SENADO FEDERAL
Gabinete do Senador **ESPERIDIÃO AMIN**

SENADO FEDERAL

COMISSÃO DE RELAÇÕES EXTERIORES E DE DEFESA NACIONAL

RELATÓRIO DE AVALIAÇÃO DE POLÍTICA PÚBLICA

A POLÍTICA NACIONAL SOBRE DEFESA CIBERNÉTICA

PRESIDENTE: SENADOR NELSINHO TRAD

VICE-PRESIDENTE: SENADOR MARCOS DO VAL

RELATOR: SENADOR ESPERIDIÃO AMIN

Senado Federal – Anexo II – Ala Senador Afonso Arinos – Gabinete 6 – CEP 70165-900 – Brasília DF
Telefone: +55 (61) 3303-9050 – E-mail: sen.fabianocontarato@senado.leg.br

Brasília, 9 de dezembro de 2019

SUMÁRIO

APRESENTAÇÃO

O pioneirismo da ciência da computação está indissociavelmente ligado ao conflito armado. Estamos a pensar sobretudo na Segunda Guerra Mundial e no matemático Alan Mathison Turing, que trabalhou na inteligência britânica como criptografista, a fim de desvendar a versão alemã da máquina eletromecânica Enigma e, por consequência, ter acesso aos códigos nazistas de guerra.

O equipamento criado por Turing era conhecido como a Bomba Eletromecânica, ou somente *The Bombe*. Não são poucas as opiniões que apontam essa invenção como uma das responsáveis pelo fim da Segunda Guerra Mundial.

A bomba nuclear é muito mais espetacular em seu potencial de destruição, visível com sua enorme nuvem de cogumelo no horizonte e milhares de mortos, e não resta dúvida do impacto gerado pela bomba de fissão de urânio e pela bomba de fissão de plutônio despejadas respectivamente nas cidades japonesas de Hiroshima e Nagasaki sob os desígnios daquela guerra.

Contudo, jamais outras bombas atômicas ou termonucleares foram utilizadas, enquanto o mundo cibernético e seus benefícios e perigos invadiram nosso cotidiano e estão nas nossas mãos e casas e a cada dia caminham para as fronteiras da inteligência artificial. Não se despreza, evidentemente, o potencial das armas nucleares no cenário geopolítico atual. Tanto é verdade que o Brasil considera a área nuclear um setor estratégico de defesa nacional, ao lado do espacial e do cibernético.

O chefe de estatística da equipe de Alan Turing, o matemático I. J. Good, assim vaticinou em 1965:

> "Defina-se uma máquina ultrainteligente como uma máquina capaz de superar todas as atividades intelectuais de qualquer homem, independentemente de quão genial ele seja. Já que o projeto de máquinas é uma dessas atividades intelectuais, uma máquina ultrainteligente poderia projetar máquinas ainda melhores; haveria então certamente uma "explosão de inteligência", e a inteligência humana se tornaria desnecessária. Desse modo, a primeira máquina ultrainteligente é a última invenção que o homem precisará fazer, contanto que a máquina seja dócil o suficiente para nos dizer como mantê-la sob controle".[1]

Atualmente, acompanha-se com apreensão o surgimento de armas autônomas com base na inteligência artificial, com capacidade de tomar decisões, e já imaginamos drones e robôs assassinos nas futuras guerras. A equipe de Turing tinha razão sobre o futuro que estava por vir.

Além disso, o uso da tecnologia na guerra tomou também outro rumo, aquele que não é físico nem visível, o ciberespaço. A Bomba Eletromecânica, outrora comparada à eficiência de uma bomba nuclear, hoje é uma baioneta.

O cenário atual é o de ataques constantes em computadores e redes de dados, cujo fim pode ser atingir infraestruturas críticas, tais como as de energia elétrica, transportes, nuclear, financeira, água; interferir em sistemas eleitorais; invadir privacidades e coisas. A capilaridade de atuação e de danos possíveis de serem causados por esse meio é assustador.

Assim, os mecanismos cibernéticos não só estão sendo utilizados para aperfeiçoar armas e métodos de guerra convencionais, mas

---

[1] GOOD, Irving John. "Speculations Concerning the First Ultraintelligent Machine". In *Advances in Computers*, New York, Academic Press, 1965, p.33.

eles mesmos constituem o próprio terreno de conflito, com cibersoldados e consequências tão difusas e cotidianas que criam dificuldades até mesmo para descrever se a situação é de paz ou de guerra.

O prussiano Carl von Clausewitz, acreditava ser a guerra um misto de paixões, de jogo (e suas probabilidades) e de política, atingindo assim o povo, as forças armadas e o governo. São famosas as suas frases a respeito, tais como: "Para assegurar a paz é preciso se preparar para a guerra" e "A guerra é a continuação da política por outros meios". Isso dito no contexto do Século XIX. Contudo, quando pensamos em uma guerra cibernética do século XXI, o próprio tempo de paz e tempo de guerra estão entrelaçados e a preparação, a defesa e o ataque parecem ser atos simultâneos temporalmente.

No artigo publicado no Jornal do Estado de São Paulo, em 11 de junho de 2019, sob o título: **Guerra Cibernética – O Mundo entrou numa fase de confronto sem frente de batalha e sem regras de engajamento**, o ex-embaixador do Brasil nos Estados Unidos, Rubens Barbosa faz citação do livro *"Cyber. La guerre permanente", de Jean Louis Gergorin e Leo-Isac-Dognin, que conforme o ex-embaixador "retrata de forma simples e direta a nova forma de ver as rivalidades e as estratégias adotadas pelas grandes potências globais. O trabalho procura responder como a emergência do instrumento cibernético se instalou no centro da Guerra permanente e quais são as consequências dessa nova relação de forças."*

Esse quadro nos impulsionou a estudar e averiguar como o Brasil está preparando seus sistemas de controle e sua defesa diante a ciberguerra.

Senador ESPERIDIÃO AMIN

INTRODUÇÃO

Com fundamento na competência do Congresso Nacional de exercer controle externo sobre os demais poderes, prevista no art. 71 da Constituição Federal, combinado com o art. 96-B, do Regimento Interno do Senado Federal, a Comissão de Relações Exteriores e Defesa Nacional (CRE) propôs avaliar a política pública sobre a defesa cibernética no ano de 2019, nos termos do Requerimento nº 24, de 2019-CRE[2].

A Resolução do Senado Federal n° 44, de 2013, prevê que a Casa Legislativa realize a avaliação de políticas públicas, que buscará, entre outras medidas, adequar os dispositivos normativos às necessidades sociais.

Nos termos do art. 1º dessa normativa, "as comissões permanentes selecionarão, na área de sua competência, políticas públicas desenvolvidas no âmbito do Poder Executivo, para serem avaliadas".

Na justificação do Requerimento nº 24-CRE, aprovado dia 9 de maio de 2019, seus autores ressaltam que *o setor cibernético é, ao lado do espacial e do nuclear, setor estratégico para a Defesa do País, o que requer seu fortalecimento, aperfeiçoando dispositivos de segurança e adotando procedimentos que diminuem a vulnerabilidade dos sistemas que possuam suporte de tecnologia da informação e comunicação*.

[2] Ver: https://www25.senado.leg.br/web/atividade/materias/-/materia/136367. Acessado em 09/12/2019.

Este relatório, portanto, pretende refletir a realidade da política pública brasileira pertinente à defesa cibernética, que tanto dista dos demais setores estratégicos, nomeadamente o nuclear e o espacial.

Este relatório está estruturado em seis capítulos. O primeiro capítulo pretende situar quais são os objetivos da política pública de defesa cibernética. Nesse ponto deve se ter ao menos certa clareza de quais são os rumos de um setor de tamanha envergadura que inicialmente se concentrou, e com êxito, na prevenção de danos que poderiam ter ocorrido nos grandes eventos ocorridos no Brasil: Rio+20, Copa do Mundo de Futebol e Olimpíadas. Além disso, é apresentado o quadro institucional brasileiro atual, a partir do que foi definido inicialmente na Estratégia Nacional de Defesa (END). Nesse sentido, há uma reflexão sobre como o Exército e o Ministério da Defesa estão organizados.

O segundo capítulo descreve qual foi o método utilizado para essa avaliação de política pública, enquanto o capítulo terceiro analisa as audiências públicas realizadas.

O quarto capítulo relata a situação orçamentária do setor cibenético, que não é nada alvissareira. Para tal constatação, com as devidas ressalvas, traça-se um paralelo com o orçamento dedicado ao setor nuclear e o cibernético.

Finalmente, em capítulo quinto, são feitas as conclusões e recomendações que se acha convenientes para melhorar nossa defesa cibernética.

1. OBJETIVOS E QUADRO INSTITUCIONAL DA POLÍTICA NACIONAL DE DEFESA CIBERNÉTICA

No Brasil, os assuntos relacionados às vulnerabilidades digitais foram tratados, inicialmente, sob a égide da Segurança da Informação, pelo Decreto nº 3.505/2000, que instituiu a Política de Segurança da Informação.

No âmbito da Defesa, o denominado Setor Cibernético foi destacado pela Estratégia Nacional de Defesa (END), aprovada pelo Decreto nº 6.703/2008, ao lado do setor espacial e do setor nuclear, como um dos três setores considerados estratégicos e essenciais para a Defesa Nacional.

A Diretriz Ministerial nº 014/2009, do Ministério da Defesa, definiu as responsabilidades relativas a cada um desses três setores estratégicos: nuclear, a cargo da Marinha; cibernético, a cargo do Exército; e espacial, a cargo da Aeronáutica. Adicionalmente, determinou providências relativas a objetivos e estratégias setoriais correspondentes a cada Força. Reforçou, ainda, que esses três setores "transcendem, por sua natureza, a divisão entre desenvolvimento e defesa, entre o civil e o militar".

O tema "defesa cibernética" vem sendo tratado pelas Forças Armadas, sob a coordenação do Exército, desde 2010. Nesse período, esforços vêm sendo realizados para incorporar e aplicar capacidades.

Em 2013, um episódio mundial de grande repercussão — a suposta espionagem de agência dos Estados Unidos em vários países — resultou em denúncias de intromissão em assuntos oficiais brasileiros. Como consequência, em 3 de setembro daquele ano, o Senado Federal instaurou uma Comissão Parlamentar de Inquérito (CPI) destinada a "investigar a denúncia de existência de um sistema de espionagem, estruturado pelo

governo dos Estados Unidos, com o objetivo de monitorar e-mails, ligações telefônicas, dados digitais, além de outras formas de captar informações privilegiadas ou protegidas pela Constituição Federal".

Os trabalhos da CPI duraram até abril de 2014, quando foram tomados depoimentos de vários especialistas e de representantes de órgãos públicos ligados às áreas de inteligência e cibernética, tais como o Ministério da Defesa, a Anatel e a Polícia Federal, bem como de representantes daqueles supostos alvos da espionagem norte-americana, a exemplo da Petrobras.

Ainda no contexto do episódio acima apresentado, o Ministério da Defesa criou um Grupo de Trabalho (GT-Ciber), instituído pela Portaria Ministerial nº 2.569-EMCFA/MD, de 6 de setembro de 2013, a fim de elaborar propostas mais imediatas para o campo da Defesa Cibernética.

No relatório apresentado pelo GT-Ciber, que foi aprovado pelo Ministro da Defesa em 13 de março de 2014, constaram medidas para mitigar as vulnerabilidades do ambiente cibernético, incluindo a criação do Comando de Defesa Cibernética (ComDCiber) e da Escola Nacional de Defesa Cibernética (ENaDCiber).

Em 27 de outubro de 2014, a Portaria Normativa nº 2.777/MD definiu a "Diretriz de Implantação de Medidas Visando à Potencialização da Defesa Cibernética Nacional". Coube ao Exército, em articulação com o Estado-Maior Conjunto das Forças Armadas (EMCFA), a Secretaria Geral do Ministério da Defesa (SG/MD) e as demais Forças Armadas, vários encargos, que encerram nossa política nacional atual de defesa cibernética.

O Estado-Maior Conjunto das Forças Armadas (EMCFA) cabe o papel de supervisor, inicialmente da criação do Comando de Defesa

Cibernética (ComDCiber) na Estrutura Regimental do Comando do Exército.

Tal Comando, já instituído, conta com o exercício de militares das três Forças Armadas, cabendo ao EMCFA as atividades de coordenação nos casos de operações conjuntas, especificando-se, em atos próprios, os aspectos inerentes ao controle operacional.

Ademais, coube ao EMCFA a supervisão da criação da Escola Nacional de Defesa Cibernética (ENaDCiber) na Estrutura Regimental do Comando do Exército, também com o exercício de militares das três Forças Armadas.

À Secretaria Geral do Ministério da Defesa (SG/MD) coube providenciar a disponibilização de recursos orçamentários e de pessoal para a viabilização das medidas e para evitar a descontinuidade de projetos, bem como elaborar proposta de criação de infraestruturas de apoio, ao pessoal que compõem os quadros de trabalho do setor cibernético. Ainda, à SG/MD coube enquadrar as tecnologias do setor cibernético dentre as prioritárias no âmbito do Ministério da Defesa.

Por fim, ao Exército Brasileiro, em articulação com o EMCFA, com a SG e com as demais Forças Armadas, foi delegada a grande tarefa. Se o tema nuclear está sob liderança da Marinha e o espacial da Aeronáutica, o cibernético coube ao Exército.

Portanto, o Brasil não criou uma quarta força armada, tampouco um setor separado autônomo ligado ao Ministério da Defesa. É o Exército Brasileiro que foi incumbido de tomar as providências necessárias à ativação do Núcleo do Comando de Defesa Cibernética (NuComDCiber),

subordinado ao Centro de Defesa Cibernética (CDCiber), dotado de pessoal e infraestrutura para os trabalhos de implantação do Comando de Defesa Cibernética (ComDCiber).

Além disso o Exército ativou o Núcleo da Escola Nacional de Defesa Cibernética (NuENaDCiber), subordinado ao Centro de Defesa Cibernética (CDCiber).

Em coordenação com o Estado-Maior Conjunto das Forças Armadas e com a Secretaria-Geral do Ministério da Defesa, coube ao Exército também a criação e a implantação do Comando de Defesa Cibernética e da Escola Nacional de Defesa Cibernética, por evolução dos respectivos núcleos.

Além disso, cabe a ele a organização e execução dos projetos de defesa cibernética, cujos principais são os seguintes:

a) implantação e consolidação do desenvolvimento conjunto de defesa cibernética;

b) implantação e consolidação do Sistema de Homologação e Certificação de Produtos de Defesa Cibernética;

c) apoio à pesquisa e ao desenvolvimento de produtos de defesa cibernética; e

d) a criação do Observatório de Defesa Cibernética.

Como síntese, em 2010, entre outras medidas, o Exército criou o Projeto Estratégico do Exército Defesa Cibernética (PEEDCiber), e em

2014, o Ministério da Defesa criou o Programa da Defesa Cibernética na Defesa Nacional (PDCDN).

Essas iniciativas estratégicas permitiram que entregas importantes contribuíssem para o êxito da Defesa Cibernética nos grandes eventos sediados pelo Brasil, desde a Rio + 20, em 2012, até a Olimpíada de 2016. Além disso, capacidades técnicas foram obtidas e empregadas, propiciando níveis adequados de proteção cibernética aos sistemas utilizados.

Em 2017, foi concluída a regulamentação e implantação do Portfólio Estratégico do Exército (Ptf EE), com a definição de uma metodologia própria para condução dos projetos e programas estratégicos da Força.

Com o fim da série de grandes eventos ocorridos no Brasil e após a implantação do Ptf EE, no contexto do prosseguimento dos trabalhos do Setor Cibernético, o desafio posto pelo Sr Cmt Ex foi a inserção política e estratégica do Setor e a sua estruturação nesses níveis. Trata-se da consolidação do Setor Cibernético, com reflexos e ações demandadas em várias áreas, inclusive nas iniciativas estratégicas que permitem gerir a obtenção das capacidades cibernéticas.

Com o elevado envolvimento do Comando de Defesa Cibernética (ComDCiber) na gestão dessas iniciativas, realizou-se um diagnóstico no sentido de encaminhar o atendimento de demandas, particularmente na vertente operacional. Foram identificadas oportunidades de melhoria na governança e gestão das iniciativas.

Especialmente no Setor Cibernético, vive-se período de ganho exponencial de maturidade no tempo e as circunstâncias evoluem rapidamente, de modo que, no diagnóstico realizado, chegou-se à percepção de que, mesmo sendo recente a implantação do PtfEE, face a evoluções ainda mais recentes, urge adaptar essas iniciativas estratégicas com a finalidade de melhor adequar a governança, a gestão e, por via de consequência, a efetividade dos resultados.

Conforme já relatado, o PDCDN tem o viés conjunto. Por este motivo, o ComDCiber, comando conjunto e órgão central do Sistema Militar de Defesa Cibernética (SMDC), é o principal beneficiado de suas entregas. O PDCDN foi criado pelo Ministério da Defesa (MD), com recursos próprios, para ser gerenciado pelo Exército, com base no Plano de Articulação e Equipamento de Defesa (PAED), com atualização de 16 de outubro de 2014, bem como na Portaria Normativa nº 2.777-MD, de 27 de outubro de 2014, que aprovou a Diretriz de Implantação de Medidas visando à Potencialização da Defesa Cibernética Nacional.

Em linhas gerais, "o PDCDN tem a finalidade de incrementar as atividades de capacitação, doutrina, ciência, tecnologia e inovação, inteligência e operações, no âmbito da Defesa Nacional, por meio de coordenação e integração sistêmica, visando a assegurar, de forma conjunta, o uso efetivo do espaço cibernético (preparo e emprego operacional) pelo Ministério da Defesa e pelas Forças Armadas e impedir ou dificultar sua utilização contra os interesses da Defesa Nacional".

2. METODOLOGIA DE AVALIAÇÃO

A avaliação de política pública proposta pela CRE constitui importante e valioso instrumento para, a partir das análises a serem realizadas, retificar ou ratificar os planejamentos para o futuro do setor cibernético da defesa, que completou uma década, conferindo o aval do Senado Federal aos avanços pretendidos pelas Forças Armadas e, em última análise, em nome da sociedade brasileira.

Diante da relevância e considerando a transversalidade do Setor Cibernético para a defesa do Estado Brasileiro, as perguntas que a presente avaliação de políticas públicas buscará responder são:

1) Como se encontra a implantação das medidas definidas pelo Ministério da Defesa?

2) Quais as transformações e os impactos, positivos e negativos, de sua implementação?

3) Esses instrumentos foram efetivamente implementados ou carecem de plena implementação? Nesse último caso, quais os gargalos a serem desobstruídos?

4) Considerando a evolução da maturidade institucional, a velocidade de eventos e alterações de cenários que caracterizam o Setor Cibernético, as medidas propostas em 2014 são suficientes? Há demandas a serem atendidas para que se obtenha o nível de defesa compatível com os cenários de curto, médio e longo prazos?

5) O que se pretende para o futuro do setor cibernético de defesa?

A fim de responder tais questões, a CRE solicitou informações ao Comando do Exército, por intermédio do ComDCiber, acerca da implantação das medidas indicadas pelo Ministério da Defesa e dos resultados obtidos com as medidas implementadas.

Além disso, foram realizadas visitas técnicas ao ComDCiber, com vistas a identificar gargalos e oportunidades de melhoria.

Em seguida, a considerar a sensibilidade do tema, foi realizada audiência reservada, a fim de identificar vulnerabilidades, com participação do ComDCiber. Evidentemente, não podemos revelar o lá declarado.

Entretanto, duas audiências públicas foram feitas, o que será no próximo capítulo detalhado.

O cronograma proposto no plano de trabalho foi o seguinte:

Atividade	Local	Convidados	Temas
1) Reunião de instalação dos trabalhos	Brasília	- Comando de Defesa Cibernética.	Apresentação e debate do plano de trabalho
2) Reuniões técnicas	Brasília	Senadores e assessorias	Reunião interna: avaliação dos trabalhos e calibragem de cronogramas. Definição de datas para as audiências públicas.
3) Análise orçamentária	Brasília	Consultoria de Orçamentos do Senado (CONORF)	Requerimento à consultoria de orçamento para análise orçamentária do setor.

Atividade	Local	Convidados	Temas
4) Audiência Reservada com Membros da CRE	Brasília	- Ministério da Defesa; - Gabinete de Segurança Institucional da Presidência da República; - Comando do Exército, da Marinha e da Força Aérea; - Ministério das Relações Exteriores; - Ministério da Justiça.	I - Diagnóstico de ameaças sensíveis do setor cibernético e gargalos do Estado para implementar uma política de Defesa Cibernética, com foco: 1) na definição de marcos legais; 2) no fortalecimento da estratégia de superação dos gargalos verificados; II – Avaliação da efetividade de colaboradores nacionais e internacionais, identificando medidas necessárias para a obtenção de resultados.
5) Duas Audiências Públicas	Brasília	1ª) Órgãos públicos: - Ministério da Defesa; - Gabinete de Segurança Institucional da Presidência da República; - Comando do Exército, da Marinha e da Força Aérea. 2ª) Representantes da sociedade civil: - Gerente geral do CERT.BR; - Representantes da ICP-Brasil.	I – Planejamento Estratégico do Setor Cibernético; II – Avaliação do planejamento e da execução orçamentária relacionados ao Setor Cibernético; III – Necessidades e cenários orçamentários relacionados ao Setor Cibernético; IV – Debate sobre a implementação das medidas definidas em 2014 e as frentes de atuação que se delineiam a partir dos resultados já verificados; V – Apontamento das ameaças e as atualizações do cenário do ambiente cibernético.
6) Visitas Técnicas	Brasília	Membros da CRE	I – Identificação das instalações do ComDCiber e ferramentas utilizadas; II – Análise dos gargalos para a implementação das infraestruturas adequadas aos cenários de curto, médio e longo prazos.
Apresentação e Votação do Relatório Final			

3. AUDIÊNCIAS PÚBLICAS

A primeira audiência pública com o fim de debater o Programa de Defesa Cibernética ocorreu no dia 5 de setembro de 2019. Conforme os temas do Item 5 do cronograma do Plano de Trabalho da Avaliação de Políticas Públicas, foram discutidos:

I – Planejamento Estratégico do Setor Cibernético;

II – Avaliação do planejamento e da execução orçamentária relacionados ao Setor Cibernético;

III – Necessidades e cenários orçamentários relacionados ao Setor Cibernético;

IV – Debate sobre a implementação das medidas definidas em 2014 e as frentes de atuação que se delineiam a partir dos resultados já verificados; e,

V – Apontamento das ameaças e as atualizações do cenário do ambiente cibernético.

Participaram dessa audiência as seguintes autoridades:

- Sr. Guido Amin Naves, General de Divisão, Comandante de Defesa Cibernética e representante do Comando do Exército;

- Sra. Luciana Mascarenhas da Costa Marroni, Contra-Almirante, representante do Comando da Marinha do Brasil;

- Sr. Ivan de Sousa Corrêa Filho, General de Brigada, representante do Ministério da Defesa;

- Sr. Arthur Pereira Sabbat, Coronel, representante do Gabinete de Segurança Institucional da Presidência da República – GSI; e

- Sr. Éric Cézzane Cólen, Coronel Aviador, Chefe da Seção de Comando e Controle do Estado-Maior da Aeronáutica (EMAER) e representante do Comando da Aeronáutica.

A seguir relatamos as exposições dos convidados.

1. Sr. Guido Amin Naves

O Sr. Guido Amin Naves, general de divisão, Comandante de Defesa Cibernética e representante do Comando do Exército, iniciou sua apresentação apontando alguns marcos do setor de defesa cibernética no Brasil.

Segundo o expositor, em 2008, a Estratégia Nacional de Defesa estabeleceu os três setores estratégicos para a defesa nacional – nuclear, espacial e cibernético – os quais foram atribuídos, respectivamente, à Marinha, à Aeronáutica e ao Exército, pela Diretriz Ministerial nº 14/2009.

Em seguida, o Exército definiu o Projeto Estratégico de Defesa Cibernética e, em 2010, estabeleceu o núcleo do Centro de Defesa Cibernética, o qual foi ativado em 2012 e é o braço operacional do Comando de Defesa Cibernética (ComDCiber). Em 2012, foi criada a Ação Orçamentária 147F, destinada a prover os recursos necessários ao desenvolvimento dessa capacidade. Nesse momento, a ação contava apenas

com recursos discricionários do Exército, não tendo sido possível o aporte pela Defesa, como já ocorria para os demais setores estratégicos.

Em 2013, diante do emblemático caso Snowden, foi realizada uma CPI no Senado Federal sobre espionagem cibernética e foi formado um grupo de trabalho interministerial capitaneado pela Defesa, que deu origem a uma série de orientações acerca de medidas a serem tomadas para potencializar a defesa nacional no País. Assim, foram criados o Programa de Defesa Cibernética na Defesa Nacional e os núcleos da Escola Nacional de Defesa Cibernética (ENaDCiber) e do Comando de Defesa Cibernética (ComDCiber). Esse último foi ativado em 2016, quando seu primeiro comandante assumiu, sendo o expositor hoje o seu terceiro comandante. Já a Escola foi ativada em 2019.

O general comentou que, nesse ínterim, com a realização de grandes eventos no Brasil, foi preciso obter e aplicar rapidamente capacidades cibernéticas para oferecer proteção adequada aos sistemas empregados nesses grandes acontecimentos mundiais. Mencionou que, na Copa do Mundo de 2014, houve 756 eventos de segurança tratados pela defesa cibernética, sendo que o grupo obteve êxito em não deixar que oferecessem risco.

O convidado reforçou que, ao longo desse período, vivenciaram-se as fases de criação e de implantação, tendo como prioridade a obtenção e aplicação de capacidades cibernéticas, em razão dos grandes eventos. Posteriormente, diante da velocidade com que mudam os cenários na área da cibernética, iniciou-se uma fase de reavaliação, baseada no que ocorreu em 2017, com o caso WannaCry, um *ransomware* que afetou o mundo inteiro. O expositor afirmou que, diante do diagnóstico obtido, conclui-se ser necessário iniciar uma fase de consolidação, antes mesmo de

concluídas as anteriores, com uma nova prioridade de inserção política e estratégica do setor. Ponderou que a inserção política é necessária, uma vez que a defesa cibernética é assunto da Nação como um todo.

O palestrante comentou que, atualmente, o setor está estruturado em quatro níveis: político – com destaque para o Gabinete de Segurança Institucional da Presidência da República (GSI) e a Secretaria de Assuntos Estratégicos – estratégico, operacional e tático. Explicou que, no nível político, fala-se em segurança cibernética, segurança de infraestruturas críticas e proteção cibernética. Nos demais níveis, fala-se em defesa cibernética, a qual engloba três áreas: proteção, exploração e ataque. Ressaltou que a defesa cibernética atua e deve atuar ininterruptamente, não só em momentos de crise.

Em seguida, o general apresentou os dois programas que foram elaborados – o Programa Estratégico do Exército Defesa Cibernética e o Programa da Defesa Cibernética na Defesa Nacional. Com base na Ação Orçamentária 147F, o primeiro, de 2010, é contemplado pelas verbas discricionárias do Exército. O segundo, de 2014, atua com verbas do Ministério da Defesa. Hoje está sendo feito um trabalho de readequação, reavaliação, e reorientação de escopos de ambos os programas.

O palestrante mostrou tabela com dados sobre o Projeto de Lei Orçamentária Anual (PLOA), a Lei Orçamentária Anual (LOA), o Limite Máximo de Empenho (LME), as emendas que foram contempladas e o que foi executado referente aos anos de 2012 a 2019. Concluiu, após a análise dos dados, que há um bom nível de execução dos valores que foram destinados à área em questão. Mencionou, ainda, que muitas foram as entregas já feitas, tais como a ENaDCiber, o ComDCiber, os laboratórios de segurança cibernética em Itaipu. Citou o desenvolvimento, a cargo da Força

Aérea, de um projeto de integração do Centro de Tratamento de Incidentes de Rede das Forças e, a cargo da Marinha, do Sistema de Proteção de Unidades Operativas, pagos pelo programa do Exército de segurança cibernética. Ademais, com relação à capacitação, informou que foram mais de mil cursos já pagos no Brasil e no exterior para capacitar militares, sendo que, em 2019, a ideia da ENaDCiber, juntamente com a Secretaria de Governo e o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), é de capacitar servidores civis, que também precisam ter conhecimento para atuar na proteção dos sistemas corporativos. Por fim, relatou que o Comando mantém interação com outros setores fora da Defesa: projetos de certificação e homologação, levantamento de requisitos, sistema de parceria com o Inmetro, com o Senac, com a Universidade Federal de Pernambuco, entre outros. Na área internacional, participaram do Fórum Ibero-Americano e do maior exercício de proteção cibernética do mundo, realizado no âmbito da Otan, além de terem realizado a segunda edição, este ano, de um exercício de proteção cibernética feito para a proteção das infraestruturas.

Respondendo a questionamentos do Senador Esperidião Amin, o general afirmou, acerca do orçamento, que, entre 2012 e 2016, período em que ocorreram grandes eventos no País, a cibernética estava atrelada a questões tipicamente operacionais. Após esse período, verificou-se a necessidade de se estruturar melhor a demanda e definir um delineamento estratégico para a defesa cibernética no Brasil, o que permitiu o enfoque em questões de orçamento para financiar esse avanço estratégico.

Sobre a questão se seria a cibernética uma quarta arma, o general citou o exemplo da Alemanha, que criou uma quarta força armada, a qual corresponde a um comando informacional e engloba a cibernética. No

seu entendimento, a cibernética é um tema transversal, que atinge inúmeros atores interessados, cada um com a sua linha de comando e subordinação, o que dificulta a governança. É necessário, no seu entender, modernizar a gestão e se desprender da ideia puramente de defesa, estendendo a preocupação também às infraestruturas críticas. Assim, a característica de transversalidade contraindicaria uma solução semelhante à da Alemanha, uma vez que é preciso agregar à cibernética as diferenças de posicionamento que há em todos os atores das Forças Armadas e no âmbito civil.

Em resposta a questionamentos do e-Cidadania, o expositor explicou que, em relação à tecnologia e aos avanços na área de defesa cibernética, há, no Brasil, pesquisa acadêmica; parque industrial, não só em Santa Catarina, mas também o porto digital no Recife e em outras áreas dedicadas à pesquisa; além de empresas da área. Comentou que há avanços importantes em todas as áreas da cibernética e no desenvolvimento de ferramentas nacionais.

Questionado sobre as normas jurídico-legais, mencionou haver a Política Nacional de Defesa Cibernética; a Política Nacional de Segurança da Informação; e, no âmbito militar, a doutrina militar, a defesa cibernética, a estratégia de defesa cibernética. Quanto aos crimes cibernéticos, ressaltou ser difícil diferenciar uma ação de crime cibernético e uma ação que implique uma ofensa à defesa cibernética do País. A investigação, em geral, cabe à Polícia Federal.

Por fim, frisou que a tecnologia brasileira é bastante compatível com as necessidades da defesa cibernética. Ressaltou, ainda, que a transversalidade do tema não ocorre somente no País. Para a defesa cibernética, as fronteiras geográficas não são relevantes, sendo importante haver a interação, não só interna, mas também com as nações irmãs e amigas.

2. Sra. Luciana Mascarenhas da Costa Marroni

A Sra. Luciana Mascarenhas da Costa Marroni, contra-almirante, representante do Comando da Marinha do Brasil, ressaltou que a Marinha tem uma participação de cooperação e colaboração com o ComDCiber, uma vez que o responsável pelo setor estratégico de defesa cibernética é o Exército. Explicou que a Marinha dispõe de proteção para a sua rede, em que é trabalhada toda a sua segurança, e que, até hoje, não houve incidente importante. Relatou que, em 2016, o Centro de Tratamento e Resposta a Incidentes Cibernéticos (CTir) da Marinha foi criado e integrado ao ComDCiber. De acordo com a convidada, a colaboração da Marinha se dá por meio de pessoal e com a troca de informações do CTir com o ComDCiber. Além disso, a Marinha se beneficia dos cursos que o Exército disponibiliza na ENaDCiber.

3. Sr. Ivan de Sousa Corrêa Filho

O Sr. Ivan de Sousa Corrêa Filho, general de brigada, representante do Ministério da Defesa, iniciou sua fala explicando que é o chefe do Centro de Defesa Cibernética, o braço operacional do ComDCiber. De acordo com o general, 90% dos ataques cibernéticos exploram o elo mais fraco, que são as pessoas, os usuários. Assim, no seu entender, as políticas públicas voltadas à garantia de segurança cibernética no País devem priorizar a educação e a conscientização das pessoas, para que adotem medidas para dificultar os ataques, como o *hackeamento* de celulares ou de redes de empresas. Em suma, é necessário o desenvolvimento de uma mentalidade de segurança na população, para que o País tenha mais segurança cibernética.

Por fim, após a apresentação de um vídeo, o convidado mostrou alguns dados sobre o plano plurianual da Defesa, referente à atividade de defesa cibernética.

4. Sr. Éric Cézzane Cólen

O Sr. Éric Cézzane Cólen, coronel aviador, chefe da seção de Comando e Controle do Estado-Maior da Aeronáutica (EMAER) e representante do Comando da Aeronáutica, destacou, de início, que a cibernética se tornou primordial para todas as Forças Armadas. No caso da Força Aérea, que emprega muita tecnologia, ressaltou que há infraestruturas críticas relacionadas ao tema da defesa cibernética. Citou o F-16, uma aeronave utilizada no mundo inteiro e que pode ser vulnerável a ataques cibernéticos. Também mencionou o *Gripen*, que possui vários computadores embarcados trabalhando em rede para que a aeronave funcione; o KC-390, que tem diversos sistemas embarcados; e o satélite brasileiro – Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGDC) – operado pelo Centro de Operações Espaciais (COPE), igualmente sujeito a vulnerabilidades.

Quanto à defesa cibernética, o coronel explicou que a FAB conta com o CTIR FAB, que tem quatro Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR). Ressaltou que existe a perspectiva de se incrementar essa capacidade de defesa cibernética sobretudo relacionada à rede de computadores empregada no sistema de comando e controle, haja vista que, no cenário operacional, há vários sistemas embarcados, diversos dispositivos conectados em rede, satélites, aeronaves, *drones*, sistemas de mísseis, ou seja, sistemas digitais sujeitos a ataques cibernéticos. Mencionou, ademais, que já há uma diretriz de planejamento do Comandante para a criação de um centro de defesa

cibernética a partir da criação e adequação de uma organização militar da Força Aérea. Segundo o convidado, está sendo cunhado um termo ainda não muito claro, a defesa cibernética operacional, com a participação do ComDCiber. Esse centro deve migrar do Sistema de Tecnologia da Informação da Força Aérea para um comando operacional em que haja prontidão para responder às demandas da cibernética.

O coronel destacou que, sendo a cibernética uma arma, o entendimento atual é de que a proteção cibernética deve ser tal qual o trabalho da defesa aérea. Quanto à proteção de sistemas embarcados, frisou ser necessário incrementar muito esse tema, especialmente em relação ao conhecimento, pois se trata de um nicho ainda muito restrito.

Respondendo a perguntas do e-Cidadania, o convidado explicou que o comando da Aeronáutica opera um satélite de forma conjunta, o qual presta serviço para as três Forças. A parte militar das comunicações de suporte ao Governo, em grande parte, se dá por meio desse satélite. Há outras comunicações, principalmente as relacionadas ao sistema de controle de tráfego aéreo, que são terceirizadas para outros satélites. Todavia, as empregadas em operações militares hoje são feitas com o satélite de apoio à defesa, sob controle do comando conjunto. A Sra. Luciana Mascarenhas da Costa Marroni, complementando a resposta, informou que a Marinha, quando apoia a operação de paz da ONU no Líbano, utiliza um satélite, uma constelação Syracuse, disponibilizada pela Otan, na banda X, que é militar. Então, nesse caso, usa-se realmente um satélite estrangeiro, nessa operação específica.

5. Sr. Arthur Pereira Sabbat

O Sr. Arthur Pereira Sabbat, coronel, representante do Gabinete de Segurança Institucional da Presidência da República (GSI), apresentou, inicialmente, dados segundo os quais, em 2018, 54% da população mundial utilizou a internet, o que significa 4,1 bilhões de usuários, sendo que 93% desses acessos se deram por dispositivos móveis. Apontou haver a estimativa de que, até 2020, haverá 30 bilhões de equipamentos classificados como pertencentes à internet das coisas. Em termos de ataques cibernéticos, afirmou serem estimadas perdas anuais da ordem de US$600 bilhões. Em consequência disso, também há a previsão de que o mercado mundial de segurança cibernética até 2020 seja avaliado em US$151 bilhões. De acordo com o palestrante, no Brasil, 100% dos órgãos federais e estaduais utilizam a internet. Cerca de 80% dos domicílios brasileiros, o que significa, aproximadamente, 116 milhões de pessoas, têm acesso à internet, e 98% das empresas brasileiras também utilizam a rede mundial de computadores. Por outro lado, apontou que, segundo relatório da União Internacional de Telecomunicações, o Brasil ocupa o 70º lugar no índice de segurança global, e que, em 2018, cerca de 70 milhões de brasileiros foram vítimas de ilícitos cibernéticos. De 2017 para 2018, houve uma perda para empresas nacionais, em termos financeiros, da ordem de US$20 bilhões. Nesse sentido, o coronel apontou o seguinte quadro atual: o Brasil é o segundo país com maior prejuízo com ataques cibernéticos.

Em seguida, o convidado explicou que o GSI é responsável pela coordenação das atividades de segurança da informação. A atividade de segurança da informação, conforme a Lei 13.844/2019 e o Decreto 9.637/2018, abrange quatro grandes áreas: a segurança cibernética, que é o carro-chefe; a defesa cibernética, que está a cargo do Ministério da Defesa;

a segurança física da informação; e a proteção de dados em termos conceituais, sejam pessoais ou organizacionais.

De acordo com o palestrante, a segurança cibernética possui características que a diferem da defesa. É baseada na prevenção, é ilimitada no tempo e no espaço, tem características de perenidade e visa a elevar o nível de resiliência de sistemas, instituições e da sociedade em geral. Está calcada na proteção, mas não realiza o ataque cibernético, uma vez que o contra-ataque ao ataque cibernético está a cargo da defesa cibernética. Sendo essa uma atividade estratégica, foi criado, em 2006, na estrutura do GSI, o Departamento de Segurança da Informação. Desde 2018, esse departamento viabilizou a publicação de 13 instruções gerais, 22 normas complementares sobre diferentes assuntos de segurança cibernética e da informação, uma estratégia de segurança da informação, e a recente Política Nacional de Segurança da Informação, pelo decreto já citado. Realizou centenas de oficinas, workshops e eventos de sensibilização. Pontuou o convidado que o GSI ainda possui, na estrutura do Departamento de Segurança da Informação, o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR GOV). Trata-se de um dos centros de responsabilidade nacional, é governamental e possui contato com mais de 300 equipes de tratamento de incidentes no Brasil pertencentes aos órgãos dos Três Poderes, a estados, municípios e Distrito Federal, integrando uma rede global composta por 72 centros de outros países. Há, portanto, um monitoramento contínuo dos ataques e dos incidentes cibernéticos contra redes governamentais. A propósito, o coronel apontou que, em 2018, houve cerca de 9.600 incidentes contra redes governamentais, sendo que, em primeiro lugar, foram fraudes, *phishings* e tentativas de invasão. Já em 2019, até o momento, foram cerca de 8 mil incidentes cibernéticos envolvendo redes governamentais, estando em primeiro lugar os vazamentos. Esses dados

chamam a atenção diante da preocupação dos órgãos públicos a respeito da Lei Geral de Proteção de Dados Pessoais, uma vez que um dos pilares é a proteção dos dados pessoais, especialmente contra ilícitos cibernéticos, com atenção especial para o vazamento. Dessa forma, o palestrante afirmou que estão sendo feitas ações de sensibilização para que essa lei, que representa uma quebra de paradigma no modo como são tratados os dados pessoais, seja incorporada e possa ser utilizada em plenitude pelos órgãos públicos, além de estarem sendo emitidos alertas, recomendações e estatísticas sobre incidentes cibernéticos.

Sobre as iniciativas e projetos em andamento, o Sr. Arthur Pereira Sabbat apontou que, em 2018, foi publicado o decreto que institui a Política Nacional de Segurança da Informação, que tem servido, por sua ênfase na governança, como fonte de inspiração para organizações públicas e privadas. Em 2019, foi reativado o Comitê Gestor de Segurança da Informação, órgão cuja finalidade é deliberar sobre assuntos de segurança da informação, inclusive cibernética. Em breve, deverá ser colocada em consulta pública a Estratégia Nacional de Segurança Cibernética, construída com a participação de mais de 40 representantes de órgãos dos setores público e privado, representantes das infraestruturas críticas nacionais, representantes do meio acadêmico e de outros personagens icônicos da sociedade de notório saber. De acordo com o palestrante, tal estratégia é pragmática e está calcada em sete eixos: proteção e segurança; universo conectado seguro; proteções estratégicas; dimensões normativas; pesquisa, desenvolvimento e inovação; dimensões internacionais e parcerias estratégicas; além de abordar o ramo educacional.

Por fim, o palestrante informou ser intenção do GSI, ainda este ano, elaborar um projeto de lei geral de segurança cibernética, que traga um

alinhamento macropolítico e estratégico para todas as ações de segurança cibernética no País. Para a concepção desse projeto, foram estudados modelos de vários países, como Estados Unidos, Reino Unido, Portugal, França, Coreia do Sul, Japão, Rússia e outros.

.....

A segunda audiência Pública ocorreu no dia 26 de setembro de 2019, completando o objetivo do item 5 do cronograma do Plano de Trabalho da Avaliação de Políticas Públicas.

Os participantes dessa segunda audiência pública foram os seguintes:

1. Sr. Fabio Reis Cortes, gerente de Arquitetura e Segurança de Tecnologia da Informação do Operador Nacional do Sistema Elétrico (ONS);

2. Sr. Marcelo Buz, diretor-presidente do Instituto Nacional de Tecnologia da Informação (ITI);

3. Sr. Ricardo Felipe Custódio, professor-supervisor do Laboratório em Segurança da Computação da Universidade Federal de Santa Catarina (LabSEC/UFSC);

4. Sr. Marcos Allemand Lopes, gerente de Departamento de Gestão da Segurança da Informação e da Continuidade de Negócios do Serviço Federal de Processamento de Dados (Serpro);

5. Sra. Cristine Hoepers, Gerente geral do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br)

6. Sr. Márcio da Silva Nunes, vice-presidente da Associação Nacional de Certificação Digital (ANCD);

7. Sr. Ilton Duccini, Diretor de Segurança Digital na Empresa Telefônica Brasil e Professor da Universidade Estadual de Campinas (Unicamp); e,

8. Sr. Eduardo Bergo, Diretor Setorial da Comissão Executiva de Segurança Cibernética da Febraban, junto ao Banco do Brasil.

A seguir relatamos a exposição dos convidados.

1. Sr. Fabio Reis Cortes

O Sr. Fabio Reis Cortes lembrou que os desafios da segurança cibernética consistem em prevenir ataques que comprometam a operação do negócio, além de detectar vulnerabilidades e ameaças, buscando identificar invasões e responder aos incidentes.

O setor elétrico, principalmente os operadores de sistemas elétricos no mundo, tem trabalhado com o conceito de resiliência cibernética, que significa a capacidade de antecipar, preparar, responder e adaptar-se não só a pequenos eventos do dia-a-dia, mas também a incidentes severos, ligados ou não a ataques cibernéticos. Para tanto, é importante o investimento em tecnologia – equipamentos, softwares, sistemas –, para detectar e bloquear ameaças e invasões, sempre com foco nos processos e nas pessoas.

Na área de prevenção, resposta e detecção, há quatro conjuntos de iniciativas importantes, que são: gestão interna das empresas; conscientização das pessoas sobre o tema e sobre como agir no ambiente conectado; evolução contínua; e colaboração do setor, com compartilhamento de informações e experiências, ação que talvez seja a mais relevante de todas. O ONS utiliza todas as tecnologias disponíveis, tais como, firewall, anti-spam, filtro de conteúdo, aplicação de patches de correção, VPN's, one-time password (OTP), senhas de uso único e específico, entre outras. Citou também processos e tecnologias de análise de vulnerabilidades, monitoramento de segurança, inteligência, correlação de eventos, inteligência artificial, ethical hacking, simulações e exercícios de invasão.

No âmbito da conscientização, as ações visam a criar uma cultura de segurança da informação nas empresas e organizações, seja por simulações de phishing, seja por campanhas mais objetivas.

Quanto à colaboração, eles procuram estabelecer relação estratégica com entidades comprometidas com segurança cibernética, dentro do setor elétrico, envolvendo o Governo e países que tenham relações com o Brasil, ou mesmo empresas e setores estrangeiros que se relacionam com as organizações do ONS. Citou, então, colaboração com o Comando de Defesa Cibernética (ComDCiber), que culminou este ano com a participação do setor elétrico no evento Guardião Cibernético 2.0, com a presença de mais de duzentas pessoas e mais de quarenta empresas. Disse que o compartilhamento de informações e experiências foi bastante válido.

Em seguida, comentou iniciativas recentes, no setor elétrico, como a participação do ONS no evento "Brazil Cyber Defence Summit", promovido pelas Forças Armadas, no qual foram apresentados os resultados

do 1º Exercício Guardião Cibernético. Também esteve presente no primeiro Colóquio Técnico de Segurança Cibernética para o Sistema Elétrico, produzido pela Abrage (Associação dos Geradores de Energia) e pela Itaipu Binacional e no I Workshop de Segurança Cibernética, promovido pelo Cigré-Brasil. Além disso, a Abrate, associação das transmissoras de energia, desenvolveu proposta de framework de segurança cibernética para seus associados; a CIER, Comissão de Integração Energética Regional, promoveu em Montevidéu grupo de trabalho sobre segurança cibernética no setor elétrico da América Latina, apresentando também um projeto em conjunto com o BID sobre esse tema. Este ano, houve a realização do Guardião Cibernético 2.0, que envolveu os setores nuclear e financeiro e, em junho, o ONS promoveu Seminário sobre Segurança Cibernética especificamente para Operação do Sistema Interligado Nacional, com participação de entidades governamentais, academia e agentes do setor elétrico.

Por fim, o palestrante disse que o ONS, os agentes e a Aneel estão trabalhando para estabelecer, dentro dos procedimentos de rede, requisitos e controles mínimos para a segurança cibernética na operação das instalações.

2. Sr. Marcelo Buz

O Sr. Marcelo Buz informou que o Instituto Nacional de Tecnologia da Informação - ITI é a Autoridade Certificadora Raiz da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, vinculado à Casa Civil da Presidência da República e responsável por desenvolver as criptografias necessárias para as assinaturas digitais.

Disse que, por ser de 2002, não atingir todos os segmentos da sociedade e possuir amarras tecnológicas que impedem o progresso digital,

a lei que instituiu a ICP-Brasil e transformou o ITI em autarquia não é adequada para os dias de hoje.

Informou também que o ITI possui corpo técnico oriundo das mais variadas instituições e órgãos deste País, como a Agência Brasileira de Inteligência, o Exército, a Polícia Federal (PF), entre outros, pois nunca fez concurso público e se vale da prerrogativa da requisição.

O Instituto executa as políticas de certificação digital, administra o credenciamento dos entes, autoridades certificadoras e de registro e ainda fomenta e cria padrões de assinaturas digitais no Brasil. Além disso, fiscaliza e audita mais de nove mil entidades. A criptografia do ITI para os artefatos das coisas é a E-521, uma das mais seguras.

Fisicamente, a Autoridade Certificadora Raiz - AC-Raiz fica na Presidência da República e é uma sala-cofre, com os mais altos níveis de segurança.

A ICP-Brasil é composta por dezessete autoridades certificadoras de primeiro nível, normativas, sendo a Receita Federal a principal delas. O sigilo fiscal do brasileiro, no que tange ao relacionamento do cidadão para com a Receita Federal, é garantido por ela. O palestrante informou, que, no dia anterior, o ITI assinou protocolo de intenções com o Inmetro, que passou a se credenciar também como autoridade certificadora de primeiro nível.

Além disso, possui 97 autoridades certificadoras de segundo nível e nove autoridades de carimbo de tempo. Com a instalação de dois relógios de césio, o Instituto está se credenciando para ser membro da UTC

– Tempo Universal Coordenado e poder carimbar o tempo em que os certificados transacionam no mundo digital.

Há ainda mais de 1200 autoridades de registro que, na ponta do processo, certificam a criptografia, para não correr risco de falsas pessoas acessarem os sistemas, principalmente em épocas em que há convergência desses serviços para portais únicos, e em que processos e documentos tramitam em meio digital. Existem também 44 prestadores de serviço de suporte, 6 prestadores de serviço biométrico e 4 prestadores de serviço de confiança, estes responsáveis por endereçarem as informações para a nuvem, o que permite ter o certificado digital no celular. Como os PSBios são interoperáveis, toda autoridade de registro passa a ter acesso às informações uma das outras de forma criptografada, o que nos permite garantir que uma pessoa não passe dentro do ICP-Brasil por dois CPFs. Se porventura isso ocorrer, a conduta padrão é revogar ambos os certificados digitais.

Atualmente, o ITI está chegando a oito milhões de certificados digitais, numa população de aproximadamente 210 milhões de pessoas. Disse que é necessário procurar meios de facilitar o certificado digital, de forma que todo cidadão economicamente ativo tenha acesso à plena segurança e direito à legítima defesa cibernética.

Destacou que a autoridade gestora da ICP-Brasil é o Comitê Gestor, responsável pela regulamentação e normatização e formado tanto pelo Estado quanto pela iniciativa privada.

A ICP-Brasil é a única infraestrutura que assegura plena validade jurídica a atos e negócios eletrônicos. Garante autenticidade, não-repúdio, integridade e confidencialidade, vale dizer, certifica que o usuário é de fato quem alega ser, impossibilita a negação de autoria, garante que os

dados não podem ser modificados sem autorização e protege-os contra acesso não autorizado.

Disse que, no mundo de hoje, não há mais espaço para discussões sobre dar integridade e autenticidade, por força de lei, a login e senha, pois a alta probabilidade de invasão dos computadores e das bases de dados por hackers, para interceptação de dados, torna esse sistema vulnerável. Defesa cibernética só é alcançada com criptografia de dados, ciência com a qual o ITI trabalha.

Colocou então o Instituto à disposição do Congresso para encontrar soluções que busquem aumentar a segurança cibernética do País, atual e futura.

3. Sr. Ricardo Felipe Custódio

O Sr. Ricardo Felipe Custódio fez um breve histórico sobre a internet, para mostrar o porquê da preocupação com uma Política Nacional de Defesa Cibernética.

Lembrou que os computadores surgiram em 1950, que começaram a ser interligados quando a internet foi inventada em 1969, e que o primeiro vírus surgiu em 1971. Em 1975, foi criada a assinatura digital, ferramenta concebida para dar segurança aos documentos eletrônicos. Em 1994, a internet chegou ao Brasil, e, em 2000, surgiram as redes sociais.

A criação da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), por vontade da Organização das Nações Unidas, ocorreu em 2001, pela Medida Provisória nº 2.200. Em 2010, aconteceram os primeiros ataques cibernéticos de um país contra o outro, ou de uma empresa contra a

outra. Em 2011, foi criado, no Brasil, o Centro de Defesa Cibernética do Exército, a partir da Estratégia Nacional de Defesa.

Em 2013, Snowden provou para o mundo que existia guerra cibernética e que as redes do mundo inteiro estavam sendo vigiadas pelo governo americano, inclusive as do Brasil. Para agravar a questão, o País, à época, tinha padrões de criptografia baseados em normas controladas pela agência de segurança americana, a NSA.

Em 2014, foi implantada a Política Nacional de Defesa Cibernética. Em 2019, houve redirecionamento do ITI, com implementação de mudanças positivas, mas destacou que considera necessário avançar mais.

Segundo ele, é importante coordenar iniciativas das diversas entidades, empresas e órgãos do Governo que trabalham com políticas de segurança cibernética, bem como avaliar a necessidade de criar ou não um novo marco regulatório.

O País tem vários desafios pela frente. Inicialmente, é necessário criar âncoras de confiança do mundo cibernético e fazer como alguns países na Europa, que publicam constantemente a lista de serviços eletrônicos confiáveis. Atualmente, no Brasil, não há esse controle; o povo brasileiro não sabe no que pode confiar. Hoje, se uma empresa americana quiser, basta revogar os certificados raiz das ACs que emitem os certificados digitais dos bancos brasileiros, para desativar o sistema bancário nacional.

Também precisa criar um barramento de Nação, para a integração dos sistemas de informação, como existe em vários países, e conceber padrões de interoperabilidade, se não semântica, ao menos

sintática, para permitir que as aplicações se comuniquem e que a defesa cibernética do sistema de informação seja possível.

Destacou que, apesar da iniciativa do ITI de ter um relógio atômico e com isso possibilitar que certificados digitais sejam emitidos nas datas corretas, há que se cuidar melhor dele.

Elogiou a iniciativa da Abin de criar um chip para fazer a geração confiável de números aleatórios, o que é necessário para a segurança da informação, mas frisou que não há muito acesso a isso no País.

A nação tem que se preparar para fazer a defesa cibernética em um ambiente de tecnologia 5G, realidade em alguns países, que permite a rápida comunicação dos equipamentos e sistemas.

Disse que, ao menos em alguns pequenos sistemas, é importante que o Brasil tenha o domínio tecnológico para criar chips, circuitos integrados e equipamentos de hardware, para serem colocados em pontos estratégicos, principalmente em ambientes de infraestrutura crítica. Isso daria ao País controle cibernético em pontos nevrálgicos.

Por fim, disse que o Brasil deve se preparar para a chegada da computação quântica, prevista para 2035, que vai quebrar toda a criptografia que existe hoje, RCA, curva elíptica, entre outros. Citou os Estados Unidos, onde o Nist (National Institute of Standards and Technology) está criando padrões de assinatura digital, protocolos de acordo de chave e padrões de comunicação quânticos, tanto usando técnicas de criptografia pós-quântica quanto algoritmos quânticos.

4. Sr. Marcos Allemand Lopes

O Sr. Marcos Allemand Lopes falou sobre o papel do Serpro como colaborador do governo federal na área de segurança, desde a instituição da Política de Segurança da Informação da Administração Pública Federal, em 2000, até os dias de hoje, ressaltando a importância da confiança e da colaboração na área de defesa cibernética.

O Serpro participou da criação do Departamento de Segurança da Informação e Comunicação, hoje DSI; incentivou a criação da ICP Brasil; colaborou na criação do CTIR Gov; na elaboração de diversas normas complementares; em ações de conscientização em segurança para a Polícia Federal, em conjunto com o Comando do Exército e o da Marinha; e, além disso, em um curso de pós-graduação na UnB, para quarenta pessoas, com foco em gestão de segurança. O próprio DSI depois montou mais seis turmas sobre esse tema, todas na UnB, sendo três a distância.

Mais recentemente, em colaboração mais próxima com o então Centro de Defesa Cibernética (CDCiber) do Exército Brasileiro – mais tarde Comando de Defesa Cibernética (Com D Ciber), o Serpro participou da Rio+20. Houve várias reuniões de planejamento, ações operacionais conjuntas, reuniões de avaliação pós ação, o que culminou, em 2014, com a assinatura de acordo de cooperação com esse Centro, para troca de conhecimento em tecnologia da informação.

Em 2006, juntamente com o Departamento de Segurança de Informação (DSIC), o Serpro elaborou um guia de referência para a segurança das infraes.truturas críticas. A empresa também participa de grupo de trabalho, há bastante tempo, no Departamento de Assuntos de Defesa Nacional, voltado para segurança da infraestrutura crítica e de finanças, em

razão da interação com sistemas que desenvolve e produz, como o Siafi, que serve ao Tesouro Nacional e à Receita Federal.

Recentemente, colaborou na elaboração da Política Nacional de Segurança das Infraestruturas Críticas, estabelecida pelo Decreto nº 9.573/2018, e que está sendo desdobrada na Estratégia Nacional de Segurança das Infraestruturas Crítica – em consulta pública até 2 de outubro; da mesma forma, na criação da Política Nacional de Segurança da Informação, prevista pelo Decreto nº 9.637/2018, e dos exercícios cibernéticos, Guardião I e Guardião II, em 2018 e 2019, respectivamente.

Destacou, então, pontos que considera fundamentais na questão da segurança cibernética, sem os quais não se consegue dar respostas adequadas e efetivas. Citou primeiramente capacitação, confiança e colaboração. Lembrou, então, da importância não só de cada setor se organizar, ter seus processos definidos, dentro de uma coordenação setorial, mas também de haver uma coordenação nacional entre os setores, para intercâmbio de saberes. Em seguida, enfatizou a necessidade de infraestrutura adequada e atualizada, e ações preventivas e reativas, dentro do conceito de resiliência das infraestruturas críticas.

5. Sra. Cristine Hoepers

A Sra. Cristine Hoepers informou que trabalha há vinte anos no Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), criado em 1997 por recomendação do Comitê Gestor da Internet no Brasil, que diagnosticou necessidade de aumentar os níveis de segurança da rede nacional.

Antes de falar de ameaças e do cenário cibernético brasileiro, comentou que a internet no País é uma das maiores do mundo, com quase 70% das redes autônomas da América Latina e do Caribe e mais de 6 mil provedores de acesso, sendo que 75% deles têm mil clientes ou menos. O ponto de interconexão de tráfego de São Paulo é o terceiro maior no mundo, sendo o primeiro em número de participantes, com mais de 1700 redes autônomas. Lembrou que o segundo maior é o de Amsterdã, com apenas 800 membros.

Falou da importância de se pensar, não só na segurança das empresas, mas também na do cidadão, pois 70% da população brasileira é usuária da internet e 97% dos acessos à rede se dá via telefones móveis; somente 43%, via computador. Os negócios e o acesso a serviços do governo eletrônico estão migrando para celulares. Para agravar, as empresas têm política diferente para a região da América Latina; vendem aparelhos de baixo custo e não os atualizam quanto à segurança. A população está vulnerável.

A Internet das Coisas (IoT), diferentemente do que se acredita, não é um problema futuro, mas atual. O CERT.br tem acompanhado os ataques tanto em notificações de incidentes quanto na própria rede de sensores, todos com algum componente da IoT. São os mais diversos tipos: mineração de criptomoedas, ataques a terceiros, fraudes de negação de serviço. A maior parte das negações de serviço que saem de redes brasileiras está sendo feita via câmeras de TV, roteadores de banda larga, smart TVs, smartphones; e as tentativas de fraudes contra o cidadão também são muito prevalentes via e-mails falsos ou de infecção dos dispositivos, e isso está migrando para celulares.

Esse universo, complexo e interdependente, pode ser representado por uma pirâmide, em cuja base estão os profissionais que desenvolvem sistemas, na maioria inseguros. Ferramentas de segurança só são inseridas dois níveis acima pelos encarregados da segurança cibernética, que tentam remendar os erros que vêm debaixo. A área de tratamento de incidentes, em que atua, depende de todas para ser efetiva e quanto mais no topo, mais exigência de qualificação e menos mão de obra disponível.

A melhora do cenário depende de cada ator fazer sua parte. A postura dos profissionais precisa mudar e, para tal, é necessário envolver a Sociedade Brasileira de Computação e repensar os currículos das universidades; mudar a métrica demandada pelo Capes e pelo CNPq por uma mais segura; modificar o sistema de incentivos para que sejam exigidos requisitos mínimos de segurança no desenvolvimento de programas e hardwares; profissionais com conhecimentos sólidos sobre protocolos de internet, e passar a certificar processos e não softwares. É necessário haver boas práticas globais, desde a base da pirâmide, que aumentem a segurança e mantenham a interoperabilidade, essencial para a inovação.

Para que a segurança cibernética seja efetiva, os sistemas devem ser mais seguros, o ambiente, bem projetado, e deve haver cooperação de todos os profissionais de tecnologia da informação, além da de gestores e usuários. É impossível um ambiente 100% seguro, mas deve-se proteger o que for mais crítico, além de conscientizar e educar usuários e profissionais.

O foco do CERT.br, que atua na área de Tratamento de Incidentes, tem sido aumentar os níveis de segurança e resiliência das redes brasileiras, fomentar a criação de CSIRTs (Grupos de Tratamento de Incidentes), treinar profissionais na área, criar massa crítica para uma comunidade nacional ativa e influenciar padrões globais.

A defesa cibernética, que fica no topo da pirâmide, coleta inteligência sobre ataques vindos de outras nações e dedica recursos para estudar vetores de ameaças de baixa probabilidade, mas altíssimo impacto. No entanto, a eficácia de suas ações depende da cooperação de todos, pois nenhum grupo ou estrutura resolverá o problema sozinho. A segurança do sistema todo começa nas "pontas" e depende de software seguro, redes resilientes, além de usuários e empresas alertas, com antivírus instalado.

O Núcleo de Informação e Coordenação do Ponto BR (NIC.br) e o Comitê Gestor da Internet no Brasil atuam mais nas três áreas centrais da pirâmide, quais sejam, segurança na administração de sistemas, segurança cibernética e tratamento de incidentes. Visam a construir uma internet mais saudável, cuja estabilidade, segurança e funcionalidade globais sejam preservadas de forma ativa, por meio de medidas técnicas compatíveis com os padrões internacionais e do estímulo ao uso das boas práticas.

Disse que o CERT.br está implementando o Programa Internet Mais Segura, iniciativa conjunta de várias associações de provedores e de indústrias de software e hardware, cujo objetivo consiste em criar uma cultura de segurança. Seus profissionais, entre outras ações, participam de reuniões regionais de provedores de acesso e atuam junto a universidades para dar treinamento em boas práticas. Além disso, produzem material educativo de uso livre, direcionado para crianças, adultos, inclusive terceira idade, escolas e empresa, muitos já sendo utilizados.

6. Sr. Márcio da Silva Nunes

O Sr. Márcio da Silva Nunes disse que a Associação Nacional de Certificação Digital (ANCD) é uma associação civil sem fins lucrativos, com sete empresas associadas, que operam três infraestruturas completas de

chaves públicas. São centenas de profissionais de desenvolvimento de softwares de segurança da informação, que trabalham para manter os padrões de funcionamento e garantir que a inovação tecnológica não se torne gatilho de crescimento de vulnerabilidades.

Os objetivos da ANCD consistem em fortalecer o Sistema Nacional de Certificação Digital; promover o uso dos certificados digitais; a conscientizar a população sobre sua importância; desenvolver, evoluir e apoiar padrões; e promover a interoperabilidade.

Os desafios são constantes e crescem a cada dia; a guerra cibernética é silenciosa; as tecnologias, disruptivas. Tudo está mudando. Sabe-se que 65% das crianças que estão hoje no primeiro ano da escola irão trabalhar em atividades que ainda não existem. Vale lembrar que a tecnologia moderna rapidamente se populariza, o que também significa problema, pois princípios importantes de segurança da informação precisam ser inseridos na cultura dos usuários.

Nos últimos 150 mil anos, o desenvolvimento humano se deu de forma local e linear, hoje é exponencial e global. O que existia há 20 anos em tecnologia pode ser encontrado no celular, hoje, e com muito maior capacidade de processamento. A todo tempo, em qualquer lugar, há um software novo, um ataque novo; por isso a importância da resiliência das tecnologias de infraestrutura e das ações de prevenção.

Inovações impactam as estratégias de competitividade das empresas, o desenvolvimento de negócios, a própria tecnologia, as pessoas no seu dia a dia e a sociedade por inteiro. O homem começa a falar em como ir para outros planetas e usa a inteligência artificial cada vez mais intensamente, quer seja para ataque ou para defesa; as assistentes virtuais

com capacidade de se passar por pessoas são realidade; a impressão 3D permite criação de componentes tanto para o bem quanto para o mal; a longevidade das pessoas está aumentando, o que significa que haverá mais pessoas, com mais ou menos cultura digital, lidando diariamente com tecnologias novas e disponíveis; a economia compartilhada permite que várias pessoas, em várias partes do mundo, desenvolvam tecnologia juntas, com boas ou más intenções, haja vista a Deep Web; as cidades se tornarão mais inteligentes, na combinação de tecnologias hardwares e softwares. Tudo isso são elementos suscetíveis a ataques.

Neste mundo imerso em softwares, os programas de computação devem equilibrar conveniência e segurança, pois segurança demais é inconveniente e conveniência demais fragiliza a segurança.

Inúmeros sistemas e aplicações fazem uso de certificados digitais emitidos pela ICP-Brasil, fundamentais para o processo de modernização dos serviços públicos e da atribuição de segurança das transações eletrônicas. Citou, entre outros, o SPED – Sistema Público de Escrituração Digital; o DIPJ – Declaração de Rendimentos da Pessoa Jurídica; SPB – Sistema de Pagamento Brasileiro; o FGTS Conectividade Social; o passaporte eletrônico.

A certificação digital não só dificulta ataques cibernéticos, mas também garante autenticidade em termos de autoria do documento, integridade sobre a informação, interoperabilidade e baixa dependência sistêmica, devido ao uso de padrões. Também reduz índices de fraudes e permite maior rastreabilidade, o que ajuda a detectar ataques e a criar melhores políticas de proteção aos dados.

A segurança da informação deveria fazer parte do currículo escolar, de forma a se criar uma cultura nessa área.

Por fim, o palestrante ressaltou que o Brasil precisa se preparar para a revolução da computação quântica e citou Peter Drucker, segundo o qual, "planejamento de longo prazo não lida com decisões futuras, mas com o futuro das decisões presentes".

7. Sr. Ilton Duccini

O Sr. Ilton Duccini disse que o desenvolvimento de tecnologia voltada para segurança cibernética se, por um lado, requer grandes investimentos, por outro pode ser fonte de dividendos para o País. Tem acompanhado empresas e empreendedores brasileiros que começam a vender tecnologias desenvolvidas por eles para países da América Latina. Vê nesse nicho uma grande oportunidade de negócios.

O conceito de guerra cibernética evoluiu e não significa mais uma nação contra a outra. Há grupos de cibercriminosos ou mesmo atores individuais capazes de causar grandes estragos ao sistema de internet de um país, que vão além de vazamento de dados ou bloqueio de um sistema. A maior preocupação do diretor responsável pela agência de inteligência americana consiste no rompimento da cadeia de integridade de informações, com manipulação e adulteração de dados, de tal forma que seja muito difícil identificar o ponto em que isso ocorreu para reverter os danos.

O palestrante então apresentou gráfico que mostra panorama histórico dos casos de guerra cibernética no mundo. O primeiro deles aconteceu na Estônia, em 2007, e deu origem ao Centro de Excelência em Defesa Cibernética da Otan, o CCDCOE. O mais conhecido, o caso de

Stuxnet, em 2010, quase colapsou toda indústria nuclear iraniana, após um malware afetar o sensor de temperatura dos geradores de enriquecimento de urânio de algumas centrífugas daquele País. Entre outros, citou a Operação Cast Lead, em 2008; a Operação Aurora em 2009, a Operação Dust Storm, em 2010; o ataque à empresa Sony, em 2014.

Com o intuito de se preparar para uma guerra dessa natureza, o Brasil deve elaborar uma Estratégia de Segurança Cibernética que vá além do proposto pela Estratégia Nacional de Defesa. É necessário complementá-la com ações reais que envolvam patrocínio estatal para o desenvolvimento de tecnologias, mudanças na Política Nacional de Segurança da Informação, de forma a abarcar também entidades privadas, e regulamentações robustas que incluam setores de infraestruturas críticas, como o financeiro, o nuclear, o bancário e o de telecomunicações. Deve definir prioridades de investimento; mapear riscos, não só para o Governo e Forças Armadas, mas também para a iniciativa pública e a privada; promover a articulação entre Academia, Forças Armadas, setor público e setor privado, de forma a conceber um currículo da cibersegurança no Brasil; e criar um ecossistema de colaboração e cooperação que extrapole fronteiras.

Por fim, o palestrante elogiou as iniciativas governamentais de criação da Escola Nacional de Defesa Cibernética e a realização do Exercício do Guardião Cibernético, que colocou em prática o princípio de um ecossistema colaborativo entre os setores de infraestruturas críticas.

8. Sr. Eduardo Bergo

O Sr. Eduardo Bergo informou que o quadro associativo da Febraban conta com 119 instituições financeiras associadas, que representam

28% dos ativos financeiros do País, sendo 97% dos ativos totais de todas as instituições bancárias brasileiras.

Mencionou dados do setor para demostrar o crescimento, da ordem de 33%, do volume de transações bancárias, com movimentação financeira, nos canais digitais nos últimos anos; nas operações feitas por celular o avanço foi de 80%. Apontou algumas leis e decretos que regulam a atuação dos bancos no País, como a Resolução nº 4.658, de 26 de abril de 2018, do Conselho Monetário Nacional, e a Instrução nº 612, de 22 de agosto de 2019, da Comissão de Valores Imobiliários, além da Lei Geral de Proteção de Dados, de 14 de agosto de 2019, que passará a vigorar em 2020.

Segurança cibernética para os bancos é crucial. O cofre digital é mais importante que o cofre físico. As principais ameaças que enfrentam são a engenharia social, ou seja, alguém tentando obter credenciais de outra pessoa; malware, ransomwares; hacking; defacement; e Ataque Distribuído de Negação de Serviço.

Mencionou ataques cibernéticos recentes, como o sofrido pelo Yahoo, em 2016; pelo Facebook e Cambridge Analytica, também em 2016; pela Equifax, em 2017; e pela rede de hotéis Marriott, em 2018. Bancos no Peru, no Chile e no Equador também foram alvos recentemente.

Existe uma Comissão de Segurança Cibernética, composta por diretores de bancos, encarregada do planejamento estratégico de cibersegurança do setor bancário. O investimento do setor bancário, no Brasil, nessa área, equivale ao do governo brasileiro e é o segundo maior do mundo.

Citou alguns exemplos de soluções e processos de segurança adotados pela área de Inteligência e Segurança Cibernética dos bancos, como: proteções específicas; dados, monitoramento e feeds; acesso, identidade e criptografia; segurança de redes; endpoints e estações de trabalho; e testes de vulnerabilidade. Além disso, eles investem em tecnologia voltada para a segurança do cliente, tais como, a utilização de QR Code, tokens, cartão com chip, uso de biometria.

As instituições bancárias também têm feito parcerias. A que surgiu entre Caixa Econômica Federal e Polícia Federal (PF), para investigação de fraudes bancárias, em 2009, chamada de Projeto Tentáculos, evoluiu. Em agosto deste ano, a Febraban acatou pedido da PF de estender o acordo de cooperação para a Secretaria de Operações Integradas do Ministério da Justiça, para encaminhamento de investigações para a Polícia Civil. A partir de agora, Febraban, Bancos e PF trabalharão conjuntamente na definição das diretrizes deste acordo.

Há projetos em andamento, que demandam investimentos pesados, como o Sistema Financeiro Aberto (Open Banking) e a implementação de pagamentos instantâneos. Além disso, a Febraban está estruturando um plano estratégico, no âmbito de sua Comissão Executiva, que abrange implementação de laboratório de segurança cibernética, organização de exercícios integrados de resiliência, implementação de um centro de formação de profissionais e criação de baseline de cyber para endereçar segurança em nuvens, terceiros e infraestrutura crítica.

Elogiou o evento Guardião Cibernético 2.0, iniciativa do CDCiber, apoiado pelas instituições financeiras.

Disse que a Febraban defende a instituição de uma política nacional de segurança que inclua o setor financeiro, em linha com as regulamentações do Bacen, CVM e da Lei Geral de Proteção de Dados; que implemente um documento único nacional e digital, com certificação embutida; que reforce a importância de estruturas especializadas para investigação de crimes cibernéticos; e, por fim, que apoie não só a criação de academias voltadas para formação de profissionais especializados, mas também a implementação de testes integrados de resiliência cibernética.

4. A PDCDN NO ORÇAMENTO FEDERAL

Em termos orçamentários, o Programa de Defesa Cibernética da Defesa Nacional - PDCDN conta com a Ação Orçamentária 147F (Implantação do Sistema de Defesa Cibernética para a Defesa Nacional), por intermédio do Plano Orçamentário nº 2 (PO 0002).

O Descritor da Ação 147F tem o seguinte escopo:

> *Implantação de Sistema de Defesa Cibernética para ampliar a capacidade do País de atuar com liberdade de ação, a fim de elevar o nível de segurança da informação e das comunicações, assim como a capacidade de defesa nas esferas civil, industrial e militar para atuação em ataques de natureza cibernética.*

Esse plano orçamentário envolve:

- Aquisição do material de suporte;

- Desenvolvimento de sistemas;

- Aquisição e instalação de equipamentos de Tecnologia da Informação e Comunicações (TIC) e de Segurança da Informação e Comunicações (SIC);

- Aquisição, atualização ou desenvolvimento de softwares;

- Contratação de serviços de comunicações;

- Construção e adequação de instalações (centros de monitoração e controle; laboratórios, residências, entre outros);

- Elaboração e gerenciamento de projetos;

- Gestão dos contratos e gestão jurídica;

- Contratação de especialistas e consultorias;

- Estabelecimento de parcerias com instituições públicas ou privadas, na área científico-tecnológica de interesse do setor cibernético;

- Aquisição e contratação de serviços para atendimento às demais despesas para o apoio à implementação da ação, tais como capacitação de pessoal no Brasil e no exterior, administração de importação (armazenagem, taxas, seguros, etc.), transporte, mobilização e acondicionamento de materiais, publicações diversas e cadernos de instrução, diárias e passagens, manutenção de depósitos, laboratórios e outros (instalações, equipamentos e materiais), material de informática, de expediente e de escritório; e

- Contratação de pessoal por tempo indeterminado nas condições e prazos previstos na Lei nº 8.745/93, para atender às atividades especiais referentes a encargos temporários de obras e serviços de engenharia.

As adequações recentes planejadas para o PDCDN preveem como principais entregas, dentre outras:

1) Estruturação do Sistema Militar de Defesa Cibernética, com sua modelagem, definição de requisitos e a respectiva regulamentação;

2) Adequação de instalações provisórias para o funcionamento da estrutura operacional do ComDCiber, com ferramentas e instalações adequadas para as demandas operacionais, numa primeira fase;

3) Construção das instalações definitivas do ComDCiber, inclusive com o Centro de Operações de Defesa Cibernética, numa segunda fase;

4) Adequação das instalações provisórias e definitivas da Escola Nacional de Defesa Cibernética;

5) Construção da nova Vila Militar, próxima ao Forte Marechal Rondon, com Próprios Nacionais Residenciais para os militares que servem no ComDCiber; e

6) Adequação das instalações e infraestruturas do Forte Marechal Rondon.

O setor cibernético é um setor estratégico para a Defesa Nacional, e como tal deve receber recursos condizentes com os desafios já citados neste documento.

Conforme já alinhado nesse relatório, o Ministério da Defesa apresentou, em 2008, a Estratégia Nacional de Defesa (END), com o objetivo de elaborar um plano de defesa focado em ações estratégicas de médio e longo prazo para modernizar a estrutura nacional de defesa. A END, aprovada pelo Decreto nº 6.703, de 18 de dezembro de 2008, definiu três setores estratégicos para defesa nacional: nuclear, cibernético e espacial. Delegou à Marinha do Brasil a gerência do programa nuclear; à Força Aérea,

o programa espacial; e ao Exército Brasileiro, a liderança da defesa cibernética em território nacional.

Assim, como resultado da delegação recebida a partir da END, o Exército Brasileiro, por meio da Portaria nº 666, de 4 de agosto de 2010, criou o Centro de Defesa Cibernética (CDCiber), inaugurado em 2012 por determinação do Comando do Exército. Sua missão é proteger os sistemas de informações e neutralizar a fonte de ataques, tentando inibir possíveis ataques digitais. O CDCiber foi o embrião para o hoje conhecido Sistema Militar de Defesa Cibernética.

Nesse contexto, a defesa cibernética inserida no planejamento governamental a partir do período de 2010 a 2012 apresenta-se no âmbito dos Planos Plurianuais conforme apresentado a seguir.

PPA 2012-2015

À época do PPA 2012-2015, a defesa cibernética encontrava-se em estruturação no âmbito do Exército Brasileiro e era encontrada no plano sob o programa Política Nacional de Defesa com os seguintes atributos relacionados:

PROGRAMA: 2058 - Política Nacional de Defesa

OBJETIVO: 0521 - Desenvolver tecnologias da informação e comunicações no Exército, visando assegurar a capacidade de defesa cibernética no campo militar e contribuir com a segurança cibernética nos campos civil e industrial.

Iniciativas:

01ZH - Implantação do sistema de defesa cibernética

PPA 2008-2011

Logicamente não se deveria encontrar menções à defesa cibernética nesse plano plurianual, tendo em vista a estruturação posterior desse ramo da defesa nacional. De todo modo, não se observou nenhuma outra referência, no âmbito de objetivos e iniciativas, a um possível estado embrionário.

PPA 2016-2019

No PPA 2016-2019, a defesa cibernética era encontrada sob o programa Defesa Nacional com os seguintes atributos relacionados:

PROGRAMA: 2058 - Defesa Nacional

OBJETIVO: 1119 - Desenvolver e elevar capacidades nas áreas estratégicas da cibernética, nuclear, espacial e nas áreas de comunicações, comando e controle, inteligência e segurança da informação.

Iniciativas:

05OO - Implantação do Comando de Defesa Cibernética do Exército Brasileiro.

05OP - Implantação da Escola Nacional de Defesa Cibernética.

05OQ - Implantação do sistema de homologação e certificação de produtos de Defesa Cibernética

PLPPA 2020-2023

Foi encaminhado, pelo Executivo, projeto de PPA no último dia 30 de agosto de 2019 ao Congresso Nacional. No projeto, que sofreu um grande processo de simplificação, **não há menção à defesa cibernética**.

Além desse desprestígio, se compararmos a execução orçamentária dos setores nuclear e o cibernético, a situação se revela drámatica.

No exercício financeiro de 2012 a 2018, o setor nuclear recebeu os seguintes aportes:

Ano	Dotação Inicial	Autorizado	Empenhado	Liquidado	Pago
2012	25.820.000	25.820.000	26.653.736	16.933.352	16.837.969
2012	0	85.405.640	0	0	0
2012	1.218.364.822	1.218.364.822	1.222.340.688	1.192.050.210	1.190.439.790
2012	192.681.266	192.681.266	186.576.205	172.775.979	172.493.679
2012	261.690.704	261.690.704	246.736.668	181.933.631	181.345.033
2012 Total	1.698.556.792	1.783.962.432	1.682.307.298	1.563.693.172	1.561.116.471
2013	316.360.000	368.360.000	371.049.999	235.815.136	169.863.749
2013	1.361.131.978	1.361.131.978	1.365.926.470	1.298.520.743	932.889.298
2013	223.746.179	223.746.179	242.379.509	68.405.061	57.836.687
2013 Total	1.901.238.157	1.953.238.157	1.979.355.979	1.602.740.940	1.160.589.734
2014	336.360.000	336.360.000	347.635.676	155.929.119	140.991.708
2014	1.590.933.486	1.461.396.363	1.251.901.136	1.241.110.712	1.129.861.219
2014	332.865.754	437.672.877	458.650.923	156.249.184	153.440.076
2014 Total	2.260.159.240	2.235.429.240	2.058.187.736	1.553.289.016	1.424.293.003
2015	346.760.000	346.760.000	254.013.314	108.191.493	77.445.006
2015	1.081.757.643	958.290.335	684.692.574	519.232.656	209.375.426
2015	277.512.302	277.512.302	128.896.714	72.462.287	33.229.996
2015 Total	1.706.029.945	1.582.562.637	1.067.602.602	699.886.436	320.050.429
2016	200.689.462	161.239.462	160.369.766	113.250.091	113.015.339
2016	341.348.666	341.348.666	340.685.870	220.948.420	219.777.358
2016	247.659.860	247.659.860	242.298.173	173.555.683	173.552.674
2016 Total	789.697.988	750.247.988	743.353.809	507.754.194	506.345.371
2017	250.030.280	387.359.725	388.099.496	229.077.091	228.923.018
2017	666.101.000	376.296.138	376.297.029	278.319.757	278.238.773
2017	364.599.000	364.599.000	377.331.960	303.838.687	302.311.929

2017 Total	1.280.730.280	1.128.254.863	1.141.728.484	811.235.536	809.473.720
2018	373.333.334	303.333.334	304.213.791	132.142.289	132.009.173
2018	423.881.000	474.754.705	483.532.044	430.444.846	430.444.846
2018	220.078.000	432.749.167	449.882.693	333.497.935	333.444.427
2018 Total	1.017.292.334	1.210.837.206	1.237.628.528	896.085.071	895.898.446
Total Geral	10.653.704.736	10.644.532.523	9.910.164.436	7.634.684.364	6.677.767.173

Já o setor cibernético, foi agraciado com o seguinte:

Ano	Dotação Inicial	Autorizado	Empenhado	Liquidado	Pago
2012	83.678.780	90.000.000	61.600.710	34.443.382	34.409.144
2012	0	20.975.667	0	0	0
2012 Total	83.678.780	110.975.667	61.600.710	34.443.382	34.409.144
2013	90.000.000	90.000.000	74.222.767	19.242.930	19.218.657
2013 Total	90.000.000	90.000.000	74.222.767	19.242.930	19.218.657
2014	70.000.000	70.000.000	61.751.715	26.396.990	23.596.824
2014 Total	70.000.000	70.000.000	61.751.715	26.396.990	23.596.824
2015	75.000.000	60.000.000	21.565.731	4.714.808	2.269.671
2015 Total	75.000.000	60.000.000	21.565.731	4.714.808	2.269.671
2016	34.246.428	34.246.428	33.984.502	19.578.594	19.313.820
2016 Total	34.246.428	34.246.428	33.984.502	19.578.594	19.313.820
2017	43.956.430	36.153.407	31.251.904	16.862.014	16.694.238
2017 Total	43.956.430	36.153.407	31.251.904	16.862.014	16.694.238
2018	24.600.000	20.347.770	20.351.612	10.393.806	10.029.081
2018 Total	24.600.000	20.347.770	20.351.612	10.393.806	10.029.081
Total Geral	421.481.638	421.723.272	304.728.942	131.632.524	125.531.437

No Projeto de Lei Orçamentária 2020 (PLOA), enviado pelo Executivo, há destinação de R$ 19 milhões para a Defesa Cibernética, direcionados ao Ministério da Defesa e ao Exército.

A nosso pedido, o relator setorial de Defesa, ilustre Senador Ângelo Coronel, sensível à importância do setor, acresceu R$ 2.138.782,00, somados a R$ 861.220,00, oriundos de recomposição dos recursos da Defesa Nacional, resultando um acréscimo à dotação inicial de R$ 3 milhões. Tal gesto atendeu, mesmo que em pequena parte, a Emenda nº 50270001, da

Comissão Mista de Controle de Atividade de Inteligência, que previa R$ 70 milhões.

Até o presente, foram destinados ao Ministério da Defesa e ao Exército para 2020 o valor de R$ 22 milhões, para a aplicação no setor cibernético.

Desse montante, somente R$ 6.334.725,00 serão destinados ao Comando de Defesa Cibernética – ComDCiber. Segundo o Comando, são necessários para o próximo ano R$ 60 milhões para implantar e modernizar um modelo capaz de atender às necessidades desse setor estratégico.

Independente das necessidades do meu Estado, apresentei emenda individual de R$ 200.000,00 à implantação e modernização da Defesa Cibernética, na ação 147F.

Apresentamos sugestão de Emenda à Comissão de Relações e Defesa Nacional – CRE, no valor de R$ 60 milhões para a Defesa Cibernética, contudo a Comissão aprovou, por escolha da Força, o Programa relativo à Aviação do Exército, como prioridade.

Em relação ao PPA 2020-2023, o Executivo encaminhou ao Congresso Nacional a mensagem sem previsão de projetos para implantação e modernização do setor de defesa cibernética. Sugerimos alterar essa realidade. Contudo, um dispositivo no parecer preliminar aprovado, mais especificamente no item 2.2.5, torna inadmissível emendas para inclusão de investimento plurianuais prioritários que não in.formassem, alternativamente, estar o investimento correspondente com a execução financeira acumulada superior a 20% em 30 de junho de 2019 ou ter previsão de conclusão até 2023. Dessa forma, entende-se que o Executivo não dará

continuidade no PPA 2020-2023 à priorização do setor verificada no PPA 2016-2019.

Portanto, não há como o Setor Cibernético se manter com esses valores. Fica o ponto, estimamos que o orçamento do setor cibernético deveria ser de 60 milhões para o ano de 2020, e 120 milhões para 2021, 2022 e 2013, a fim de atingir os objetivos já fixados.

5. RECOMENDAÇÕES E ENCAMINHAMENTOS

Os trabalhos levados a cabo pela CRE para avaliação da Política Nacional sobre Defesa Cibernética ressaltaram a importância extremamente sensível para a Defesa Nacional desse setor. Em alguns Países, a Cibernética é a Quarta Força Armada.

Nesse capítulo, consolidamos nossas recomendações e encaminhamentos. Objetivamente, faremos três recomendações, uma de cunho orçamentário, outro normativo e, por fim, uma para os membros desta Comissão.

A primeira, de caráter orçamentário, é de extrema urgência para o País. Simplesmente, perde o sentido detalharmos todas as medidas de caráter estrutural, como a melhoria da Escola de Defesa Cibernética ou do Exercício Guardião Cibernético, que simula uma guerra cibernética e envolve representantes das infraestruturas críticas brasileiras, se não há dotação orçamentária.

Nossa maior crítica é a não observância, no aspecto orçamentário, do Setor Cibernético como destaque pela Estratégica Nacional de Defesa Nacional, ao lado do setor espacial e do setor nuclear. Portanto, estimamos que o orçamento do setor cibernético deveria ser de 60 milhões para o ano de 2020 e duplicar nos três anos seguintes para atingir os objetivos já fixados pelo Estado brasileiro.

A segunda recomendação, de caráter normativo, esbarra, inicialmente em obstáculos de iniciativa. Notamos que carecemos de um

marco nacional com status de lei federal que congregue as incipientes orientações infralegais que orientam atualmente a política nacional de defesa cibernética. Contudo, essa normativa deveria ser preparada pelo Poder Executivo, pois necessariamente envolveria a necessidade de versar sobre órgãos daquele Poder. Projeto de Lei de autoria de parlamentar padeceria de vício de iniciativa se enfrentasse toda a complexidade desse novo estatuto legal. Recomendamos que se elabore e proponha urgentemente essa norma.

Por fim, esta Comissão precisa dar o valor que esse estratégico setor requer. Recomendamos que seja criada uma Subcomissão da CRE dedicada à defesa cibernética. Estamos ficando para trás no campo de defesa cibernética e podemos pagar um preço caro por isso. Logo entrará nova era digital, como computadores quânticos, tecnologia 5G, e nós, talvez, estejamos apegados a espécie de "Linha Maginot", fortificações físicas construídas pela França na década de 30, que se revelou grande erro estratégico, a culminar na derrota para a Alemanha em 1940 e à ocupação daquele País.

Senador ESPERIDIÃO AMIN