imediatos para os Órgãos de Inteligência do EB.

Para a Atividade de Inteligência, a produção de conhecimento para proteção dos sistemas que controlam a funcionalidade das ICN é fundamental para que o agente decisor possa intervir com oportunidade, minimizando ou neutralizando os possíveis danos causados por ações mal intencionadas. A correta aplicação dos preceitos de segurança orgânica também contribuirá para que os riscos sejam mitigados. Para tanto, é fundamental ter seus recursos humanos preparados para o ambiente cibernético, inclusive os da área de inteligência, alocando-os em uma estrutura organizacional eficiente e prática. Esta estrutura deve possuir a capacidade de, permanentemente, acompanhar a evolução das formas de ataques e cooptação de pessoas a fim de impedir intrusões maliciosas nos sistemas informatizados das ICN.

O presente artigo busca investigar a seguinte indagação: a atual estrutura organizacional do Sistema Brasileiro de Inteligência (SISBIN) permite uma eficiente proteção das Infraestruturas Críticas Nacionais, particularmente do setor de energia elétrica, contra ataques cibernéticos?

2 A INTELIGÊNCIA E A GUERRA CIBERNÉTICA

O Gabinete de Segurança Institucional da Presidência da República (GSI-PR) e a Agência Brasileira de Inteligência (ABIN), como órgão central do Sistema Brasileiro de Inteligência (SISBIN), tem como uma de suas missões, monitorar o funcionamento seguro das ICN e desenvolver uma mentalidade de segurança nessas corporações, abrangendo também a segurança cibernética (BRASIL, 2012c).

O GSI-PR é um órgão essencial da Presidência e presta assistência imediata e constante ao Chefe de Estado. Entre outras atribuições, o GSI-PR tem competência para prevenir e gerenciar crises em caso de ameaça à estabilidade institucional. Além disso, possui o status de ministério e assessora a Presidência nos assuntos militares e de segurança. Coordena, ainda, as atividades de Inteligência de Estado e de Segurança da Informação (BRASIL, 2012i).

O GSI-PR não possui ascendência sobre os demais ministérios e órgãos governamentais. Desta forma, para obter maior resultado em suas decisões atinentes à Segurança das ICN e na Segurança Cibernética, o Gabinete utiliza-se da Câmara de Relações Exteriores e Defesa Nacional (CREDEN) e do Conselho

de Defesa Nacional (CDN), que possuem poderes para intervir na segurança das ICN.

O Conselho de Defesa Nacional (CDN) é presidido diretamente pela Presidenta da República e entre suas atribuições está a de "propor os critérios e condições de utilização das áreas indispensáveis à segurança do território nacional" o que lhe garante o poder de regular, discutir e propor assuntos relativos às ICN (BRASIL, 2012e). A Medida Provisória nº 2216-37, de 2001, que modifica a Lei nº 8.183 de 11 de Abril de 1991, atribuiu ao Ministro Chefe do GSI-PR a missão de secretário-executivo do CDN, cabendo a ele a execução das atividades permanentes necessárias ao exercício da competência do CDN. Além disso, concedeu poder ao GSI-PR para instituir grupos e comissões especiais, integrados por representantes de órgãos e entidades, pertencentes ou não à Administração Pública, com o fim de tratar de problemas específicos, afetos ao Conselho de Defesa Nacional. Por meio desse dispositivo legal, o GSI-PR adquiriu poderes para formar Grupos de Trabalho para o estudo da segurança das ICN (BRASIL, 2012f).

A CREDEN foi criada por meio do Decreto Presidencial nº 4801, de 6 de agosto de 2003, com a finalidade de formular políticas públicas e diretrizes de matérias relacionadas com a área das relações exteriores e defesa nacional do Governo Federal ou sempre que se fizer necessária a participação de mais de um ministério. O Ministro-Chefe do GSI-PR é o presidente da CREDEN e convoca os demais integrantes, dentre eles diversos Ministros de Estado de áreas afins. Entre os assuntos sobre os quais tem acompanhamento destacam-se: cooperação internacional em assuntos de segurança e defesa, integração fronteiriça, operações de paz, narcotráfico e outros delitos de configuração internacional, atividade de Inteligência, segurança para as infraestruturas críticas (incluindo serviços segurança da informação, definida no art. 2º, inciso II, do Decreto nº 3.505, de 13 de junho de 2000) e segurança cibernética (BRASIL, 2012d).

Devido às suas atribuições muitas das legislações (portarias, decretos, e outros) que regulamentam a Proteção das ICN e a Segurança Cibernética são oriundas da CREDEN e do CDN, conferindo um maior peso institucional aos dispositivos.

Subordinados ao GSI-PR, estão a Secretaria de Acompanhamento e Estudos Institucionais (SAEI), o Departamento de Segurança da Informação e Comunicações (DSIC) e a Agência Brasileira de Inteligência (ABIN).

Entre suas diversas atribuições, a SAEI se destaca por monitorar e coordenar a atividade de segurança de infraestruturas críticas. Além disso, coordena e supervisiona a realização de estudos relacionados com a prevenção da ocorrência e articulação do gerenciamento de crises. Em outra vertente, essa Secretaria realiza estudos estratégicos, especialmente sobre temas relacionados com a segurança institucional.

Na área de segurança em ICN, a SAEI coordena as reuniões dos Grupos de Trabalho (GT) de Segurança de ICN. Estes grupos formaram-se a partir de 2007, com a resolução nº 2 da CREDEN de 24 de Outubro, a qual prevê, em seu art 2º, a criação dos Grupos Técnicos de Segurança das Infraestruturas Críticas (GTSIC), com a finalidade de propor medidas relacionadas com a segurança das ICN (DEMETERCO, 2012).

O mesmo autor destaca que o propósito dos GTSIC é fundamentalmente sistematizar os estudos. O objetivo é levantar as vulnerabilidades e as ameaças às ICN, assim como identificar suas interdependências com outras estruturas semelhantes, propondo, por fim, um método de gerenciamento de risco das mesmas. Este estudo conduzirá a um sistema de informações que conterá dados atualizados das ICN para apoio à decisão. As reuniões são periódicas e mensais a fim de dar continuidade aos trabalhos dos mais de cem funcionários das diversas agências e ministérios e entidades que integram os grupos (idem, 2011).

O DSIC é um órgão do GSI-PR, bastante atuante na Administração Pública Federal (APF) e que conduz

diversos seminários, palestras, cursos, buscando difundir a mentalidade de segurança em TI. Dentre suas atribuições, previstas no art. 6º do Decreto nº 7.411, de 29 de dezembro de 2010 (BRASIL, 2012i), cabe destacar aquelas que mais se relacionam com o escopo do presente trabalho, a saber:

- planejar e coordenar a execução das atividades de segurança cibernética e de segurança da informação e comunicações na administração pública federal;

- definir requisitos metodológicos para implementação da segurança cibernética e da segurança da informação e comunicações pelos órgãos e entidades da administração pública federal; e

- estudar legislações correlatas e implementar as propostas sobre matérias relacionadas à segurança cibernética e à segurança da informação e comunicações.

Subordinada diretamente ao Ministro-Chefe do GSI-PR, a ABIN é um órgão de Estado e foi instituída pela lei nº 9.883, de 7 de dezembro de 1999. Ela tem como missão principal assessorar o Presidente da República por meio da produção de conhecimentos estratégicos que apontem oportunidades, antagonismos e ameaças aos interesses da nação.

O Decreto Presidencial nº 3505, de 13 de Junho de 2000, em seu art. 5º destaca que compete à ABIN, por intermédio do seu Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (CPESC), apoiar o CDN nos assuntos de caráter científico tecnológicos. Este apoio é voltado para os assuntos de Segurança em TI, nos quais, eventualmente, se inserem os sistemas de controle das ICN (BRASIL, 2012b). Ressalte-se que, nas atribuições da ABIN, não existe dispositivo específico determinando que a mesma realize o Gerenciamento de Risco das ICN no país.

2.1 A GUERRA CIBERNÉTICA

Antes de apresentar os conceitos diretamente associados à Guerra Cibernética, faz-se necessário realizar uma distinção semântica entre segurança, proteção e defesa. O senso comum indica que, isoladamente, o termo "proteção" remete a uma idéia de prevenção, um estado anterior a uma ruptura do *status quo*. Ferreira (1999), em seu conceituado dicionário, define "proteção" como sendo um estado atual, que perdura durante um espaço de tempo ou ainda "cuidado que se toma em favor de" alguém ou algo. Já o termo "segurança" é definido, pelo mesmo autor, como sendo o estado de alguém que se acha seguro. Prossegue ainda conceituando "defesa" como sendo "a resistência a um ataque", indicando claramente uma ação.

O Decreto Presidencial nº 3.505, de 13 de Junho de 2000, aborda a Segurança da Informação sob o seguinte prisma:

> *Art. 2º Para efeitos da Política de Segurança da Informação, ficam estabelecidas as seguintes conceituações:*
> *[...]*
>
> *II - Segurança da Informação: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento (BRASIL, 2012b).*

Oliveira (2012) procurou fornecer seu entendimento acerca do significado do termo cibernético. Segundo ele atualmente, o termo "cibernética" é utilizado procurando estabelecer as relações entre o homem e a máquina e seus efeitos nas diversas atividades humanas. Sua origem vem do termo grego *kybernetike*, que significa condutor, governador, aquele que tem o leme ou o timão. Recebendo um tratamento mais científico no século XX, passou a caracterizar o estudo do controle e da comunicação dos seres vivos e das máquinas, sob o enfoque da transmissão da informação nesses ambientes.

De acordo com o Ministério da Defesa, durante o I Seminário de Defesa Cibernética, espaço cibernético é o espaço virtual composto por dispositivos computacionais conectados em rede ou não, no qual as informações trafegam, são processadas e eventualmente armazenadas (BRASIL, 2010).

Para efeito deste estudo, o espaço cibernético será considerado como sendo o ambiente delimitado pela conexão de computadores via sistema de redes, físicas ou não, onde a informação trafega a velocidades quase instantâneas e, como consequência, as pessoas, ora denominadas usuários, podem se comunicar de diversas maneiras: via mensagens eletrônicas, grupos de discussão, realização de vídeo-conferências, transmissão de dados, e outros (CANONGIA e MANDARINO JR, 2009. p. 25).

De acordo com o Livro Verde de Defesa Cibernética, a atuação da Segurança Cibernética poderá compreender aspectos e atitudes, tanto de prevenção, quanto de repressão. De fato, a segurança cibernética remonta à proteção dos ativos de informação estratégicos, principalmente aqueles relacionados com o controle do funcionamento das ICN. Por esta característica, abrange o controle de sistemas privados e públicos, o que confere à relação entre as partes envolvidas, um caráter jurídico muito mais complexo (BRASIL, 2010).

Com isso, pode-se afirmar que segurança cibernética engloba o conjunto de normas que visam a proteger, com ações preventivas, o ambiente eletrônico no qual trafegam as informações. Vale destacar que, para esta proteção virtual obter sucesso, é imprescindível uma eficiente implementação de medidas de segurança orgânica na corporação pública ou privada que administra a transmissão dos dados. Estas medidas devem ser alvo de constantes reavaliações, para que o gestor possa, eventualmente, corrigir rumos ou reforçar as ações preventivas mais eficazes.

Nesse sentido, a Segurança Cibernética vem se caracterizando cada vez mais como uma função estratégica de Estado, e essencial à manutenção e preservação das infraestruturas críticas de um país, tais como Energia, Transporte, Telecomunicações, Águas, Finanças, Informação, dentre outras.

Para a expressão Defesa Cibernética, entende-se que a mesma compreenderá ações operacionais de combates ofensivos. Carvalho (2011b, p. 18) ensina que é o conjunto de ações, fundamentada em um planejamento tipicamente militar, executadas no todo ou em parte no ambiente cibernético, com a finalidade de: proteger os sistemas de informação, fornecer dados para Inteligência e causar prejuízos aos sistemas do oponente. Para as Forças Armadas, estas ações, que envolvem o preparo e o emprego de grupos constituídos nas ações ofensivas, defensivas e exploratórias em ambiente cibernético, caracterizam a Guerra Cibernética. Este conceito difere de Segurança Cibernética que é voltada para ações preventivas e medidas de segurança orgânica (CARVALHO, 2011).

Mandarino Jr (2010) complementa esta assertiva, afirmando que a lógica da Guerra Cibernética está em atacar as informações do oponente, em qualquer setor que faça uso de meios informatizados. Ou seja, poderia ser composta de uma simples desfiguração de *site*, um bloqueio de serviços eletrônicos de bancos ou até um comprometimento do funcionamento de uma ICN.

Todas estas definições ligadas à área cibernética se traduzem em uma nova e desafiadora fonte de dados, ao mesmo tempo em que é um meio de busca para a Atividade de Inteligência:

> *A atividade de inteligência exerce papel fundamental nos ambientes de Segurança, Defesa e Guerra Cibernética. Ela é essencial na busca de informações, empregando todas as fontes disponíveis, para identificar e prevenir ameaças cibernéticas e proporcionar respostas adequadas, com oportunidade.*
> *Além disso, os profissionais que atuam no Setor Cibernético devem desenvolver atitude arraigada de contrainteligência, a fim de proteger o conhecimento e as informações inerentes às suas atividades (OLIVEIRA, 2011. p. 112).*

Visualizando atender a esta situação evolutiva, a END de 2008 assinalou que um dos setores de importância estratégica para o Estado é o cibernético, tendo como prioridade a capacitação de recursos humanos e o desenvolvimento de tecnologias da informação para as Forças Armadas atuarem em rede. Partindo dessa premissa, definiu que o Ministério da Defesa (MD) deve planejar para que o Sistema de Defesa Nacional disponha

de meios que permitam a segurança das infraestruturas críticas (BRASIL, 2008).

As Forças Armadas, por estarem voltadas para a Guerra Cibernética, estão inseridas somente nos níveis operacionais e táticos daquele setor e, a priori, não estão sendo cogitadas para atuarem na Segurança Cibernética, a qual estaria restrita ao nível político (a cargo do GSI-PR). Entretanto, é difícil acreditar que, na prática, a Segurança permaneça restrita somente ao nível político, pois ela permeia os níveis estratégicos e operacionais, posto que não há Defesa e Guerra Cibernéticas eficientes se não houver previamente a execução de uma adequada política na área de Segurança Cibernética. Desta forma, o Ministério da Defesa e as Forças Armadas também deveriam participar da Segurança Cibernética, além dos papéis de Defesa e Guerra. Caso as ações das Forças Armadas se restrinjam ao contexto de Guerra Cibernética, a tendência natural é que elas venham a se afastar das ações preventivas voltadas para Segurança Cibernética.

No âmbito da Defesa, a Diretriz Ministerial nº 14/2009, de 9 de novembro de 2009, do MD, definiu que caberá ao Exército Brasileiro (EB) a gestão e o desenvolvimento do setor cibernético no âmbito do Ministério da Defesa. Com isto, o EB terá a atribuição que definir sua abrangência e propor ações para integrar o setor nas três Forças (CARVALHO, 2011. p.11).

Neste escopo, o Centro de Defesa Cibernética do Exército (CDCiber) foi criado pela Portaria do Comandante do Exército nº 666, de 4 de Agosto de 2010. Suas principais atribuições são: coordenar as atividades do setor cibernético no Exército e promover ações que atendam ao preconizado na Estratégia Nacional de Defesa, com ênfase na atuação em rede. Atualmente, o CDCiber tem o foco de suas ações voltado para proteger inicialmente as estruturas de informática do Exército, desenvolver pesquisas no setor, fomentar a capacitação humana, gerenciar a aquisição de materiais específicos e desenvolver uma doutrina de emprego, em consonância com a END.

No futuro, após consolidado como um setor dentro do Exército, há uma possibilidade de evolução do CDCiber para a esfera do Ministério da Defesa. Sobre essa assertiva, o atual Chefe do CDCiber se pronunciou, em entrevista à imprensa escrita:

> *É, este é o Centro de Defesa Cibernética, por enquanto, do Exército. Se no futuro o Ministério da Defesa decidir que vamos exercer também o papel de Centro de Defesa Cibernética das Forças Armadas, é perfeitamente viável e até consta das diretrizes do Ministério da Defesa que tenhamos, nesse centro, militares da Marinha e da Força Aérea.*
>
> *[...]*
>
> *A infraestrutura de telemática é uma coisa em que hoje as empresas estão totalmente envolvidas. Imagina-se que algo semelhante deva ocorrer no futuro, em que teríamos militares das três forças trabalhando em conjunto, e serviços prestados por empresas habilitadas. (SANTOS, apud SÁ, 2012).*

Segundo Mandarino (2010), em reunião da CREDEN, em 2008, o Diretor do DSIC apresentou a complexidade e a dificuldade de cooperação entre os órgãos da APF no quesito segurança cibernética. A proposta, feita e aprovada, foi a de que, a segurança deve ser coordenada pelo GSI-PR (por meio do DSIC), haja vista ser um órgão essencial da Presidência da República. Mas essa coordenação envolve inúmeros atores, desde ministérios até agências reguladoras, passando inclusive por empresas de capital misto.

3 O SETOR DE ENERGIA ELÉTRICA E A SEGURANÇA CIBERNÉTICA

A partir dos anos 90, o setor elétrico brasileiro passou por grandes transformações, deixando de ser centrado no monopólio estatal para adotar um novo arranjo de mercado, com a participação de múltiplos agentes e investimentos compartilhados com o capital privado (COUTINHO, 2007). Esta reestruturação permitiu descentralizar o antigo padrão, com o objetivo de que o setor privado se incumbisse do financiamento do segmento elétrico, enquanto o Estado ficaria com a função de regulação. Como consequência desta nova forma de atuar, a concorrência entre as empresas se encarregaria de transferir aos consumidores os ganhos de eficiência.

Em 1996, foi criada a Agência Nacional de Energia Elétrica (Aneel), que tinha como finalidade regular e fiscalizar a produção, transmissão e comercialização de energia elétrica, garantindo um ambiente equilibrado, com companhias obtendo resultados e consumidores satisfeitos (OLIVEIRA, 2012).

A partir do governo do Presidente Luís Inácio Lula da Silva, instituiu-se o chamado novo modelo do setor elétrico que mesclava o intervencionismo público com certo nível de concorrência. Em 2004, com esse padrão, o Estado recebeu novamente a responsabilidade de planejamento do setor. Os principais objetivos eram: promover a concorrência tarifária, garantir a segurança no longo prazo para fornecimento de energia e promover a inclusão social. Além disso, o segmento elétrico passou a ser coordenado por diversos atores institucionais, responsáveis por planejar, monitorar, avaliar, acompanhar e sugerir as ações para seu eficiente funcionamento (Ibidem).

Com o novo quadro, o Governo centralizou o poder de fixar as políticas, o planejamento e o monitoramento do sistema. A Aneel manteve suas funções de implementar as diretrizes governamentais e de fiscalizar os agentes executores. Estes, por sua vez, continuaram participando das entidades responsáveis pela comercialização e operação do sistema, sem, contudo, exercerem o mesmo grau de controle previsto no antigo padrão.

Neste contexto, o que se verifica hoje é a exploração dos serviços de energia elétrica por terceiros, a segmentação das atividades (geração, transmissão, distribuição e comercialização), e a regulamentação e fiscalização do sistema por agências reguladoras.

A estrutura administrativa que compõe o sistema é a descrita na figura 1, a qual identifica as principais instituições do setor: o Conselho Nacional de Política Energética, o Ministério de Minas e Energia, a Empresa de Pesquisa Energética (criada pela Lei nº 10.847), a Agência Nacional de Energia Elétrica, a Câmara de Comercialização de Energia Elétrica (responsável pela viabilização dos mercados livre e regulado), o Operador Nacional do Sistema (agora com maior controle pelo Governo) e o Comitê de Monitoramento do Setor Elétrico.

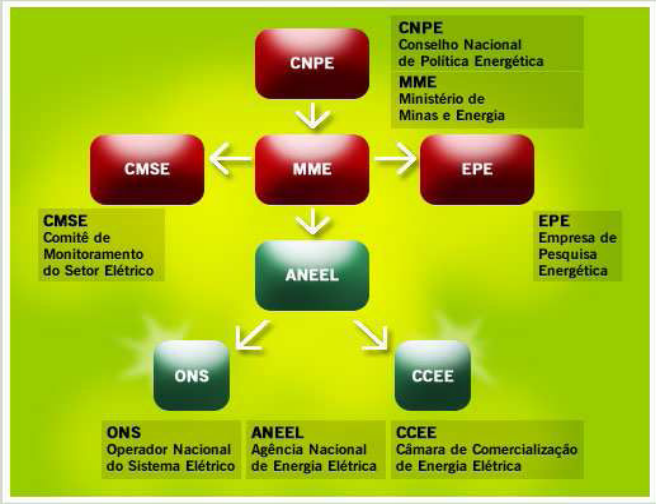

Fig 1 - Estrutura Administrativa do Setor de Energia Elétrica.
Fonte: ONS

A Aneel permanece como o órgão regulador, responsável pela normatização das políticas e diretrizes estabelecidas e a fiscalização dos serviços prestados. O Sistema Interligado Nacional (SIN) e os sistemas isolados formam o sistema nacional de energia elétrica e é composto pelas empresas geradoras e transmissoras, sob a regulamentação da Aneel. Ele é altamente interconectado e dinâmico, possuindo cerca de novecentas linhas que perfazem um total de aproximadamente oitenta e nove mil quilômetros. O Operador Nacional do Sistema Elétrico (ONS) é uma empresa de capital privado sem fins lucrativos, responsável pela coordenação e a supervisão da operação centralizada de geração e transmissão do sistema interligado (OLIVEIRA, 2012).

O Centro Nacional de Operação do Sistema (CNOS) e os Centros Regionais de Operação do Sistema (CROS) abrigam os sistemas informatizados de controle e gerenciamento de energia das empresas concessionárias e do Operador Nacional do Sistema. Estes Centros monitoram os dados obtidos pelas Unidades Terminais Remotas (UTR) e pelos Sistemas de Supervisão e Controle Local (SSCL) para garantir que o sistema está

funcionando adequadamente (Figura 2). Os Centros de Operação também despacham mensagens de controle para as Unidades Geradoras e Subestações para regular o fluxo de potência que poderá ser repassado.

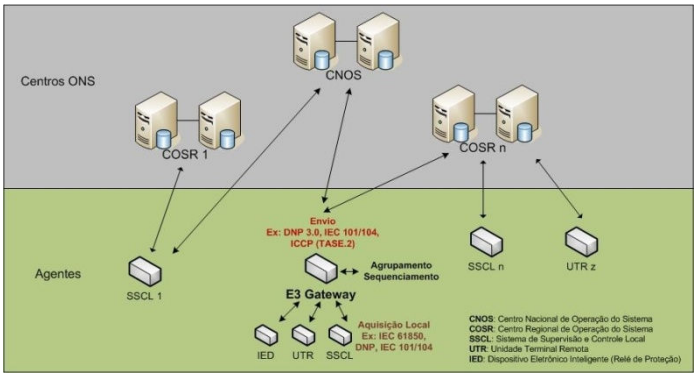

Figura 2 - Representação da Distribuição de Energia.
Fonte: Empresa Elipse.

Os Sistemas Computacionais de Controle permitem aos operadores a regulação do fluxo de potência (geração, transmissão e distribuição) e são chamados de Sistemas de Gerenciamento de Energia Elétrica (em inglês, EPMS ou simplesmente EMS). Já os sistemas de controle utilizados para monitoramento da segurança, confiabilidade e proteção do sistema elétrico são chamados de Sistemas de Controle Supervisório e Aquisição de Dados (em inglês, SCADA – "Supervisory Control and Data Acquisition") (COUTINHO, 2007).

Do exposto, percebe-se que a organização do setor elétrico no Brasil é composta por diversos atores de caráter público e privado que gerenciam a geração, transmissão e distribuição de energia.

3.1 A ENGENHARIA E AS VULNERABILIDADES NOS SISTEMAS AUTOMATIZADOS DE CONTROLE DA ENERGIA ELÉTRICA

Por volta de 1940, o controle dos sistemas das usinas hidrelétricas era realizado por meio da lógica de relés, que enviavam sinais para mesas de controle com chaves e luzes de advertência. O operador era o maior responsável por interpretar os sinais e luzes e adotar as medidas corretas em um menor prazo de tempo possível. Entretanto, para não sobrecarregar a capacidade do operador, muitos sinais eram deixados de fora do painel.

Para suprir as deficiências existentes, começaram a surgir os sistemas automatizados que supervisionavam, controlavam e adquiriam dados dos relés do sistema. Este mecanismo deu origem ao Sistema SCADA, composto inicialmente por uma estação de monitoramento central de grande porte e por unidades remotas de controle (UTR – Unidade Terminal Remota). Apesar do salto qualitativo no controle operacional, o sistema ainda apresentava limitações quanto à quantidade de tarefas de controle a executar e o número de interfaces gráficas na tela do computador. (ERKILLA e SCHIMITT, 2002).

Com o surgimento dos controladores lógicos programáveis (PCL – Programable Control Logic), os relés antigos foram substituídos. Posteriormente, o avanço dos microprocessadores permitiu a criação dos sistemas de controle distribuídos (DCS – Distributed Control System), o que levou o controle inteligente até as unidades de campo com redundância dos controladores e das telas gráficas que se apresentam para os operadores. Como isso, o operador passou a ter um controle e supervisão da usina de forma centralizada e organizada (ibidem).

Atualmente, o sistema SCADA moderno é o responsável pela interface com o operador por meio de telas e gráficos em tempo real. Além disso, executa funções lógicas, de controle e arquiva dados históricos, permitindo a conexão em redes de processo e a configuração de redes lógicas com o propósito de supervisão do sistema (ibidem).

Por meio da evolução dos sistemas de controle das usinas percebe-se que a automação por meio de *softwares* e terminais computacionais é irreversível, pois confere economia, confiabilidade operacional e otimização do gerenciamento. Mas isso não significa que tais sistemas sejam imunes a ataques cibernéticos. De fato, a introdução maciça de softwares baseados na comunicação em redes internas (*intranet*), externas (*internet*) e sem fio (*wireless*) tem tornado os sistemas de controle de processos das ICN do setor elétrico ainda

mais vulneráveis a ataques cibernéticos. Esta tendência traz consigo os riscos de ataques perpetrados por *hackers* e ciberterroristas.

Dessa forma, invasões cibernéticas podem produzir efeitos desastrosos, caso os dispositivos eletrônicos de controle sejam manipulados de forma proposital e direcionada. A fim de proteger o segmento de energia elétrica contra esse tipo de ameaça, faz-se necessário identificar suas vulnerabilidades. Ralph Langner, o homem que primeiro decodificou o vírus *Stuxnet*, que imobilizou parte das centrífugas de enriquecimento de urânio no Irã, colocou, em entrevista, seu ponto de vista acerca desta nova modalidade de arma cibernética. Segundo ele, este vírus pode ser copiado facilmente e poderia infectar qualquer sistema de usinas controladas de forma automatizada em tempo real (LANGNER, apud MILLS, 2012).

Em princípio, um ataque cibernético, conduzido por outra nação, provavelmente estará contido numa fase que antecederá uma guerra (a escalada da crise). Mas, para grupos terroristas, grupos ativistas, em luta por suas convicções, ou mesmo para indivíduos sem motivações políticas, a invasão de um sistema de ICN do setor elétrico ocorreria sem a necessidade de o cenário se apresentar como sendo de uma guerra. Portanto, ataques cibernéticos de vulto podem acontecer mesmo em tempo de paz, inclusive por ocasião dos grandes eventos mundiais - como forma de protesto ou desafio - tais como aqueles previstos para o Brasil sediar nos próximos anos.

Infere-se que a intensa automação dos sistemas que controlam as ICN pode vir a proporcionar uma eficácia operacional inversamente proporcional à segurança contra invasões de rede.

4 RESULTADOS ALCANÇADOS

A fim de instrumentalizar os dados colhidos durante a consulta bibliográfica foram realizadas pesquisas quantitativas e qualitativas durante os meses de abril a junho de 2012, por meio da remessa de questionários de respostas objetivas e do contato pessoal, no caso das entrevistas.

No tocante à pesquisa quantitativa, com a finalidade de selecionar a população a ser observada, foram ouvidos grupos formados por militares integrantes do Sistema de Inteligência do Exército (SIEx). Com isso formou-se um total de 49 (quarenta e nove) indivíduos direcionados para a pesquisa quantitativa, os quais responderam um questionário de 13 (treze) perguntas.

As respostas apontaram que 85,71% (oitenta e cinco vírgula setenta e um por cento) dos entrevistados acham muito importante possuírem pessoal habilitado em defesa/segurança cibernética nos Órgãos de Inteligência. Há que se destacar ainda que, 12,24% (doze vírgula vinte e quatro por cento) responderam ter certa relevância a presença de militares com esta habilidade. Ou seja, considerando as respostas com inclinação favorável, obtém-se mais de 97% (noventa e sete por cento) de respostas indicando a necessidade de que haja militares com essa habilidade nos Órgãos de Inteligência.

Foi questionado, também, acerca da importância de o SIEx estar permanentemente acompanhando e contribuindo para a evolução da mentalidade de segurança cibernética das ICN. A esmagadora maioria (mais de 97%) respondeu que este acompanhamento prévio seria imprescindível ou importante numa situação de eventual crise.

A última pergunta do questionário voltou-se para relacionar a capilaridade do EB com a possibilidade de que o SIEx efetivamente possa colaborar com a segurança cibernética nas empresas que operam as ICN do setor de energia elétrica. Cerca de 83% (oitenta e três por cento) dos entrevistados achou positiva essa possibilidade de apoio. Destes % (cinquenta e um por cento) declararam que esta deveria ser uma tarefa em apoio à ABIN, e 22,45% (vinte e dois vírgula quarenta e cinco por cento) ressaltaram que esta missão já faz parte das atribuições do SIEx e, portanto, seria perfeitamente factível.

No que tange à pesquisa qualitativa, as principais considerações dos entrevistados serão destacadas a seguir:

a) Oficial da Seção de Ensino de Guerra Cibernética do Centro Integrado de Guerra Eletrônica (CIGE): segundo ele, seria possível que o EB, por meio do SIEx, acompanhasse a segurança em TI das empresas públicas e privadas do setor de energia elétrica. Entretanto, este tipo de relacionamento teria de ser baseado em um caráter de cooperação, sem jamais deixar transparecer uma atitude de auditoria ou fiscalização, pois encontraria significativa resistência e não teria respaldo em lei. Completou informando que, atualmente, somente o TCU efetivamente realiza auditorias na área de TI nas empresas da Administração Pública Federal (APF), haja vista a natureza eminentemente fiscalizatória daquele tribunal. Ao que sabe, estas auditorias são focadas na avaliação da aplicação dos recursos públicos na gestão de TI do órgão ou empresa e não visa a especificamente verificar a segurança cibernética da instituição (FONTENELE, 2012).

b) Chefe de Gabinete do Ministério das Minas e Energia: de acordo com o entrevistado, os procedimentos de segurança das empresas e energia elétrica são regulados pela ANEEL. Estas empresas devem manter os padrões estabelecidos, sob pena de terem suas concessões canceladas. Entretanto, a segurança em TI é efetivada pelas próprias empresas e pelas próprias usinas geradoras. O entrevistado ainda ressaltou que atualmente o Sistema Integrado Nacional (SIN) apresenta destacada redundância nas linhas principais. Desta maneira, se uma linha sofrer interrupção abrupta de qualquer ordem, a carga é transferida para outras linhas e a chance de ocorrer um colapso é mínima (MENDES, 2012).

c) Chefe da Seção de Doutrina da EsIMEx: quanto à interação entre o setor cibernético e a Inteligência, o entrevistado citou que ainda existem discussões e estudos a serem realizados nesta área. A proposta de criação do Batalhão de Inteligência, com uma subunidade de guerra cibernética, poderia ser uma solução. Outra opção seria criar um destacamento de Guerra Cibernética, oriundo do CDCiber, com mobilidade tal que permitisse sua atuação em todo o território nacional. Para ele, a possibilidade de o SIEx participar da segurança cibernética das ICN não seria nada mais do que a segurança de ponto sensível que o Exército Brasileiro sempre fez, agregando o componente cibernético. Para ele o Programa PROTEGER será uma excelente ferramenta para facilitar o relacionamento com as empresas que operam as ICN. Pelo Programa, as atuais Áreas de Segurança Integrada serão transformadas em Áreas de Proteção Integrada, visando proteger a sociedade e as ICN (TEIXEIRA, 2012).

d) Diretor-Gerente do Operador Nacional do Sistema (ONS): segundo ele, a missão principal do ONS é o controle do equilíbrio do Sistema Elétrico Nacional, garantindo a confiabilidade, a segurança e a continuidade do negócio. Na prática, esta entidade não possui ativos do sistema, somente recebe as informações dos agentes e emite os comandos para equilibrar a geração e a distribuição das cargas energéticas. Quanto à interação do ONS com o DSIC ou o GSI, ele ressaltou que possui mais contato com a SAEI, nos Grupos de Trabalho de Segurança das ICN. O ONS participa das reuniões sobre as ICN, mas, nelas, não é muito abordado o tema de segurança em TI ou cibernética, o que pode ser uma falha, provavelmente devido à falta de unificação nos órgãos que gerenciam a segurança das ICN (FILHO, 2012).

e) Oficial de Inteligência da ABIN: a proteção às ICN é um dos temas que a ABIN acompanha, particularmente na composição do mosaico de temas semanal apresentado à Presidenta da República. Somente a partir de 2008, a ABIN iniciou o gerenciamento de risco de ICN, e apoiando-se em cooperação voluntária entre as partes envolvidas. Hoje a ABIN possui uma metodologia própria de análise de risco, chamada ARENA. Entretanto, verifica-se que pouquíssimas estruturas foram analisadas pelo órgão até a presente data (UHE Tucuruí, UHE Sobradinho e instalações da

ELETRONORTE). Quanto à existência de uma seção específica na ABIN voltada para a segurança cibernética em ICN, ele relatou que ainda não existe. Acrescentou que, quando há incidentes nas ICN, a ABIN é chamada a apoiar. Mas estas situações são esporádicas e não há um controle, por parte da Agência, de tentativas de invasão aos sistemas de TI. Quando ocorre um problema, o CPESC (Centro de Pesquisa em Segurança das Comunicações) da ABIN presta o apoio técnico, além de trabalhar sempre em conjunto com o DSIC do GSI-PR. Ao ser questionado se o Exército Brasileiro poderia contribuir para a segurança cibernética das ICN, o Oficial de Inteligência da ABIN foi favorável, principalmente se o EB atuar junto às empresas públicas. Mas ressaltou que, antes de tudo, devem haver diretrizes ou normas sobre os limites de atuação. Esta regulamentação teria que apontar o que as Organizações Militares (OM) precisariam acompanhar e qual o Repertório de Conhecimentos Necessários (RCN). O entrevistado destacou, por último, que o ritmo de trabalho dos Grupos de Trabalho das ICN é lento e complexo pois envolve muitos atores com interesses diversos. Segundo ele, a frequência das reuniões do GT no último ano diminuiu, prejudicando a progressividade dos levantamentos (SILVA, 2012).

f) Oficial do CDCiber: o entrevistado foi questionado se as estruturas atuais do GSI-PR, por meio do DSIC, bem como da ABIN seriam suficientes para acompanhar a evolução da proteção cibernética sistemas de informação das empresas que controlam as ICN do setor energético brasileiro. Ele posicionou-se afirmando ser difícil que alguma entidade tenha estrutura suficiente, no curto prazo. O GSI-PR, via DSIC, está se apoiando no CDCiber, em forma de parceria muito positiva. Ao ser perguntado se o entrevistado acreditava que o SIEx poderia participar da análise de risco e do acompanhamento das empresas do setor de energia elétrica, no que tange à segurança cibernética, o Oficial respondeu que essa possibilidade estaria inserida em um contexto de disponibilidade de material e de capacitação de pessoal. Segundo ele, o ideal seria disseminar células estruturais com pessoal e material vocacionados para defesa cibernética pelos Comando Militares de Área. Mas isso em um futuro no médio prazo, pois o primeiro passo é consolidar o CDCiber (CARNEIRO, 2012).

g) Assessora Técnica do DSIC: a entrevistada explicou que o GSI-PR é um órgão no nível ministerial e com caráter estratégico. Assim sendo, ele trabalha com visão prospectiva das ICN e portanto, a atual gestão do GSI passou a adotar a terminologia de Estrutura Estratégica que englobaria não só as ICN já existentes, mas também as que estão em construção e aquelas ainda em fase de projeto, ou seja, um horizonte futuro. Dentro da estrutura do GSI-PR, a SAEI é o órgão vocacionado para a segurança das ICN. Nesse sentido, organizou-se Grupos de Trabalho (GT) para realizar o levantamento das ICN em cinco setores (água, transportes, energia, comunicações e finanças). Segurança da Informação e a Segurança Cibernética agem em todos estes setores. Os GT basicamente trabalham no levantamento das ICN, verificando quais realmente são estratégicas. Eles devem realizar a análise de risco, e elaborar o plano de proteção das ICN. Um dos grupos é responsável pela área de Segurança Cibernética e permeia todos os outros. Nesse sentido, este grupo está trabalhando muito com o CDCiber diretamente. De fato o CDCiber foi escolhido como ponto focal para acompanhar o perfil das forças externas cibernéticas, para construção de cenários e para monitorar o espaço cibernético. Há uma expectativa de que ocorra uma evolução rápida do CDCiber para que ele represente o MD com as três Forças. A entrevistada deixou claro que o GSI-PR não tem competência regulamentar para impor ações aos demais órgãos, particularmente os Ministérios. Portanto, não tendo poder fiscalizador, se embasa nos Acórdãos do Tribunal de Contas da União (TCU), muitas vezes usados para calcar as Instruções Normativas do DSIC. Para a entrevistada, o apoio do EB na proteção Cibernética às ICN seria importante para aumentar a capacidade de segurança do setor (CANONGIA, 2012).

h) Assessora da Coordenação-Geral de Cenários Institucionais da SAEI (GSI-PR): a partir de 2006, por determinação presidencial, foram feitos estudos a fim de levantar a localização e a importância das ICN, além de realizar uma análise de risco e descrever a interdependência entre elas. Para tanto, foram articulados Grupos de Trabalho (GT) em cada setor (Transporte, Telecomunicações, Energia, Água e Finanças). Posteriormente, os GT foram ampliados acrescentando mais quatro setores (Cibernético, Nuclear, Espacial e Ativos de Informática), formato que permanece até hoje. O setor de energia envolve muitos atores e diversas vertentes e por isso foi subdividido em 12 (doze) subgrupos. Um deles é o grupo da energia elétrica. Segundo a entrevistada, foram realizadas muitas reuniões, que às vezes são altamente produtivas, mas em outras ocasiões se avança muito pouco. Para ela, não haveria ganhos substanciais na participação do EB na Segurança Cibernética. Ela acrescentou que a Política Nacional de Segurança das ICN, apesar de ser fundamental para o setor, ainda permanece em estudos (SOUZA, 2012).

i) Auditora da Secretaria de Fiscalização em Tecnologia da Informação (SEFTI) do Tribunal de Contas da União (TCU): primeiramente a entrevistada informou que o TCU realiza a fiscalização da gestão e governança em TI. Segundo ela, o negócio da SEFTI é o controle externo de TI na Administração Pública Federal (APF). A missão é assegurar que a Tecnologia da Informação agregue valor ao negócio da APF em benefício da sociedade. Para ela, a governança envolve políticas, normas e emprego dos recursos previstos em orçamento e capacitação dos recursos humanos. Quanto à Segurança da Informação, a SEFTI/TCU verifica como é o controle, o acesso e a continuidade do negócio. Realiza também auditorias nos sistemas de informação a fim de certificar que os recursos federais estão sendo bem aplicados na gestão de TI do órgão auditado. Com estas atribuições, a SEFTI emite seus relatórios por meio dos Acórdãos, que servem para toda a APF. Isto é positivo para a segurança em TI, pois, com base no Acórdão resultante de auditoria, o TCU pode determinar que a APF adote determinadas medidas que serão elaboradas pelo GSI-PR ou DSIC. Assim, muitas vezes, os Acórdãos do TCU indicam a direção que as Instruções Normativas do DSIC devem seguir. Com isto, a natureza fiscalizadora do TCU consegue imprimir uma reação positiva nos entes auditados, além de atuar em parceira com o DSIC, fornecendo-lhe o respaldo para que a APF cumpra os requisitos necessários a implementar uma segurança cibernética eficaz. Entretanto, os entes privados que controlam parte das ICN do setor elétrico não são objeto de auditoria direta pelo TCU (QUEIROZ, 2012).

j) Oficial-General, Chefe do Escritório de Projetos do Exército: de acordo com o entrevistado, um dos fatores decisivos para a manutenção da ordem social em Operações de Garantia da Lei e da Ordem, Operações na Faixa de Fronteira e Defesa Nacional, está calcado na continuidade do fornecimento dos serviços essenciais para a sociedade. Esses serviços são providos por meio das Infraestruturas Críticas Nacionais e desta reflexão nasceu o Projeto PROTEGER. A força motriz do projeto é articular um sistema integrado para a proteção das ICN. Com isso, um dos objetivos do projeto é oferecer ao Estado a capacidade nominal de antecipação e pronta-resposta para a proteção das ICN e da sociedade. Neste sentido, a capilaridade e presença do Exército Brasileiro, com OM distribuídas em todo o território nacional, aparece, como recurso ímpar ao Estado brasileiro, para dispor de pessoal capacitado a implementar soluções que vão desde a obtenção e gerenciamento das informações, até a pronta resposta às situações de crise. Em situações de crise, a integridade territorial, o bem estar da sociedade e a estabilidade institucional estariam ameaçados, sejam por causas externas ou internas, naturais ou humanas. O incremento da capacidade de proteção das ICN, somado aos sistemas de segurança orgânica e de segurança pública já existentes, contribuirá para mitigar os riscos que possam comprometer a

continuidade da prestação de serviços essenciais em significativas parcelas do território nacional. A concepção do projeto se fundamenta em quatro vetores fundamentais: reconhecimento e diagnóstico, identificação de necessidades, equipamento e instalações e treinamento integrado a outros órgãos. Neste caso, a proposta de preparo e emprego do EB estaria voltada para ações de Garantia da Lei e da Ordem, com as Organizações Militares recebendo Áreas e Subáreas de Proteção Integrada, em uma divisão de responsabilidade equivalente às atuais Áreas de Segurança Integrada. De fato, o grande mérito do Projeto PROTEGER está em realizar a sistematização do processo de proteção das ICN, reduzindo os riscos sobre as ICN, fortalecendo o Estado brasileiro, assegurando o bem-estar da sociedade e elevando a capacidade operacional das Forças Armadas. O desenvolvimento do setor cibernético no EB é distinto do PROTEGER, mas interagem entre si e acontecem de forma paralela (IASBECH, 2012).

Face ao exposto no presente capítulo, pode-se inferir que a ampla maioria dos entrevistados é favorável ao aumento da participação do EB na Segurança Cibernética das ICN, desde que haja uma regulamentação clara.

Verificou-se que a ABIN não possui um setor específico para monitorar as ICN. Do mesmo modo, apesar dessa Agência possuir uma metodologia própria de Análise de Risco (ARENA), a mesma não está sendo aplicada, de forma rotineira, na segurança das ICN.

Cabe destacar que o DSIC e a SAEI, apesar de serem órgãos distintos dentro do GSI-PR, desempenham papel de extrema relevância no gerenciamento da segurança das ICN. Possivelmente, obteriam resultados mais rápidos, caso houvesse um único setor que tratasse do assunto no âmbito do GSI-PR. Por outro lado, o apoio do TCU ao GSI-PR mostrou ser uma ferramenta que concede maior peso às deliberações do GSI-PR, no que tange à segurança cibernética.

O Projeto PROTEGER apresenta-se como uma sistematização da segurança das ICN, o que contribuirá para os trabalhos de Levantamento e Análise de Risco das ICN na SAEI.

5 CONCLUSÃO

A estrutura de Inteligência do SISBIN não mostrou ser eficaz no acompanhamento da proteção das ICN do setor elétrico no Brasil. O próprio controle das ICN está em desenvolvimento, tendo em vista que levantamento de boa parcela das ICN permanece sendo realizado pelos Grupos de Trabalho (GTSIC). A multiplicidade de atores e a falta de um órgão com vocação para centralizar, coordenar e fazer cumprir as normas dificulta o progresso mais rápido dos trabalhos.

O Setor de Segurança Cibernética, capitaneado pelo DSIC, mostrou-se bem estruturado e organizado, conferindo uma grande eficiência na difusão da mentalidade de segurança em TI no âmbito da APF. A dificuldade que o DSIC possui, ao não ter ascendência efetiva sobre os demais atores, vem sendo contornada com o apoio do TCU, que lhe confere respaldo, com caráter impositivo aos agentes do setor de energia elétrica. Esta intervenção do TCU, via SEFTI, provoca uma reação positiva nas empresas e nos órgãos da APF, contribuindo para a melhora na qualidade da segurança dos sistemas informatizados.

Entretanto, ficou latente, durante as entrevistas, que há a necessidade de coordenação entre o DSIC e a SAEI, pois ambos os setores estudam as ICN sob perspectivas diferentes e realizam trabalhos estanques. Uma oportunidade de melhoria seria a ativação de uma estrutura dentro do GSI-PR que congregasse todos os órgãos que tratam da segurança das ICN, seja segurança física, seja segurança cibernética, pois elas não são dissociadas.

Não obstante, há uma necessidade premente de aprovação da Política de Segurança de ICN, para que o Plano Nacional de Segurança de ICN possa ser colocado em prática antes da ocorrência dos grandes eventos mundiais previstos para o País sediar, a partir de 2012.

Os resultados dos questionários quantitativos apontam também para a percepção de que, caso o SIEx possua recursos humanos capacitados e material adequado, poderá apoiar o acompanhamento da proteção às ICN do setor elétrico. Na verdade, a pesquisa bibliográfica e a entrevista com Teixeira (2012) e Fontenele (2012) indicam que esta já é uma atribuição do SIEx e que, somente estará sendo agregado o valor do setor cibernético, como meio de obtenção de dados e como ambiente operacional. Ficou bastante claro, também, que este apoio deverá ser sob forma de cooperação, de parceria, a fim de não ferir suscetibilidades entre as entidades. O amparo legal para este apoio fundamenta-se na própria missão constitucional das Forças Armadas, bem como nas diretrizes traçadas pela Estratégia Nacional de Defesa.

A possibilidade de o setor cibernético de Defesa apoiar a segurança das ICN do setor elétrico, ainda é bastante incipiente, haja vista o estado embrionário o qual se encontra o CDCiber. No entanto, já se vislumbra que, no futuro, o CDCiber poderá tornar-se o Comando de Defesa Cibernética do Ministério da Defesa e a partir daí ter um alcance maior. Saliente-se que, mesmo em estágio de implantação, o CDCiber, em 2012, passou muito bem por seu primeiro teste, no gerenciamento da segurança cibernética da Conferência Mundial "Rio+20", em parceria com órgãos públicos e privados. Verificou-se, na prática, a integração entre setor público militar e civil e órgãos privados direcionados para proteção cibernética, obtendo multiplicidade nos resultados alcançados.

As vulnerabilidades existentes no setor cibernético das ICN do setor elétrico são primordialmente calcadas no tipo de controle automatizado que as empresas utilizam cada vez mais. Para tanto, a segurança dos softwares utilizados e os meios de transmissão dos dados merece atenção especial por parte do Estado, a fim de impedir qualquer tentativa de intrusão nos sistemas e proteger a sociedade.

As análises de risco das ICN do setor elétrico ainda não foram realizadas por falta de coordenação e pela lentidão na execução dos trabalhos dos grupos técnicos formados com esta finalidade. Paralelamente, o não aproveitamento da metodologia ARENA desenvolvida pela ABIN demonstra o pouco sincronismo nas ações integradoras da SAEI com a ABIN e o DSIC.

Após a reflexão conclusiva, as propostas de ações a serem adotadas pelas entidades responsáveis são as seguintes:

- unificar, no âmbito do GSI-PR, em uma Secretaria (ou similar) a coordenação dos trabalhos de segurança das ICN, inclusive a parte de segurança cibernética. Este órgão deveria englobar todos os demais órgãos relacionados com o tema, com estabelecimento de metas, a fim de permitir uma avaliação do ritmo de desenvolvimento dos trabalhos;

- a fim de permitir a maior inserção do setor cibernético de defesa na segurança cibernética das ICN, poderia ser formalizado, oportunamente, um termo de cooperação ou convênio entre o Ministério da Defesa e o Ministério das Minas e Energia, com a concordância das agências reguladoras. Desta maneira, o SIEx e CDCiber teriam um instrumento legal para melhor acompanhar e difundir as boas práticas em segurança de TI para os agentes do setor elétrico;

- no âmbito do Ministério da Defesa, a ação de segurança cibernética deveria ser acrescida para as Forças Armadas, além da ação de Defesa Cibernética já prevista;

- executar exercícios simulados de Guerra Cibernética no âmbito do MD envolvendo Comandos Militares de Área em operações conjuntas. Em um primeiro momento, bastaria inserir o tema cibernético nas operações conjuntas já planejadas; e

- prosseguir na implantação do Projeto PROTEGER, o qual permitirá um avanço significativo na efetiva coordenação da proteção às ICN.

Devido à interdependência estabelecida entre estas infraestruturas críticas, toda a sociedade está exposta às ameaças de segurança. Para proteger as ICN

de ataques cibernéticos, o Estado deve melhor coordenar suas ações para manter os objetivos de segurança para as redes automatizadas de operação.

O Estado necessita adotar medidas, no curto prazo, para acelerar o processo de Proteção das ICN, consolidando o setor cibernético no Ministério da Defesa e capacitando seus recursos humanos. Com o apoio do GSI-PR, particularmente do DSIC, poderá conscientizar os usuários de TI das ICN acerca da mentalidade de segurança a ser incorporada. Entretanto, a unificação de esforços é vital para dirimir eventuais morosidades facilmente encontradas em relações tão complexas quanto as estudadas até aqui.

Por último, é imprescindível a coordenação eficaz da proteção das Infraestruturas Críticas Nacionais para que o país não permaneça vulnerável a atores hostis, cujas motivações sejam suficientes para deflagrarem um ataque cibernético contra redes do setor elétrico, principalmente no momento em grandes eventos mundiais estão sendo realizados no Brasil.

REFERÊNCIAS

BRASIL. Conselho de Defesa Nacional. Secretaria Executiva. **Portaria nº 34, de 5 de Agosto de 2009: Institui Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação, no âmbito do Comitê Gestor de Segurança da Informação – CGSI**. Brasília, 2009. Disponível em <http://www.in.gov.br/imprensa/visualiza/index.jsp?jornal=1&pagina=4&data=06/08/2009>. Acesso em: 2 jun. 2012.

_____. **Constituição da República Federativa do Brasil** 15. ed. Rio de Janeiro: DP&A, 2004. Promulgada em 05 out. 1988. Versão atualizada até as Emendas Complementares 41 e 42 de 2003.

_____. Ministério da Defesa. **Doutrina Militar de Defesa - MD51-M-04,** 2. ed. Brasília**,** 2007.

_____. Ministério da Defesa. **Estratégia Nacional de Defesa** - END**,** Brasília, 2008. 59 p.

_____. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército. **Minuta de Nota de Coordenação Doutrinária ao I Seminário de Defesa Cibernética do Ministério da Defesa.** Brasília, 2010.

_____. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Decreto nº 2.335 de 6 de Outubro de 1997: Constitui a Agência Nacional de Energia Elétrica - ANEEL, autarquia sob regime especial, aprova sua Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e Funções de Confiança e dá outras providências.** Brasília, 1997. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto/d2335.HTM>. Acesso 10 junho 2012a.

_____. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Decreto nº 3.505, de 13 de junho de 2000: Institui a política de segurança da informação nos órgãos e entidades da administração pública federal.** Brasília, 2000. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acesso em 2 junho 2012b.

_____. Presidência da República. Casa Civil. Subchefia para assuntos Jurídicos. **Decreto nº 6540, de 13 set. 2008 – Altera o SISBIN.** Disponível em < https://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Decreto/D6540.htm#art4 > Acesso em 5 maio 2012c.

_____. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Decreto nº 4801, de 6 ago. 2003 - Cria a Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo.** Disponível em < http://www.planalto.gov.br/ccivil_03/decreto/2003/d4801.htm> Acesso em 5 maio 2012d.

_____. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei nº 8.183 de 11 de abril de 1991: Dispõe sobre a organização e o funcionamento do Conselho de Defesa Nacional (CDN)**. Brasília, 1991. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8183.htm>. Acesso 30 maio 2012e.

_____. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Medida Provisória nº 2216-37 de 31 de Agosto de 2001: Altera dispositivos da Lei nº 9.649, de 27 de maio de 1998, que dispõe sobre a organização da Presidência da República e dos Ministérios, e dá outras providências.** Brasília, 2001. Disponível em: < http://www.planalto.gov.br/ccivil_03/mpv/2216-37.htm>. Acesso 3 junho 2012f.

_____. Presidência da República. **Estrutura da Presidência**. Disponível em <http://www2.planalto.gov.br/presidencia/estrutura-da-presidencia>. Acesso em 18 mar 2012g.

_____. Presidência da República. Gabinete de Segurança Institucional. **Estrutura da ABIN**. Disponível em http://www.gsi.gov.br/sobre/estrutura/abin>. Acesso em 18 Mar 2012h.

_____. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Decreto nº 7411, de 29 dez. 2010 –** Dispõe sobre remanejamento de cargos em comissão do Grupo-Direção e Assessoramento Superiores - DAS, aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Gratificações de Exercício em Cargo de Confiança do Gabinete de Segurança Institucional da Presidência da República; altera o Anexo II do Decreto nº 7.063, de 13 de janeiro de 2010, e dá outras providências. Disponível em < http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2010/Decreto/D7411.htm > Acesso em 5 maio 2012i.

_____. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Livro verde: segurança cibernética no Brasil** / Gabinete de Segurança Institucional,

Departamento de Segurança da Informação e Comunicações; Claudia Canongia e Raphael Mandarino Junior (Org.) – Brasília: GSIPR/SE/DSIC, 2010. 63 p.

_____. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Guia de Referência para Segurança da Informação e Comunicações/** Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações; organização Claudia Canongia, Admílson Gonçalves Júnior e Raphael Mandarino Júnior. – Brasília: GSIPR/SE/DSIC, 2010 (b). 151 p.

BRANQUINHO, Marcelo. **O uso de padrões abertos para proteção de sistemas SCADA e de automação.** Palestra. Nov 2011. Rio de Janeiro.

CANONGIA, Cláudia; MANDARINO Jr, Raphael. Segurança Cibernética: o Desafio da Nova Sociedade da Informação. **Revista Parcerias Estratégicas**. Brasília: Centro de Gestão e Estudos Estratégicos (CGEE) no Ministério da Ciência e Tecnologia, dez. 2009, V. 14, n. 29, P 21-46. ISSN 1413-9375.

CANONGIA, Cláudia. 2012. **Entrevista concedida a Luis Henrique Santos Franco**.

CARNEIRO, João Marinonio Enke. 2012. **Entrevista concedida a Luis Henrique Santos Franco.**

CARMO, E. K. **A Guerra Cibernética e a Contrainteligência Virtual.** [S.I.] set. 2011. Monografia de Conclusão de Curso de Altos Estudos de Política e Estratégia (Especialização). Escola Superior de Guerra. Rio de Janeiro, 2011

CARVALHO, Paulo Sergio Melo de. **A Defesa Cibernética e as Infraestruturas Críticas Nacionais**. Artigo Científico. Brasília, 2011. 20 f.

CARVALHO, Paulo Sergio Melo de. O Setor Cibernético nas Forças Armadas Brasileiras. **Desafios Estratégicos para a Segurança e Defesa Cibernética**. Anais. Brasília, 2011b. P. 13-36.

CLARKE, Richard A; KNAKE, Robert K. **Cyberwar: the next threat to national security and what to do about it**. New York, USA: Harper Collins, 2010, 290 p, ISBN 978-0-06-196223-3.

COUTINHO, Maurílio Pereira. **Detecção de Ataques em Infraestruturas Críticas de Sistemas Elétricos em Potência usando técnicas inteligentes.** Tese de Doutorado. Out. 2007. Universidade Federal de Itajubá, MG. 259 fl.

DARTORA, Jurandir; FRANÇA, Amauri Terres. **Integração de sistemas digitais para teleoperação de usinas**. 3º Simpósio de Especialistas em Operação de Centrais hidrelétricas. Nov. 2002. Foz do Iguaçu, PR.

DEMETERCO, Fernando Antônio. Segurança das Infraestruturas Críticas. In: Ciclo de Estudos Estratégicos da Escola de Comando e Estado-Maior do Exército, 10. 2011, Rio de Janeiro. **Anais...** Rio de Janeiro: ECEME, 2011. 18 p.

DEMETERCO, Fernando Antônio. Segurança das Infraestruturas Críticas. In: Ciclo de Estudos Estratégicos da Escola de Comando e Estado-Maior do Exército, 10. 2011, Rio de Janeiro. **Palestra.** Disponível em: <http://www.eceme.ensino.eb.br/ciclodeestudosestrategicos/index.php/CEE/XCEE/paper/download/2/5> Acesso em: 10 jun. 2012.

DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO GSIPR. **Instrução Normativa GSI No. 1, de 13 de junho de 2008**: Disciplina a gestão de segurança da informação e comunicações na administração pública federal, direta e indireta, e dá outras providências. Brasília, junho 2008. Publicada no DOU No. 115, de 18 Jun 2008 – Seção 1. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic>. Acesso em: 12 mar. 2012.

DINIZ, Eugenio. CONSIDERAÇÕES SOBRE A POSSIBILIDADE DE ATENTADOS TERRORISTAS NO BRASIL - **II ENCONTRO DE ESTUDOS TERRORISMO -** Brasília Julho – 2004. II Encontro de Estudos: Terrorismo. – Brasília: Gabinete de Segurança Institucional; Secretaria de Acompanhamento e Estudos Institucionais, 2004. 123p. (Pg 15-46)

DO CARMO, Euzimar Knippel. **O Sistema de Defesa Cibernético Brasileiro – Uma Proposta** – Brasília: O autor, 2011. 120 p.; Ilustrado; 25 cm. Monografia (especialização) – Universidade de Brasília. Instituto de Ciências Exatas. Departamento de Ciência da Computação, 2011.

ENTREVISTA com o Cyberczar brasileiro. **Revista Galileu**. Disponível em < http://revistagalileu.globo.com/Revista/Galileu/0,,EDG87000-7833-216,00-ENTREVISTA+ COM+O+CYBERCZAR+BRASILEIRO.html> Acesso em 14 jun. 2012.

ELETROBRAS. O papel da Eletrobras. Disponível em < http://www.eletrobras.com/elb/data/Pages/LUMIS641DB632PTBRIE.htm> Acesso em: 14 jun. 2012a.

ELETROBRAS. Nossas empresas. Disponível em < http://www.eletrobras.com/elb/data/Pages/LUMISBF7839BFPTBRIE.htm > Acesso em: 14 jun. 2012b.

ELIPSE. Empresa de Software para supervisão e controle de processos. Disponível em < http://www.elipse.com.br/noticia_int.aspx?id=967&idioma=1>. Acesso em: 2 Jun. 2012.

ERKILLA, Tommy; SCHIMITT, Marcio. **Evolução das tecnologias para automação de hidrelétricas e exemplos práticos de aplicação.** 3º Simpósio de Especialistas em Operação de Centrais Hidrelétricas, nov. 2002. Foz do Iguaçu, PR.

FERREIRA, Aurélio Buarque de Holanda. **Dicionário Aurélio eletrônico: século XXI**. V.3.0. Nova Fronteira, Rio de Janeiro, 1999. CD-ROM.

FILHO, Braz Campanholo. 2012. **Entrevista concedida a Luis Henrique Santos Franco**.

FONTENELE, Marcelo Paiva. 2012. **Entrevista concedida a Luis Henrique Santos Franco**.

GUARINI, Priscilla de Castro. **Esquemas de Controle de segurança aplicados à operação do sistema interligado nacional**. 2007. 95 f. Monografia (graduação). Universidade Federal do Rio de Janeiro (UFRJ). Departamento de Engenharia Elétrica, Rio de Janeiro, RJ, Dez. 2007.

IASBECH, José Fernando. 2012. **Entrevista concedida a Luis Henrique Santos Franco**.

MANDARINO JR, Raphael. **Um Estudo sobre a Segurança e a Defesa do Espaço Cibernético Brasileiro**. 2009. 156 f. Monografia (especialização). Universidade de Brasília (UnB). Departamento de Ciência da Computação – DCE, Brasília, DF, Jun. 2009.

MANDARINO JR, Raphael. **Segurança e Defesa do Espaço Cibernético Brasileiro**. Recife: Cubzac, 2010. 182 p. il. ISBN: 978-85-61293-13-0.

MENDES, Gualter Carvalho. 2012. **Entrevista concedida a Luis Henrique Santos Franco**.

OLIVEIRA, Luiz Guilherme de. Tendências Tecnológicas do Setor Elétrico. **Inovação tecnológica no setor elétrico brasileiro: uma avaliação do programa de P&D regulado pela Aneel.** Fabiano Mezadre Pompermayer, Fernanda De Negri, Luiz Ricardo Cavalcante (Org.), Brasília: Ipea, p. 55 - 87, 2011. Disponível em < http://www.ipea.gov.br/portal/images/stories/PDFs/livros/livros/livro_inovacaotecnologica.pdf>. Acesso em: 10 maio 2012.

OLIVEIRA, João Roberto de. Sistema de Segurança e Defesa Cibernética Nacional: Abordagem com Foco nas Atividades Relacionadas com a Defesa Nacional. **Desafios estratégicos para segurança e defesa cibernética**. Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes e Whitney Lacerda de Freitas (Org.), Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011. P. 105-128. ISBN 978-85-85142-32-2.

QUEIROZ, Roberta. 2012. **Entrevista concedida a Luis Henrique Santos Franco.**

SÁ, Nelson de. **General detalha implantação do Centro de Defesa Cibernética, novo órgão brasileiro.** 7 maio 2012. Disponível em <http://www1.folha.uol.com.br/tec/1085498-general-detalha-implantacao-do-centro-de-defesa-cibernetica-novo-orgao-brasileiro.shtml> Acesso em: 12 maio 2012.

SILVA, Pedro Jorge S. 2012. **Entrevista concedida a Luis Henrique Santos Franco**.

SOUZA, Regina Maria de Felice. 2012. **Entrevista concedida a Luis Henrique Santos Franco**.

TEIXEIRA, Carlos Augusto Ramires. 2012. **Entrevista concedida a Luis Henrique Santos Franco.**

TRIBUNAL, de Contas da União. **Organização.** Disponível em < http://portal2.tcu.gov.br/portal/page/portal/TCU/institucional/conheca_tcu/institucional_competencias> Acesso em: 9 jun. 2012.