



## **Grupo de Estudo de Sistemas de Informação e Telecomunicação para Sistemas Elétricos-GTL**

### **SEGURANÇA CIBERNÉTICA: PANORAMA, DESAFIOS E AÇÕES EM ANDAMENTO NO SISTEMA ELÉTRICO BRASILEIRO**

**GILBERTO PIRES DE AZEVEDO (1); MAXLI BARROSO CAMPOS (2); MARIA CRISTINA GONÇALVES DE CARVALHO (3); REGIS DE SOUZA DE CARVALHO (4); PAULO CESAR PELLANDA (5)**

**CEPEL (1); EXÉRCITO BRASILEIRO (2); FURNAS (3); ELETRONUCLEAR (4); IME (5)**

#### **RESUMO**

Este trabalho busca traçar o panorama atual da Segurança Cibernética no sistema elétrico brasileiro. São abordadas as principais ameaças cibernéticas às infraestruturas críticas, especificamente no setor elétrico, as iniciativas em andamento, as questões regulatórias, as atividades de pesquisa e desenvolvimento e é apresentado o resultado de uma enquête realizada com especialistas em Segurança Cibernética no setor elétrico.

#### **PALAVRAS-CHAVE**

Segurança Cibernética, Segurança da Informação, Sistemas Elétricos, Sistemas de Controle Industrial, Infraestruturas Críticas

#### **1.0 - INTRODUÇÃO**

O avanço da digitalização dos sistemas elétricos, associado à sua crescente integração com grandes redes de computadores, é um processo irreversível e dinâmico que atingirá novos patamares com a consolidação das Redes Elétricas Inteligentes (*Smart Grid*) e da Internet das Coisas (*IoT – Internet of Things*). No entanto, a conexão às redes computacionais amplia a vulnerabilidade dos sistemas elétricos a ataques cibernéticos e, dentro de alguns anos, problemas de segurança em escala próxima àquela que atinge a Internet pública estarão presentes também nas redes elétricas, que estão entre as infraestruturas críticas de qualquer país.

As infraestruturas críticas englobam diversos serviços essenciais para uma comunidade ou país, *fazendo uso cada vez maior de TIC (tecnologias de informação e comunicação) para melhorar a qualidade dos serviços prestados e fornecer novos serviços baseados em novas tecnologias aos seus clientes, ressaltando que a operação contínua e confiável desses serviços é crítica para todos os setores da sociedade* (1,2). Esses fatores tornam estas infraestruturas críticas cada vez mais complexas e interdependentes, expondo a sociedade a maiores vulnerabilidades e ameaças à sua segurança. Por exemplo, eventos em um sistema elétrico interligado, que em um primeiro momento podem parecer pouco importantes, podem levar a falhas em cascata e ao colapso a nível regional ou mesmo nacional. Devido à interdependência das infraestruturas, tais eventos podem acarretar a interrupção de serviços de comunicações ou de emergência, fechamento de sistemas financeiros etc.

Entender e vencer os novos desafios de segurança cibernética é essencial não somente para a operação confiável do sistema elétrico existente, mas também para a evolução da sua estrutura. Caso contrário, ou a inserção das novas tecnologias será inviabilizada, ou ocorrerá em meio a riscos muito elevados, que deixarão países inteiros vulneráveis a ataques cibernéticos. Em algumas partes do mundo - como na Europa, onde a aposta em geração distribuída é componente chave da estratégia para a redução das emissões de carbono - a

(\*) Av. Horácio Macedo 354 – Cidade Universitária, Ilha do Fundão - CEP 21941-911 Rio de Janeiro, RJ – Brasil



segurança cibernética há algum tempo já faz parte das áreas de pesquisa prioritárias para o sistema elétrico. Esses países preparam-se para obter uma vantagem competitiva importante, pois o compartilhamento do conhecimento adquirido não ocorrerá sem custos nem de forma aberta.

A percepção da relevância da Segurança Cibernética como elemento essencial para viabilizar as transformações no setor elétrico reflete-se em ênfase crescente à pesquisa no assunto. Isto pode ser constatado pela evolução do número de publicações sobre o tema nos últimos anos. A figura a seguir mostra os resultados de pesquisas na base de dados do IEEEExplore sobre publicações que incluem as palavras chave “cyber physical systems security” (em azul) e “cyber physical systems security” AND “power systems” (em vermelho). O comportamento geral das duas curvas é similar e mostra um crescimento explosivo do número anual de publicações, em especial a partir de 2008. Observa-se também, na média dos últimos 11 anos (2008-18), o expressivo percentual de 39% das publicações do IEEE sobre segurança de sistemas ciber físicos que abordaram também o tema em sistemas elétricos de potência.

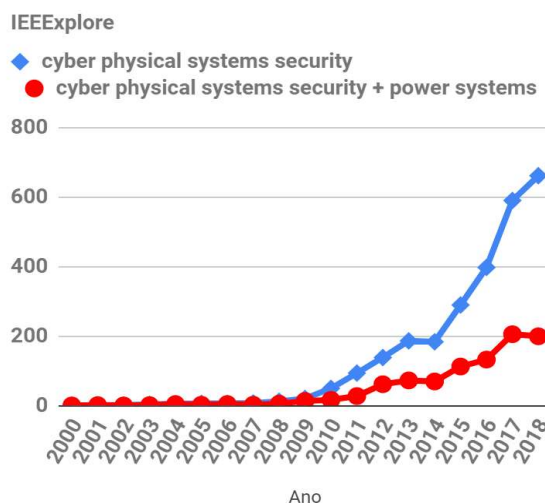


Figura 1 – Número anual de publicações com as palavras chave “cyber physical systems security” (em azul) ou “cyber physical systems security” AND “power systems” (em vermelho).

## 2.0 - CONCEITOS

A Segurança Cibernética é parte da Segurança da Informação. Enquanto esta última se refere à proteção de informações - armazenadas ou não em meio eletrônico – contra quaisquer formas não autorizadas de acesso, uso, divulgação, destruição, modificação etc., a Segurança Cibernética aborda a proteção tecnológica de sistemas, redes e programas computacionais contra ataques realizados por meio digital.

No Brasil, o Livro Verde de Segurança Cibernética (3) define:

- Infraestruturas Críticas: “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.”
- Infraestruturas Críticas da Informação: “Subconjunto de ativos de informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade.”
- Ativo de Informação: “...os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso”.

De acordo com (1), entende-se por produto ou serviço de uma infraestrutura crítica aquilo que é produzido pela mesma. Setor crítico compreende um conjunto de produtos e serviços da infraestrutura crítica que são dirigidos como uma responsabilidade governamental e/ou privada comum. Dependência é uma ligação ou conexão entre

(\*) Av. Horácio Macedo 354 – Cidade Universitária, Ilha do Fundão - CEP 21941-911 Rio de Janeiro, RJ – Brasil



dois produtos ou serviços, através do qual o estado de um influencia o outro. A dependência existe quando a entrada, criação, produção ou distribuição de um produto crítico ou serviço requer outro produto crítico ou serviço. Intradependência e interdependência referem-se à dependência mútua de produtos e serviços dentro da mesma infraestrutura crítica ou entre infraestruturas críticas, respectivamente. O aumento da interdependência entre infraestruturas críticas leva ao crescimento das vulnerabilidades. Nos casos mais extremos, interrupções de serviços, modificação ou destruição inadequada de informação podem ameaçar vidas e propriedades, possivelmente interrompendo atividades essenciais de governos e de corporações, resultando em riscos para a vida, para a liberdade e para propriedade (5,6).

### **3.0 - AMEAÇAS CIBERNÉTICAS AO SETOR ELÉTRICO**

As motivações para ataques cibernéticos ao sistema elétrico são variadas: autoafirmação de indivíduos ou grupos; vandalismo; roubo de informações; extorsão; concorrência desleal; terrorismo; e guerra. Apesar de haver formas simples e de baixa tecnologia de causar grandes incidentes no sistema elétrico, os ataques cibernéticos permitem que as ações sejam conduzidas em relativo anonimato, a qualquer momento, à distância e sem risco imediato para os atacantes. A crescente vulnerabilidade do sistema elétrico a tais ataques, associada à também sempre crescente dependência da sociedade em relação à energia elétrica, inclui o setor entre as infraestruturas críticas das nações e sua proteção torna-se assunto de segurança nacional.

Ataques cibernéticos bem-sucedidos podem capitular uma nação inteira a manobras políticas e/ou militares (7). Podem ser realizados por terroristas à distância de forma parcial ou totalmente anônima, são relativamente baratos e seguros para os atacantes, e podem afetar um conjunto de alvos muito maior que ataques físicos convencionais. Uma lista de possíveis alvos de ataques cibernéticos no Brasil seriam sistemas com funções vitais, como o comando das redes de energia elétrica, do tráfego aéreo, das redes de telecomunicação em geral, dos “enlaces” com sistema de satélites e das redes do Ministério da Defesa. A vulnerabilidade destes sistemas complexos essenciais na vida moderna é agravada pelo alto nível de integração entre redes de telecomunicações e a Internet, de forma que as informações que regem as tomadas de decisão são feitas utilizando dispositivos que fazem parte desta infraestrutura. Esse cenário cria um ambiente propício a ações ofensivas diferentes das tradicionais e que podem afetar significativamente a infraestrutura crítica de um país.

Atualmente uma das principais ameaças às infraestruturas críticas, inclusive no setor elétrico, são os malwares classificados como “ransomwares”. Estes malwares são compostos por código malicioso que usa criptografia para causar indisponibilidade dos dados armazenados. Criptografam-se arquivos, diretórios locais e móveis nos ativos infectados, inclusive nos serviços de armazenamento em nuvem, exigindo-se o pagamento de resgate (geralmente em bitcoins) para restabelecer a disponibilidade do acesso ao usuário. O ransomware é considerado uma ameaça cibernética criminal crescente com diversas variantes (8), e observa-se claramente a necessidade de priorização da segurança dos dados das grandes corporações. Em 2017, 65% das empresas afetadas por ataques “ransomware” perderam o acesso a um volume significativo de dados e o setor financeiro sofreu o maior impacto em custos, dentre os setores afetados. Os ataques de *ransomware* aumentaram em mais de 90% entre 2016 e 2017 (9) e mais de 50% das empresas atacadas em 2017 foram empresas industriais.

Ainda não são muitos os ataques cibernéticos especificamente direcionados ao setor elétrico. Em 2012, o malware Shamoon atuou no Oriente Médio atacando uma usina de geração de energia, causando destruição nos dados de 30.000 desktops; em 2013, o Havex atacou diversas empresas do segmento de energia em 25 países, principalmente nos EUA, com objetivo de roubo de dados industriais; em 2015, um caso complexo de ataque ransomware via APT Black Energy direcionado para a Companhia ucraniana de distribuição de energia elétrica, envolveu uma invasão nos computadores e sistemas SCADA da companhia causando um blackout de três horas para cerca de 80 mil clientes (3). Em 2016 um ataque ransomware na Central de Geração Elétrica de Israel causou interrupção de diversos computadores da companhia. Até o momento, o alcance dos ataques tem sido limitado pelo nível ainda relativamente baixo (se comparado ao futuro próximo) de automação do sistema elétrico. Mas certamente muitos outros ataques virão, e as variantes de ransomware merecem atenção especial, por ser este um malware que pode facilmente gerar indisponibilidade em infraestruturas críticas.

### **4.0 - ENQUETE SOBRE A SITUAÇÃO DA SEGURANÇA CIBERNÉTICA NO SETOR ELÉTRICO BRASILEIRO**

Para obter um panorama da situação da segurança cibernética no Brasil isento do viés das opiniões dos autores

(\*) Av. Horácio Macedo 354 – Cidade Universitária, Ilha do Fundão - CEP 21941-911 Rio de Janeiro, RJ – Brasil



deste trabalho, foi realizada uma enquete online envolvendo somente especialistas com conhecimento de Segurança Cibernética no Setor Elétrico. Dela participaram mais de 50 pessoas, um número expressivo considerando que os convites foram enviados a um público restrito.

A primeira etapa da enquete consistia na identificação dos negócios aos quais as instituições dos participantes estão associadas. Ressaltando que os participantes puderam indicar mais de um segmento de atuação (por exemplo, a empresa pode atuar simultaneamente em geração e transmissão), os resultados foram: (i) Geração de Energia - 43,9%; Transmissão de Energia - 22,8%; Distribuição de Energia - 7%; Consultoria - 29,8%; Centro de Pesquisa ou Universidade - 26,3%. Chama a atenção a baixa participação do setor de Distribuição de Energia, onde as novidades trazidas pelo advento do Smart Grid gerarão forte demanda por Segurança Cibernética.

Nas questões sobre Governança de Segurança da Informação e Gestão de Riscos, 60% responderam que suas empresas possuem área específica para esses temas. Tal número deve ser interpretado com cautela pois pode passar um retrato otimista da realidade, já que o público da pesquisa foi composto por especialistas e muitas empresas talvez sequer possuam pessoal qualificado. Dentre as empresas que seguem normas de segurança de alguma entidade, 29% seguem as da NERC-CIP; as demais seguem uma variedade de outras normas.

As questões seguintes abordaram a situação do quadro de profissionais de Segurança da Informação, tanto em TI (rede corporativa) como em TO (rede de operação). O nível de treinamento e capacitação dos profissionais de TI foi considerado *alto* em apenas 19,3% das respostas, enquanto 33,3% o avaliaram como *baixo* e 47,3% como *médio*. Para TO, os resultados foram um pouco piores: *alto* - 20,7%; *baixo* - 53,4%; e *médio* - 25,9%. Quanto ao número de funcionários com capacitação em Segurança da Informação, 75% o classificaram como *insuficiente*. Para o tratamento de incidentes de segurança cibernética, 49,1% responderam que suas instituições não possuem equipes para tal; 14% possuem equipes mistas de TI e TO; 12,3% possuem equipes separadas para TI e TO, e 24,6% somente equipes de TI.

No quesito Dependência Tecnológica, apenas 10,5% responderam que usam soluções de um único fornecedor e, em 89,5% das respostas, os fornecedores têm equipe de suporte no Brasil. Quanto ao atendimento prestado pelos fornecedores, 43,9% consideram que atende às expectativas e necessidades, enquanto 47,4% avaliam que atende parcialmente e 8,8% que não atende.

As respostas às questões sobre atividades de Pesquisa, Desenvolvimento e Inovação (P&D+I) em Segurança Cibernética mostraram que a relevância dessas atividades é amplamente reconhecida pelos especialistas: 84,2% consideraram que a participação em atividades de P&D+I poderia contribuir para a evolução técnica da área. Nas questões sobre o envolvimento das instituições no desenvolvimento de produtos inovadores e em pesquisas na área, excluindo os que comunicaram não saber a resposta, 66% informaram que a sua instituição participa do desenvolvimento de produtos inovadores (software, equipamentos ou processos) e 63% em atividades de pesquisa. A utilização de recursos vinculados à Lei 9.991/2000 ("P&D ANEEL") também foi objeto de questão específica, mas seus resultados serão discutidos na seção 5.4 deste trabalho.

A parte final da pesquisa abordou a percepção subjetiva dos especialistas sobre a situação geral da segurança cibernética no setor elétrico brasileiro:

- "Como você avalia o nível global de segurança cibernética entre as empresas e entidades do setor elétrico brasileiro?" 02% - Alto; 33% - Médio; 65% - Baixo.
- "Como você avalia a capacidade do sistema elétrico brasileiro resistir a ataques cibernéticos que visem provocar danos e desligamentos com impacto sistêmico?" 5% - Alta; 37% - Média; 58% - Baixa.
- "Como você avalia o nível de conscientização para os reais riscos de Segurança Cibernética entre os gestores de empresas e entidades?" 2% - Adequado; 28% - Razoável; 70% - Insuficiente.
- "Como você avalia os atuais regulamentos sobre Segurança Cibernética específicos para o sistema elétrico brasileiro?" 3,5% - Adequados; 31,5% - Razoáveis; 65% - Insuficientes.

As respostas dos especialistas não deixam dúvidas: o nível atual de maturidade sobre o tema no Brasil é insuficiente, assim como a regulamentação e a conscientização dos gestores das empresas, deixando o sistema elétrico do país vulnerável a ataques com impacto sistêmico.



## **5.0 - PANORAMA E AÇÕES EM ANDAMENTO NO BRASIL**

### **5.1- Histórico**

A preocupação com Segurança Cibernética no Setor Elétrico Brasileiro, no contexto da defesa da infraestrutura crítica da nação, remonta a 2008, quando o Gabinete de Segurança Institucional da Presidência da República (GSI) criou os Grupos Técnicos de Segurança das Infraestruturas Críticas. O GSI editou um Guia de Referência para a segurança das infraestruturas críticas da informação, direcionado para o contexto de segurança da informação e que precisa ser revisado para atender às demandas atuais voltadas para infraestruturas críticas. Atualmente o Departamento de Segurança da Informação e Comunicações (DSIC) do GSI está conduzindo um Grupo de Trabalhos específico de Infraestrutura Crítica (IC) visando construir um plano nacional de proteção de IC alinhado à Política Nacional de Segurança da Informação, com previsão de aprovação ainda em 2019.

Quanto à implantação da defesa cibernética no Brasil, cabe ao Exército Brasileiro coordenar as ações no âmbito do Ministério da Defesa, conforme atribuição definida por meio da Diretriz Ministerial nº 0014/2009 (10). Esta diretriz complementou a Estratégia Nacional de Defesa (11), que, na sua primeira versão, criava três setores estratégicos para defesa: o Nuclear, sob coordenação da Marinha do Brasil, o Espacial sob coordenação da Força Aérea e o Cibernético, que à época não recebeu no documento uma indicação de qual Força Armada seria a coordenadora deste relevante setor.

Sob a perspectiva militar, este setor incorpora um nicho peculiar que compreende os conceitos de defesa cibernética, no nível estratégico-militar, e de guerra cibernética, no nível operacional-militar. A estrutura deve propiciar os meios e os processos que permitam ações no espaço cibernético sempre que as Forças Armadas venham a ser chamadas a atuar, em situações de crise ou de conflito, ou antecipando-se a estas situações. A partir de 2017 as ações das Forças Armadas na defesa cibernética das infraestruturas críticas começaram a ganhar mais visibilidade, principalmente porque ficou evidente que um ataque cibernético em uma infraestrutura crítica poderia deixar o país vulnerável a ações de um inimigo e impactar diretamente a segurança nacional.

### **5.2- Exercício Guardiã Cibernética**

O Comando de Defesa Cibernética iniciou, em 2018, a coordenação da primeira edição do Exercício Guardiã Cibernética, com o objetivo de disponibilizar em um único espaço físico, em Sobradinho - Brasília, um ambiente propício para tratar e discutir os principais desafios em segurança cibernética, assim como iniciar um processo de estabelecimento de importantes princípios da proteção cibernética voltados para setores de infraestruturas críticas nacionais, pautada na troca de experiências, colaboração e com um forte viés de parceria entre todos os envolvidos. O exercício entrou no calendário anual da segurança cibernética nacional e, em sua segunda versão, além dos setores nuclear e financeiro (presentes na primeira edição), participaram os setores de telecomunicações e elétrico. Na sua primeira edição, em 2018, participaram 115 civis e militares oriundos de 23 organizações e empresas ligadas à Defesa, Governo, comunidade acadêmica e setores estratégicos. Na segunda edição, em 2019, foram 38 organizações e 204 participantes e observadores, com diferentes comitês nacionais e internacionais como observadoras.

Como principais contribuições do exercício, pode-se destacar que a atividade (i) contribui para incrementar a atuação colaborativa junto a diversos atores importantes para a proteção cibernética de infraestruturas críticas de interesse para a Defesa Nacional, especialmente Forças Armadas, governo, comunidade acadêmica e estruturas estratégicas; (ii) permite identificar premissas para o estabelecimento de protocolos para o compartilhamento de informação no âmbito dos participantes; (iii) incentiva a troca de experiências e de boas práticas entre os envolvidos; (iv) possibilita identificar, por meio dos problemas cibernéticos simulados, oportunidades de melhorias nos protocolos e processos de contingência existentes nas organizações e empresas; (v) proporciona ao ComDCiber um maior conhecimento acerca do cenário cibernético em setores estratégicos de interesse para a Defesa Nacional, facilitando as coordenações e incrementando a consciência situacional para o eventual emprego de equipes voltadas para as ações de proteção. A realização do exercício tem ajudado na construção de uma forte comunidade nacional de segurança cibernética, pautada na troca de experiências, colaboração e com um forte viés de parceria entre todos os envolvidos.





## XXV SNPTTE SEMINÁRIO NACIONAL DE PRODUÇÃO E TRANSMISSÃO DE ENERGIA ELÉTRICA

10 a 13 de novembro de 2019  
Belo Horizonte - MG

4015  
GTL/22

### 5.3- Outros Eventos e Iniciativas

Nos últimos anos, empresas de segurança cibernética começaram a dedicar atenção às especificidades do setor elétrico, foram organizados os primeiros eventos especializados, foram montados grupos de pesquisa e associações de empresas de geração e transmissão criaram grupos de trabalho para estudar os desafios envolvidos. Algumas dessas iniciativas são examinadas a seguir.

Em 2018, a ABRATE - Associação Brasileira das Empresas Transmissoras de Energia Elétrica criou a Força Tarefa de Segurança Cibernética com o objetivo de produzir um framework de segurança para infraestruturas críticas do setor elétrico, contemplando a definição de práticas de segurança cibernética em instalações de transmissão de energia elétrica para sistemas de telecomunicações, sistemas SCADA e demais recursos relacionados às redes de automação. O framework ABRATE foi produzido tomando como base o Framework for Improving Critical Infrastructure Cybersecurity do NIST e o C2M2 (Cybersecurity Capability Maturity Model) do subsetor de eletricidade do Departamento de Energia Americano –DOE. O framework foi apresentado em janeiro de 2019 ao Conselho da ABRATE e aprovado para divulgação.

Também em 2018, no mês de julho, a ABRAGE - Associação Brasileira das Empresas Geradoras de Energia Elétrica, por meio do seu Comitê Estratégico de Segurança em Instalações (CESI), promoveu em Itaipu o Colóquio Técnico de Segurança Cibernética para o Sistema Elétrico – Realidades e Desafios na Busca de Soluções. O evento foi uma iniciativa conjunta da ABRAGE, de Itaipu Binacional e do Centro de Estudos Avançados em Proteção de Estruturas Estratégicas (CEAPE) da Fundação Parque Tecnológico Itaipu. Contou ainda com a parceria do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), da Agência Nacional de Energia Elétrica (ANEEL), do Operador Nacional do Sistema (ONS), da Marinha do Brasil, do Exército Brasileiro, da Força Aérea Brasileira e da Universidade de Brasília. O objetivo do evento foi debater conceitos, riscos, ameaças, vulnerabilidades e outras questões cibernéticas evidenciadas e aplicadas à segurança das infraestruturas críticas do sistema elétrico, compartilhando idéias e propostas que pudessem subsidiar caminhos para soluções ou mesmo apontá-los.

Empresas privadas e entidades científicas também voltaram sua atenção para o assunto e promoveram eventos. Em dezembro de 2018 o CIGRÉ-Brasil realizou em Brasília o I Workshop de Segurança Cibernética para Sistemas de Geração, Transmissão e Distribuição de Energia Elétrica (WSEC-GTD), abordando diversos aspectos como normas, regulamentação, casos reais, gestão, riscos, pesquisas e desafios técnicos. Empresas privadas também vêm promovendo eventos relevantes, em geral abrangendo outros setores que também utilizam sistemas de controle industriais. Um exemplo é a Conferência de Segurança Cibernética para o Setor de Energia, Utilities e Indústrias no Brasil, que já está na sua quinta edição e relata a participação de mais de 400 pessoas de 160 empresas nas suas primeiras 4 edições.

### 5.4- Pesquisa, Desenvolvimento e Inovação – P&D+I

As atividades de P&D+I são essenciais em um tema dinâmico como a Segurança Cibernética no setor elétrico, sempre em rápida evolução. Se em alguns países já é significativo o número de pesquisadores e publicações, no Brasil estão sendo dados os primeiros, mas importantes, passos nesse sentido. Alguns grupos de pesquisa estão sendo estruturados, com destaque para o Centro de Estudos Avançados em Proteção de Estruturas Estratégicas (CEAPE2), implantado na Fundação Parque Tecnológico de Itaipu – FPTI com a participação do Exército Brasileiro. Universidades como o IME, UTFPR, UNIOESTE e UNB têm ou estão criando grupos voltados para o tema, com envolvimento direto ou indireto nos projetos daquele Centro.

Atividades de pesquisa experimental, ensaios, testes e homologações em breve poderão ser desenvolvidos em laboratórios de Smart Grid ou de simulação em tempo real que estão sendo implantados no IME em conjunto com a FPTI, no Cepel, ONS e em outras entidades. A modernização dos equipamentos de monitoramento e controle da usina de Itaipu, prevista para os próximos anos, motivou o desenvolvimento de um projeto conjunto entre o IME e a FPTI, já em curso, que, prevê a implantação de um ambiente de simulação do tipo *hardware in the loop* incluindo dispositivos físicos industriais que representem infraestruturas críticas na área de sistemas elétricos de potência e de Tecnologia de Automação (TA). O ambiente de simulação proverá condições para P&D+I nas áreas de Tecnologia da Informação e Comunicação (TIC) e segurança cibernética aplicadas à TA de infraestruturas críticas, notadamente de sistemas elétricos de potência. O laboratório será estruturado em camadas, de acordo com a aplicação dos ativos relacionados com TIC e TA: a camada de negócios compreende a internet e equipamentos que possam realizar o acesso externo; a camada de gerenciamento

(\*) Av. Horácio Macedo 354 – Cidade Universitária, Ilha do Fundão - CEP 21941-911 Rio de Janeiro, RJ – Brasil

Tel: (+55 21) 2598-6135 – Email: gilberto@cepel.br



## XXV SNPTTE SEMINÁRIO NACIONAL DE PRODUÇÃO E TRANSMISSÃO DE ENERGIA ELÉTRICA

10 a 13 de novembro de 2019  
Belo Horizonte - MG

4015  
GTL/22

compreende ativos de redes e servidores; a camada de supervisão e monitoramento compreende os equipamentos de monitoramento como o computador do operador e o sistema SCADA; a camada de produção e controle compreende os equipamentos físicos de controle como controladores lógicos programáveis e unidades terminais remotas, que se comunicam com o nível superior e atuam sobre o sistema físico por meio de equipamentos físicos; e camada de simulação eletromecânica compreende os equipamentos e software responsáveis pela simulação em tempo real de sistemas elétricos - RTDS (*Real Time Digital Power System Simulator*).

Na enquete discutida na seção anterior, um resultado preocupante é que apenas 7% dos especialistas informaram que as suas empresas utilizam recursos vinculados à Lei 9.991/2000 ("P&D ANEEL"), apesar da disponibilidade de recursos para esse fim entre as empresas do setor elétrico ser da ordem de várias centenas de milhões de reais. Uma análise dos títulos de 2.516 projetos de P&D cadastrados na ANEEL em maio de 2019 (12) permitiu identificar apenas 4 projetos associados à segurança cibernética de sistemas elétricos, que representavam irrisórios 0,1% do total dos R\$ 8,586 bilhões de investimentos nos projetos. Isto indica que há um espaço significativo para avanços nas atividades de P&D+I em segurança cibernética utilizando os recursos da Lei 9.991/2000, desde que seja feito um esforço para aproximação entre os gestores de P&D+I nas empresas e os pesquisadores do tema.

O desconhecimento mútuo pode explicar a baixa utilização desses recursos de P&D ANEEL nas pesquisas em Segurança Cibernética, e uma eventual Chamada Pública de Projetos Estratégicos de P&D pela ANEEL com foco em Segurança Cibernética para o Setor Elétrico seria de grande valia para colocar o tema em evidência não apenas para os gestores de P&D, mas também para as diretorias das empresas. Neste sentido a UTCAL - Utilities Telecommunications Council da América Latina elaborou, com o apoio do CPqD, um Projeto de Cibersegurança no Setor Elétrico Brasileiro que foi levado ao conhecimento da ANEEL para avaliação. O órgão regulador poderá optar por disparar uma Chamada Pública de P&D Estratégico, demonstrando que o tema é de interesse estratégico para o setor, ou a UTCAL poderá conduzir um projeto cooperado entre os seus associados; em ambos os casos, pode-se utilizar recursos derivados da Lei 9.991/2000 ("P&D ANEEL").

### 5.5- Regulamentos

A regulamentação dos requisitos de segurança cibernética no sistema elétrico brasileiro ainda é incipiente. A revisão 2016.12 do Submódulo 10.14 dos Procedimentos de Rede do ONS (13) limita-se a destacar que os centros de operação do ONS e dos agentes devem dispor de "recursos tecnológicos para proteção contra ataques cibernéticos na Rede de Supervisão e controle dos centros de operação", sem maior detalhamento. O ONS, porém, já indicou que será elaborado um novo submódulo dos Procedimentos de Rede para abordar especificamente questões de segurança cibernética.

Por enquanto, a falta de definição de requisitos de segurança cibernética por parte dos órgãos reguladores nos leilões de novos empreendimentos faz com que os recursos investidos na implantação da respectiva infraestrutura não sejam incluídos na remuneração futura. Isto transforma os dispêndios com segurança cibernética em custos a serem minimizados ou eliminados. Por consequência, alguns empreendimentos são realizados sem maiores preocupações com a segurança, em especial em SPEs nas quais que as empresas responsáveis pela construção não são as mesmas que farão a operação. Por força de contratos de O&M, algumas empresas são obrigadas a incorporar em suas redes empreendimentos que não atendem aos requisitos mínimos de segurança cibernética, colocando-as sob risco.

### **6.0 - CONCLUSÃO**

A evolução dos sistemas elétricos de potência ao longo dos próximos anos aponta para caminhos que passam inexoravelmente por uma grande conectividade às redes computacionais, as quais agregarão ao sistema não apenas as suas facilidades, mas também seus inúmeros riscos. A segurança cibernética passará de um requisito secundário para a operação confiável dos sistemas elétricos, como ainda tem sido tratada, para um elemento essencial para viabilizar a sua sobrevivência e a sua evolução.

Neste trabalho mostrou-se que, se a situação da segurança cibernética no Brasil ainda está longe da ideal, por outro lado há diversas iniciativas importantes e articuladas em andamento no país. As Forças Armadas vêm

(\*) Av. Horácio Macedo 354 – Cidade Universitária, Ilha do Fundão - CEP 21941-911 Rio de Janeiro, RJ – Brasil

Tel: (+55 21) 2598-6135 – Email: gilberto@cepel.br



## XXV SNPTTE SEMINÁRIO NACIONAL DE PRODUÇÃO E TRANSMISSÃO DE ENERGIA ELÉTRICA

10 a 13 de novembro de 2019  
Belo Horizonte - MG

4015  
GTL/22

desempenhando um papel de destaque na defesa cibernética da infraestrutura crítica da nação em geral, incluindo o setor elétrico, e entidades civis ligadas ao setor também estão se mobilizando, realizando estudos, propostas e eventos. Algumas empresas privadas nacionais também vêm tendo atuação relevante.

A segurança cibernética do setor elétrico é um tema de pesquisa intensiva em muitos países. No Brasil estão sendo criados laboratórios aptos a dar suporte a atividades de pesquisa e desenvolvimento no assunto, assim como novos grupos de estudo em universidades e centros de pesquisa; além disso, espera-se que a ANEEL em breve reconheça a importância dessas pesquisas lançando uma Chamada Pública para Projetos de P&D específica sobre Segurança Cibernética. Finalmente deve-se lembrar que, apesar das especificidades do sistema elétrico brasileiro, a integração com ações de pesquisa em andamento no exterior poderá trazer importantes benefícios e aumentar a produtividade das atividades realizadas aqui.

### 7.0 - REFERÊNCIAS BIBLIOGRÁFICAS

- (1) "Detecção de ataques em infraestruturas críticas de sistemas elétricos de potência usando técnicas inteligentes" - COUTINHO, Maurílio Pereira.. - Programa de Pós-graduação em engenharia elétrica, Universidade Federal de Itajubá – 2007
- (2) "Os Ciber Ataques e a Soberania Nacional" - CARDOSO, Luiz Souza - Revista Planejamento Civil de Emergência. Nº 09 –2007
- (3) 'CRASH OVERRIDE': THE MALWARE THAT TOOK DOWN A POWER GRID – Andy Greenberg – WIRED - <https://www.wired.com/story/crash-override-malware/> (consultado 01.04.2018) – 06.12.2017
- (4) "Livro Verde da Segurança Cibernética no Brasil" – organizado por Raphael Mandarin Junior e Claudia Canongia – Brasília – 2010
- (5) "Proposta de arquitetura para coleta de ataques cibernéticos às infra estruturas críticas" - Carvalho., R.S – 2014 – Dissertação de Mestrado - IME – Instituto Militar de Engenharia - Departamento de Engenharia de Sistemas e Computação
- (6) "Segurança do Espaço Cibernético no Contexto de um País" - BEZERRA, E. Kowask; NAKAMURA, E. Tissato; LIMA, M. Barbosa; RIBEIRO, S. Luís - I Conferência Interacional de Perícias em Crimes Cibernéticos, ICCyber - 2004.
- (7) "Introdução à Guerra Cibernética: a necessidade de um despertar brasileiro para o assunto" - DUTRA, André M. Carvalhais - Instituto Tecnológico da Aeronáutica - 2009.
- (8) "Cartilha de Segurança para Internet" - CERT.BR - <https://cartilha.cert.br/ransomware/> - 2018
- (9) "Ransomware – What it is and what to do about it" – National Cybersecurity and Communications Integration Center's (NCCIC)
- (10) Ministério da Defesa. Diretriz Ministerial nº 14 – Integração e Coordenação dos Setores Estratégicos da Defesa. Brasília, 9 de novembro de 2009.
- (11) Ministério da Defesa. Estratégia Nacional de Defesa – Portaria nº 6.703, de 18 de dezembro de 2008.
- (12) "Lista de Projetos de P&D (Resolução Normativa 316/2008)" – ANEEL - [http://www.aneel.gov.br/documents/656831/14930488/Projetos\\_PED-ANEEL\\_%28Res\\_Norm\\_316-2008%29-2018-05-23.xls/f02bb791-2810-0b67-1498-faed68e1f6f6](http://www.aneel.gov.br/documents/656831/14930488/Projetos_PED-ANEEL_%28Res_Norm_316-2008%29-2018-05-23.xls/f02bb791-2810-0b67-1498-faed68e1f6f6) - acessado em 15/05/2019.
- (13) "Procedimentos de Rede" - ONS - Operador Nacional do Sistema Elétrico - <http://ons.org.br/paginas/sobre-ons/procedimentos-de-rede/vigentes> - acessado em 15/05/2019.

### 8.0 - DADOS BIOGRÁFICOS



**Gilberto Pires de Azevedo** é natural do Rio de Janeiro (1960) e graduou-se em Engenharia Elétrica pela PUC-RJ em 1984, concluiu mestrado também em Engenharia Elétrica na COPPE-UFRJ em 1989, doutorado em Ciência da Computação na PUC-RJ em 1998 e especialização em Gestão Estratégica da Inovação Tecnológica no Setor de Energia Elétrica na UNICAMP em 2012. Atua no CEPEL – Centro de Pesquisas de Energia Elétrica como pesquisador desde 1985, em áreas variadas como análise de redes elétricas, centros de controle de energia elétrica, interação homem-computador, desenvolvimento de software, sistemas multiagentes, segurança da informação, redes elétricas inteligentes e gestão da inovação tecnológica.



**Maxli Barroso Campos** é natural do Rio de Janeiro, especialista em Gerência de Redes de Computadores pelo NCE/UFRJ, Gestão de Segurança da Informação e Comunicações pela UNB e Mestre em Sistemas e Computação pela UNIFACS (Salvador) e é profissional certificado

cio Macedo 354 – Cidade Universitária, Ilha do Fundão - CEP 21941-911 Rio de Janeiro, RJ –

Tel: (+55 21) 2598-6135 – Email: gilberto@cepel.br





**XXV SNPTTE**  
**SEMINÁRIO NACIONAL DE PRODUÇÃO E**  
**TRANSMISSÃO DE ENERGIA ELÉTRICA**

10 a 13 de novembro de 2019  
Belo Horizonte - MG

4015  
GTL/22

Certified Information Systems Security Professional (CISSP). Atualmente é Chefe da Divisão de Sistemas e Segurança do Departamento de Gestão Estratégica do Comando de Defesa Cibernética (Com D Ciber), trabalhando como analista em segurança cibernética na supervisão de projetos estratégicos no âmbito do Ministério da Defesa e como coordenador do grupo de estudos do Exercício Guardião Cibernético.

**Maria Cristina Gonçalves de Carvalho** é natural do Rio de Janeiro e graduou-se em Engenharia Operacional Eletrônica pelo CEFET-RJ EM 1978 e em Engenharia Elétrica também pelo CEFET-RJ em 1982. Concluiu o curso de pós-graduação em Análise de Sistemas na PUC-RJ em 1988. Trabalha na Eletrobras Furnas desde 1982 e atua como coordenadora da Rede Operativa de Furnas desde 2005.



**Regis de Souza de Carvalho** é natural do Rio de Janeiro e graduou-se em Bacharel em Ciência da Computação pela UNICARIOCA-RJ. É pós-graduado em Logística Empresarial e MBA executivo em Políticas Públicas pela UCAM - Universidade Cândido Mende-RJ. Possui Mestrado em Sistemas e Computação (Defesa Cibernética) pelo IME- Instituto Militar de Engenharia. É professor universitário, palestrante e integrante do grupo de trabalho de elaboração do Plano Nacional de Tratamento e Resposta de Incidentes Computacionais (PNTIR), vinculado ao GSI - Presidência da República e do GT de Segurança Cibernética para as Utilities de Energia Elétrica no Brasil (CIGRÉ-BR). É Analista de Tecnologia da Informação na Eletrobras Eletronuclear desde 2006 e atua na área de Segurança e Infraestrutura de TIC.



**Paulo César Pellanda** é natural de Curitiba (1962) e graduou-se em Engenharia Elétrica pela UTFPR em 1985, concluiu mestrado também em Engenharia Elétrica no IME em 1993, doutorado em Sistemas Automáticos pelo Institut Supérieur de l'Aéronautique et de l'Espace - ISAE (França) em 2001 e mestrado em Ciências Militares pela Escola de Comando e Estado Maior do Exército - ECEME (2103). Possui especialização em Gestão de Projetos e Negociação (2008) e Master in Business Administration (2013) pela Fundação Getúlio Vargas, especialização em Política, Estratégia e Altos Estudos pela ECEME (2103) e Curso Superior de Defesa pela Escola Superior de Guerra do Ministério da Defesa (2013). Atua no Departamento de Engenharia Elétrica do IME desde 1994, onde foi o chefe do departamento e coordenador do Programa de Pós-Graduação em Engenharia de Defesa. As áreas de ensino e pesquisa do seu interesse incluem análise de circuitos, controle de sistemas elétricos de potência e sistemas de controle com aplicações nos campos aeroespacial, de estruturas flexíveis e de sistemas elétricos.

(\*) Av. Horácio Macedo 354 – Cidade Universitária, Ilha do Fundão - CEP 21941-911 Rio de Janeiro, RJ – Brasil

Tel: (+55 21) 2598-6135 – Email: gilberto@cepel.br