SENADO FEDERAL
SECRETARIA-GERAL DA MESA
SECRETARIA DE REGISTRO E REDAÇÃO PARLAMENTAR

REUNIÃO
05/09/2019 - 46ª - Comissão de Relações Exteriores e Defesa Nacional

O SR. PRESIDENTE (Nelsinho Trad. PSD - MS) - Invocando a proteção de Deus, declaro aberta a 46ª Reunião, Extraordinária, da Comissão de Relações Exteriores e Defesa Nacional da 1ª Sessão Legislativa Ordinária da 56ª Legislatura do Senado da República.

Expediente.

A presente audiência pública tem o objetivo de debater o Programa de Defesa Cibernética, tema muito bem proposto pelo nobre Senador Esperidião Amin, em atendimento ao Requerimento nº 24, de 2019-CRE, conforme o item 5 do cronograma do Plano de Trabalho da Avaliação de Políticas Públicas: 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.

Tenho a honra de anunciar e convidar para esta Mesa de trabalho as seguintes autoridades: General de Divisão Guido Amin Naves, Comandante de Defesa Cibernética e representante de Comando do Exército; Contra-Almirante Luciana Mascarenhas da Costa Marroni, representante do Comando da Marinha do Brasil; General de Brigada Ivan de Sousa Corrêa Filho, representante do Ministério da Defesa; Coronel Aviador Éric Cézzane Cólen, Chefe da Seção de Comando e Controle do Emaer, representando o Comando da Aeronáutica; Cel. Arthur Pereira Sabbat, representante do Gabinete de Segurança Institucional da Presidência da República.

Sejam todos muito bem-vindos! Obrigado pela presença.

Interatividade da reunião. Esta audiência pública será realizada em caráter interativo, com a transmissão pelos canais de comunicação do Senado Federal. A população pode participar enviando observações e perguntas aos palestrantes por meio da internet, no Portal e-Cidadania, no endereço www12.senado.leg.br/ecidadania.

A participação dos internautas é sempre de extrema valia para os nossos trabalhos.

Registro a presença em Plenário das seguintes autoridades: Gen. de Divisão João Roberto Oliveira; Contra-Almirante Marcio Tadeu Francisco das Neves; Contra-Almirante Carlos André Coronha Macedo; Cel. Edson Ribeiro dos Santos Júnior; Cel. Antônio Bispo de Oliveira Filho; Cel. Alexander Eduardo Vicente Ferreira; Cel. Luís Sérgio da Costa Souto; Cel. André Luís Nogueira Terra; Cel. Marco Antônio Rocca de Andrade; Capitão de Fragata Fabio Kenge Arakaki; Capitão de Fragata Rodrigo Abrunhosa Collazo; Tenente-Coronel Sylvio André Diogo Silva; Major Vitor Augusto Kopp Jantsch; 1ª Tenente Fabiana de Oliveira Ozaka.

Antes de passar a palavra aos nossos convidados, concedo, com muita honra, a palavra ao Senador Esperidião Amin, como Relator do Requerimento 24, de 2019, desta Comissão, que deu origem a esta audiência pública para debater o Programa de Defesa Cibernética, para fazer suas considerações iniciais.

Antes, porém, gostaria de registar a presença do Senador Marcos do Val, sempre assíduo nesta Comissão.

Com a palavra Senador Amin.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Unidos pelo Brasil/PP - SC. Como Relator.) - Sr. Presidente, prezado Senador Marcos do Val, autoridades já referidas, eu fico feliz por participar deste momento, Presidente Nelsinho Trad, porque ele dá a partida a uma grande tarefa e a uma das duas grandes prioridades eleitas nesta Comissão para que, em termos de acompanhamento, nós possamos contribuir para o aprimoramento das políticas públicas, no caso relacionadas à questão da influência dos meios cibernéticos na economia, na vida, enfim, na sociedade.

Hoje, contando com a presença especialmente dos representantes de Governo e, particularmente, das Forças Armadas, creio que damos a partida mais bem lançada. Tivemos oportunidade de já participar de outros eventos, e não posso deixar de registar a nossa satisfação e a de outros Senadores, que, inclusive, se comprometeram a aqui comparecer quando dos exercícios de ataque cibernético no Comando de Defesa Cibernética do Exército em junho passado.

Então, creio que caberá à nossa capacidade de sermos objetivos e de tratarmos dessa questão, que é multidisciplinar - não é interdisciplinar, é multidisciplinar -, dessa questão complexa e desafiadora. Caberá à nossa competência, à nossa capacidade de dispor racionalmente as várias inserções do assunto na nossa sociedade para sermos eficazes na que deverá ser a quinta grande reunião, que será o laudo da avaliação de como está essa política pública no Brasil.

De minha parte, quero lhe agradecer pessoalmente pelo apoio pessoal e político que sempre deu para que esse tema prosperasse e, inclusive, vencesse disputas que ocorreram quanto à nossa preferência e, de maneira muito evidente, inovando em matéria de avaliação de política pública no Brasil.

Eu gostaria ainda de, por uma questão de relação pessoal, agradecer a presença aqui do meu ex-aluno, Egon Schaden Júnior, que é o Presidente Executivo da Associação Nacional de Certificação Digital, aqui entre nós.

Muito obrigado, Presidente.

O SR. PRESIDENTE (Nelsinho Trad. PSD - MS) - Fala dos palestrantes. Esclareço aos senhores palestrantes que irei conceder a palavra por 20 minutos para cada um, com a possibilidade de prorrogação para a conclusão de suas exposições. Em seguida, abriremos a fase de interpelações pelas Sras. e Srs. Senadores presentes e inscritos.

Para dar início à audiência pública, concedo, neste instante, a palavra ao General de Divisão Guido Amin Naves, Comandante de Defesa Cibernética, que tão bem nos recebeu dois meses atrás numa visita que fizemos ao seu comando.

Com a palavra General de Divisão Guido Amin Naves.

O SR. GUIDO AMIN NAVES (Para exposição de convidado.) - Bom dia a todos, Presidente Senador Nelsinho Trad, Senador Esperidião Amin, Senador Marcos do Val, demais autoridades e convidados, senhoras e senhores.

Em primeiro lugar, cabe-me aqui nada mais que agradecer esta possibilidade de elevar a discussão em torno da defesa cibernética nacional a este nível do nosso Senado Federal. Isso é muito importante para nós, essa inserção político-estratégica desta capacidade tão importante e transversal a tudo que se faz neste País. É muito importante para nós, Sr. Presidente. Então, muito obrigado pela oportunidade de discutir em tão alto nível esses assuntos que são tão caros a nós, ao nosso trabalho e ao nosso dia a dia no Comando de Defesa Cibernética.

Eu trouxe uma apresentação para levantar algumas ideias e alguns dados para alimentar o debate que se seguirá.

Em primeiro lugar, eu queria trazer alguns marcos do setor de defesa cibernética no Brasil.

Isso começou em 2008, quando a Estratégia Nacional de Defesa estabeleceu os três setores estratégicos para a defesa nacional, nuclear, espacial e cibernético. Essa diretriz de 2014 atribuiu à Marinha o setor nuclear, à Força Aérea, o setor espacial e, ao Exército, o setor cibernético.

A partir daí, o Exército estabeleceu o Projeto Estratégico de Defesa Cibernética com certos projetos e, em decorrência disso, estabeleceu em 2010 o núcleo do Centro de Defesa Cibernética. Esse núcleo, em 2012, foi ativado, e hoje é o braço operacional do Comando de Defesa Cibernética.

Em 2012 também, foi criada a Ação Orçamentária 147F, que é a ação orçamentária destinada a prover os fundos necessários ao desenvolvimento dessa capacidade. Essa ação, inicialmente, era apenas com recursos discricionários do Exército; não tinha sido possível ainda nesse momento a Defesa aportar recursos como ela já vinha fazendo para os demais setores estratégicos.

Em 2013, o caso Snowden foi um caso emblemático no mundo todo, afetou o nosso País, o nosso Governo. Houve uma CPI aqui no Senado Federal, houve um grupo de trabalho interministerial capitaneado pela Defesa, e tudo isso levou a uma série de orientações, de medidas a serem tomadas para potencializar a Defesa Nacional no País.

Por conta disso, nasceu o Programa de Defesa Cibernética na Defesa Nacional. O projeto estratégico do Exército, em 2017, transformou-o em programa, nós avançamos a metodologia do Exército em gestão de projetos e programas estratégicos.

Esse projeto, na verdade, sempre foi um programa, passamos a denominá-lo corretamente, normatizamos o portfólio estratégico, de forma que hoje nós temos dois programas estratégicos que cuidam da cibernética: um programa singular do Exército, com recursos discricionários do Exército; e um programa da Defesa, com recursos da Defesa.

Em decorrência desse Programa de Defesa Cibernética na Defesa Nacional, em 2015 foram ativados os núcleos da Escola Nacional de Defesa Cibernética e do Comando de Defesa Cibernética.

Em 2016, o Comando foi ativado, e o seu primeiro comandante assumiu. Eu, na verdade, sou o terceiro comandante do Comando de Defesa Cibernética, o CDCiber, enquadrado pelo Comando como seu braço operacional.

Até 2017 nós estávamos provisoriamente no Quartel General do Exército, no SMU, em Brasília. Aí passamos a ocupar instalações no Forte Marechal Rondon, próximo à Torre Digital de Brasília, onde estamos até agora. Vamos permanecer neste Forte, ainda que em novas instalações que estão planejadas, visto que as instalações que ocupamos hoje, que muitos dos Srs. Senadores conheceram por ocasião do exercício que fizemos no começo de julho, são instalações que não foram construídas para abrigar um Comando Cibernético. São instalações também provisórias, em que pese as definitivas ficarem no mesmo local nesse Forte Marechal Rondon.

Em 2019, agora em fevereiro, a nossa Escola Nacional de Defesa Cibernética foi ativada e seu primeiro comandante assumiu a sua posição. Lembro que, nesse período todo, tivemos todos esses grandes eventos no Brasil e foi preciso, nesse processo, obter e aplicar rapidamente capacidades cibernéticas para oferecer proteção adequada aos sistemas empregados nesses grandes eventos.

Como exemplo: na Copa do Mundo de 2014, tivemos 756 eventos de segurança tratados pela defesa cibernética e conseguimos que nenhum deles atravessasse a nossa borda e oferecesse algum risco, o que acabaria comprometendo até a imagem do Brasil perante o mundo, já que estávamos aqui sediando a Copa do Mundo. Talvez, se tivéssemos deixado alguns deles passarem antes dos 7 a 1, isso não tivesse ocorrido conosco, mas, enfim, é melhor que o Brasil passe bem por essa situação. Acho que o placar de 7 a 1 foi menos doloroso do que seria uma catástrofe cibernética inviabilizando a Copa do Mundo no Brasil.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Unidos pelo Brasil/PP - SC. *Fora do microfone*.) - Há controvérsias.

O SR. GUIDO AMIN NAVES (Para exposição de convidado.) - Há controvérsias, concordo com o senhor, mas, enfim, vamos lá. Isso já é história.

Nessa linha do tempo, senhores e senhoras, nós tivemos - eu resumi bastante - estas duas fases: criação e implantação, cuja prioridade era a obtenção e a aplicação de capacidades cibernéticas, haja vista os grandes eventos que acabei de citar.

Após isso, após o último grande evento, fizemos uma reavaliação. Em cibernética as coisas evoluem muito rápido, a maturidade aumenta muito rápido, as circunstâncias evoluem muito rápido, de forma que a cada cinco anos mais ou menos a gente muda de era na cinética. Então, fizemos uma reavaliação baseada no que ocorreu em 2017, o caso do WannaCry, um *ransomware* que abalou o mundo todo - há um pequeno filme aqui que pode mostrar alguma coisa -, e um diagnóstico da nossa situação em cibernética naquele momento, em 2017, 2018.

Pode colocar o filme.

(Procede-se à exibição de vídeo.)

O SR. GUIDO AMIN NAVES - Vamos voltar ao eslaide?

Bom, com esse diagnóstico que fizemos, nós concluímos que era preciso iniciar já uma nova fase, mesmo antes de terminar a criação e a implantação. É uma fase de consolidação e de mudar um pouco a prioridade.

Viram que as questões de âmbito nacional nos levam a buscar uma nova prioridade, que é a inserção política e estratégica do setor. A obtenção e a aplicação de capacidades não terminam nunca, estão sempre evoluindo, mas é preciso buscar essa inserção política, porque a defesa cibernética é assunto da Nação como um todo, não é assunto de nenhum estamento de *per se* ou de qualquer grupo isolado. A Nação inteira tem que se envolver na sua proteção cibernética, para ter um maior nível de sucesso, visto que essa ameaça é muito capaz e não tem como ser eliminada.

No Brasil, temos essa estrutura hoje, nos níveis político, estratégico, operacional e tático. Há os atores, com destaque no nível político, o próprio GSI, a Secretaria de Assuntos Estratégicos. No nível político se fala de segurança cibernética, fala-se de segurança de infraestruturas críticas, tão importantes para nós, para o País como um todo, e se fala de proteção cibernética. Nos níveis mais abaixo, estratégico, operacional e tático, fala-se de defesa cibernética. A defesa cibernética engloba três áreas: proteção, exploração e ataque. E ali está posicionado o nosso Comando de Defesa Cibernética.

Há uma questão interessante. Esse é o espectro dos conflitos. Há um autor que eu, aliás, li por indicação de um colega diplomata, um livro muito interessante que eu li, em que ele cria um novo passo entre a paz e a crise, que é a não paz, é o

tempo de não paz. Você não está em crise, mas também não está em paz, então é não paz. Enfim, é um conflito bastante... É um espectro bastante fácil de entender, mas o importante é aqui: a defesa cibernética não atua só em crise, ela atua 24 por 7, 365, 366, em cada quatro anos; ela não pode parar um minuto, precisamos estar atentos, temos que ser um comando operacional conjunto ativado permanentemente, tal qual a nossa defesa aérea. É a mesma coisa. Nós não podemos estar... Nós temos que ter, inclusive, o amparo normativo e legal para estarmos operativos todo o tempo. Não é possível que a gente esteja aguardando um decreto de GLO ou algum tipo de estado de exceção, alguma coisa assim, ou até, num caso extremo, uma declaração de guerra, por assim dizer, para que possamos atuar. É importante que a defesa cibernética atue todo o tempo, sob pena de, quando for necessário, não haver a consciência situacional, não haver a inteligência necessária para tomar alguma atitude em defesa do Estado brasileiro, da sociedade brasileira.

Os dois programas que nós temos foram desenhados, o primeiro, em 2010, singular do Exército; o outro, em 2014. Estamos em 2019 e já estamos fazendo um trabalho de readequação, reavaliação, reorientação de escopos e assim por diante, estruturando melhor a demanda que precisamos daqui para frente.

A questão orçamentária. Nós temos, então, a Ação Orçamentária 147F. Como eu já disse, ela tem dois POs, o 1 e o 2. O PO1 é, vamos dizer assim, contemplado pelas verbas discricionárias do Exército, e o PO2, pelas verbas da Defesa. Na verdade, quanto a esses dois, nós estamos agora nesse trabalho de readequação, buscando coordenar ainda mais os esforços, visto que o Exército é responsável por todo o setor cibernético, e essas coisas estão assim, porque a evolução histórica assim permitiu que chegássemos.

Os números. O PO1, desde 2012: estão aí as PLOAs, LOAs, LMEs, as emendas que foram contempladas e o que foi executado. E "executado" significa empenhado, o que foi liquidado, o que foi pago. Aí entram "restos a pagar" e começam a distorcer um pouco os números. Então, aqui é mais fácil de entender. Veja que nós temos um excelente nível de execução, como costuma acontecer com as Forças Armadas em geral.

Vejam, isso foram verbas que o Exército tirou da sua discricionária para colocar na cibernética. O que a Defesa contemplou nesse período? Bem menos. E aqui não vai absolutamente crítica a isso; isso é o que foi possível fazer e também em função do nível de estruturação que havia na demanda. Nós estamos tratando disso neste exato momento, estruturando melhor a demanda para que possamos pleitear - e certamente há uma confiança muito grande de que conseguiremos - um aporte mais significativo para podermos proceder às entregas de que o Estado e a sociedade precisam. Estão aí os valores.

Aqui dá para ver um pouquinho mais o que foram - em amarelinho - as LOAS; em vermelho, a LME; quando não há amarelo, é porque a LME foi igual à LOA, e o que está em verde é o executado. Então, como sempre, a gente tem um bom nível de execução daquilo que foi destinado a esta área.

Entregas, já foram feitas muitas: o próprio Comando, o próprio ComDCiber, a escola, já estamos funcionando, operando laboratórios de segurança cibernética já em Itaipu, que é uma das principais estruturas críticas do nosso País.

Nós já temos desenvolvimentos pagos pelo nosso programa a cargo da Força Aérea, um projeto de integração do Centro de Tratamento de Incidentes de Rede das Forças e, a cargo da nossa Marinha, Comando de Operações Navais, o Sistema de Proteção de Unidades Operativas, proteção de sistemas embarcados, que é uma preocupação muito grande nossa na Defesa.

Com relação à capacitação nessas áreas todas mencionadas: são mais de mil cursos já pagos no Brasil e no exterior para capacitar militares. Este ano, a ideia dessa escola, que é a Escola Nacional de Defesa Cibernética, não é capacitar só militares, este ano a Secretaria de Governo e o MCTIC já estão interessados e estão em acertos conosco para aproveitar os nossos processos, esses cursos, para poderem matricular seu pessoal, servidores civis do Governo, servidores de Estado, que também precisam ter as capacitações necessárias para atuar na proteção dos sistemas corporativos.

Nós temos também uma interação muito grande com outros setores fora da Defesa: projetos de certificação e homologação, levantamento de requisitos, já temos um sistema de parceria com o Inmetro, outro com o Senac, com a Federal de Pernambuco e outros trabalhos.

Coisas que já fizemos aqui. Na área internacional, esse Fórum Ibero-Americano leva dez países tratando de assuntos interessantes para todos nós. Já participamos do maior exercício de proteção cibernética do mundo, realizado no âmbito da Otan, participamos efetivamente do exercício. E já realizamos a segunda edição este ano - alguns dos Srs. Senadores nos deram o prazer de sua presença lá para acompanhar o exercício - de um exercício de proteção cibernética feito para a proteção de nossas infraestruturas críticas - setor financeiro, telecomunicações, elétrico, nuclear; águas e transportes entraram como observadores para, eventualmente, no ano que vem estarem presentes no exercício.

Com isso, Senador, eu encerro a minha fala. Teria um pequeno filme que mostra o resumo desse exercício, mas, dado o tempo, eu não vou passá-lo.

Fico à disposição para as perguntas de todos.

Muito obrigado.

O SR. PRESIDENTE (Nelsinho Trad. PSD - MS) - Conforme a nossa dinâmica nas outras audiências, passo de pronto a palavra à Contra-Almirante Luciana Mascarenhas da Costa Marroni, representante do Comando da Marinha do Brasil.

A SRA. LUCIANA MASCARENHAS DA COSTA MARRONI (Para exposição de convidado.) - Bom dia a todos!

Como o General Amin já falou, o responsável pelo setor estratégico de defesa cibernética é o Exército; então, a Marinha tem uma participação de cooperação e colaboração com o Comando de Defesa Cibernética.

Nós temos a nossa rede de proteção da rede da Marinha, onde nós trabalhamos toda a nossa segurança. Até hoje não tivemos nenhum incidente importante, o que significa que nós estamos realizando um bom trabalho.

Em 2016 foi criado o CTir da Marinha. O General mostrou ali que houve a integração dos CTir das Forças. Até então a Marinha não tinha o CTir, que foi criado em 2016 e integrado ao ComDCiber.

Nossa colaboração ao ComDCiber é com pessoal, e o nosso CTir também troca informações: além de fazer o tratamento dos nossos incidentes, troca informações com o ComDCiber. Além disso, nós nos beneficiamos dos cursos que o Exército disponibiliza na ENaDCiber, recém-criada, e nós já estamos capacitando diversos militares para trabalhar nessa área.

Muito obrigada.

O SR. PRESIDENTE (Nelsinho Trad. PSD - MS) - Agradecemos a Contra-Almirante Luciana Mascarenhas da Costa Marroni.

De pronto, o General de Brigada Ivan de Sousa Corrêa Filho, representando aqui o Ministério da Defesa.

O SR. IVAN DE SOUSA CORRÊA FILHO (Para exposição de convidado.) - Obrigado, Sr. Presidente.

Srs. Senadores, senhores oficiais, demais autoridades, minha função atual: sou o Chefe do Centro de Defesa Cibernética, que é o braço operacional do Comando de Defesa Cibernética comandado pelo General Amin.

O General já apresentou bem amplamente a situação do setor. Eu gostaria apenas de destacar uma preocupação. Ali no Centro a gente verifica que 90% dos ataques cibernéticos exploram o elo mais fraco, que é a pessoa, o ser humano. Então, qualquer política pública para garantir melhor condição de segurança cibernética no País, a gente nota isso lá, tem que explorar a educação e a conscientização das pessoas. No caso de celular "hackeado": o dono do celular pode tomar uma série de medidas para dificultar, pelo menos, aquele ataque, não digo impedir. Quando a pessoa é um alvo, muito dificilmente ela escapará do ataque, mas ela pode dificultar. E isso também se aplica às empresas. A empresa normalmente é atacada usando o pessoal dela, a fragilidade do pessoal. Queria só destacar mais esse ponto, além do que o General Amin falou.

(Intervenção fora do microfone.)

O SR. IVAN DE SOUSA CORRÊA FILHO - Ah, sim.

Quero só destacar esse aspecto, porque é um aspecto importante, essa necessidade do desenvolvimento da mentalidade de segurança na população como um todo para que o País tenha mais segurança cibernética.

Eu vou aproveitar também, em função de termos ainda um pouco de tempo, para passar o filmete que o General Amin deixou de passar sobre o Exercício Guardião Cibernético. Esse filmete representa bastante bem esse trabalho que a Defesa vem realizando, de cooperação com as infraestruturas estratégicas, para que a gente consiga melhorar a condição de segurança cibernética dessas infraestruturas críticas.

Por favor.

(Procede-se à apresentação de vídeo.)

O SR. IVAN DE SOUSA CORRÊA FILHO - Esse aspecto que eu levantei aqui também destaca essa necessidade de atuação colaborativa, que é o grande mote para conseguir proteção cibernética efetiva.

Eu vou pedir também para projetar um eslaide - esse aí, obrigado - que indica o nosso planejamento.

Então, são os valores que estão no nosso plano plurianual. Este ano, agora, nós estamos estruturando a demanda, nos preparando para conseguirmos executar de uma forma realmente eficiente esses valores que estão previstos para os próximos anos no orçamento da Defesa para o programa, no PPA...

O SR. GUIDO AMIN NAVES (*Fora do microfone*.) - PPA.

O SR. IVAN DE SOUSA CORRÊA FILHO - Isso, no PPA, da Defesa, para a atividade de defesa cibernética.

Obrigado, Presidente.

O SR. PRESIDENTE (Nelsinho Trad. PSD - MS) - De pronto, passo a palavra ao Cel. Aviador Éric Cézzane Cólen, Chefe de Seção do Comando e Controle do Emaer e representante do Comando da Aeronáutica.

O SR. CORONEL AVIADOR ÉRIC CÉZZANE CÓLEN (Para exposição de convidado.) - Bom dia, Senador Nelsinho Trad, Sr. Senador Esperidião Amin, Sr. Senador Marcos Durval!

É um prazer estarmos aqui com a oportunidade de mostrar alguma coisa dos trabalhos que nós estamos fazendo na Força Aérea.

Cumprimento também as demais autoridades presentes, os oficiais generais.

O General Amin já falou bastante sobre como o ComDCiber conduz esse trabalho de segurança cibernética. O ComDCiber, como elemento central deste sistema em nossa parte de defesa cibernética, nos orienta, nos conduz neste trabalho. Como diz a Contra-Almirante, nós trabalhamos de forma colaborativa e cooperativa o tempo inteiro.

Aqui nós tivemos a oportunidade de verificar a questão da cibernética nacional como um todo, em termos de quanto é relevante o tema cibernética para a Nação, o quanto é importante, como disse o Gen. Corrêa Filho, não só a defesa de sistemas, mas da população também.

Nós pretendemos aqui hoje apresentar uma perspectiva nova com que nós, Força Aérea, estamos trabalhando atualmente. Então, a intenção é que os senhores hoje possam conhecer de forma bem singela e rápida como está o sistema de defesa cibernética na Força Aérea Brasileira hoje e conhecer a perspectiva da FAB para cibernética.

Aqui são algumas tiras de reportagens que nós elencamos. A mais recente é relativa ao ataque cibernético dos Estados Unidos que desativou computadores militares do Irã. Nesse ataque cibernético foram desativados, então, os sistemas de mísseis dos iranianos. Satélites americanos ficaram sujeitos a ataques cibernéticos também. Então, uma sensibilidade que eles... A cibernética tornou-se primordial para todas as Forças Armadas, e esse tema tem se destacado cada vez mais.

O F-16, uma aeronave bastante utilizada no mundo inteiro: já foi identificado o quanto ela pode ser vulnerável a ataques cibernéticos. Então, muitas vezes nós discutimos, mas a cibernética não deixa de ser importante. Como já foi dito, há infraestruturas críticas da nossa vida diária que estão sujeitas ao tema da defesa cibernética.

Só que nós, Força Aérea, hoje, estamos pensando além disso. Particularmente, a Força Aérea emprega muita tecnologia. Então, hoje, a gente fala assim... Um Gripen, aqui é só um pictorial do painel do Gripen. Nós entendemos que não podemos falar que o Gripen é um computador voador; não, são vários computadores ali embarcados trabalhando em rede para fazer funcionar a aeronave.

O mesmo se pode dizer quanto ao KC-390. Nós tivemos a oportunidade de receber a primeira aeronave ontem. Ela também tem bastantes sistemas embarcados. Podemos citar, por exemplo, que o sistema de planejamento das aeronaves é carregado no solo, no sistema de planejamento no solo, e, depois, carregado na aeronave. Então, nós estamos sujeitos, vamos colocar assim, à questão do ataque cibernético com os sistemas embarcados em nossas aeronaves.

E há o satélite. Nós operamos o nosso lá, o SGDC, um satélite da Defesa operado pelo Cope, Centro de Operações Espaciais. Nós também temos grande preocupação com as vulnerabilidades, haja vista que uma potência, como é o caso dos Estados Unidos, já sofreu ataques cibernéticos no seu satélite. Nós temos grande preocupação com as vulnerabilidades que, eventualmente, o nosso satélite possa ter.

Nesse sentido, então, vamos passar um roteiro bem curto para os senhores: a situação da defesa cibernética na FAB e as perspectivas da FAB para a cibernética.

Como já disse, a cibernética está bem estruturada. Hoje, a FAB tem o CTIR FAB, nós trabalhamos com quatro ETIRs e pretendemos incrementar essa capacidade, em função da importância que o tema tem, em função da criticidade que determinadas unidades estão adquirindo.

Então, nós estamos trabalhando e planejando para, num futuro não muito distante, esperamos - dependemos, lógico, da disponibilidade dos recursos -, incrementar essa nossa capacidade cibernética tal qual já foi apresentado aqui hoje pelos Generais e comentado pelo Almirante, incrementar a nossa defesa cibernética relacionada principalmente à rede de computadores que nós empregamos em nosso sistema de comando e controle.

Essa é a nova preocupação que nós temos na Força Aérea, como já destaquei, a perspectiva para a FAB e para a cibernética no futuro, porque isso aqui é o que nós imaginamos de um cenário operacional, no qual nós temos vários sistemas

embarcados, diversos dispositivos conectados em rede, temos satélites, temos aeronaves, temos *drones*, temos sistemas de mísseis, tudo isso conectado em rede, ou seja, são sistemas digitais sujeitos a ataques cibernéticos.

Na própria reportagem, aquela que nós mostramos do ataque cibernético que o Estados Unidos sofreu no seu satélite, a preocupação é o quão profundo foi esse ataque, porque, eventualmente, os próprios sistemas de comando e controle da Otan e dos Estados Unidos podem ter sido afetados via ataque pelo satélite.

Então, a nossa preocupação está no emprego e nessa questão, não expandindo a nossa necessidade. Nós temos uma necessidade tal qual já apresentado aqui, com as nossas infraestruturas como um todo, todavia entendemos que há um nicho, uma capacidade muito grande que nós temos que adquirir, que é relacionada aos sistemas embarcados.

Nós temos já uma diretriz de planejamento do nosso Comandante, ele já nos orientou para a criação de um centro de defesa cibernético a partir da criação e adequação de uma organização militar da Força Aérea. Nós estamos cunhando um termo que não existe ainda muito claramente, a defesa cibernética operacional. Nós vamos trabalhar com o ComDCiber, estamos na fase embrionária dessa discussão. Há um grupo de trabalho que está trabalhando nessa linha; o Comando da Aeronáutica está discutindo internamente ainda e com a participação do ComDCiber, que tem nos acompanhado e nos orientado em relação a esse tema. Nesse nosso centro de defesa cibernética, uma das propostas - não está solidificada ainda - seria migrar... Hoje a nossa parte de defesa cibernética está bem relacionada à questão de TI, à nossa Diretoria de Tecnologia de Informação, e nós estamos entendendo que o cenário mundial, as perspectivas que nós entendemos para o futuro, as plataformas que nós possuímos hoje, que são cada vez mais digitais, tudo isso nos leva à expectativa de fazer migrar o Centro de Defesa Cibernética para o Comando Operacional.

Então, está bastante claro para nós o entendimento de que a cibernética virou uma arma, tal o exemplo que o General comentou, o ComDCiber, tal qual o trabalho da defesa aérea. Esse é o entendimento que nós estamos tendo, de que a nossa proteção cibernética tem que ser igual à defesa aérea que nós temos hoje, com a capacidade que nós temos hoje de pronta resposta para proteger os ativos que nós temos. Então, essa é a perspectiva com a qual nós estamos trabalhando ainda internamente na Força Aérea com o apoio...

Tivemos a oportunidade... A Marinha já apresentou um trabalho ao Comandante, do que está sendo feito por eles. Interagimos constantemente com o ComDCiber em relação a este tema, mas nós já despertamos para esta necessidade: precisamos incrementar muito esse tema, especialmente em relação ao conhecimento, que é bastante restrito, de acesso.

A gente fala de proteção de infraestruturas críticas. Nós temos no mercado muita coisa já disponível, os bancos e as empresas trabalham com isso. Agora, quando nós falamos de proteção de sistemas embarcados, esse é um nicho muito mais limitado de conhecimento. Então, nós já identificamos grandes dificuldades na busca desse conhecimento, como nos capacitar, como preparar a Força para efetivamente proteger os seus sistemas embarcados e evoluir na questão da cibernética para efetivamente termos um emprego operacional. Mais uma vez, nós entendemos que a cibernética é uma arma que nós temos que... E o futuro... São dois nichos que nós, na Força, entendemos como fundamentais para o futuro: a cibernética e o espaço. O mundo operacional, os conflitos futuros caminham para isso.

A cibernética tem um nicho dissuasório que... Com pouco investimento, comparado à aquisição de uma aeronave, pode-se fazer um estrago muito grande. Então, nós estamos trabalhando bastante agora nesse tema, de forma que a gente possa aperfeiçoar e fazer evoluir essa nossa capacidade.

O nosso roteiro é curto, só para mostrar aos senhores como está a defesa cibernética hoje na Força Aérea. Nós estamos muito focados na proteção de nossas redes de computadores principalmente, e a nossa perspectiva para o futuro é a cibernética, efetivamente, como uma arma de guerra, tanto para proteger como para outras atividades.

Então, nós estamos trabalhando para isso. O Centro de Defesa Cibernética que hoje nós estamos trabalhando, modelando, vai nascer com essa perspectiva já. A nossa ideia é tirar da TI, da nossa Diretoria, do Sistema de Tecnologia da Informação da Força Aérea, e migrar para um comando operacional em que a gente tenha essa prontidão, uma pronta resposta para o que a gente precisa no emprego de cibernética.

Espero que tenhamos atendido o objetivo e que vocês tenham podido entender um pouco o sistema de defesa cibernética da Força Aérea, bem como as perspectivas que nós temos para o futuro em relação à cibernética.

Obrigado.

O SR. PRESIDENTE (Nelsinho Trad. PSD - MS) - Agradecemos as palavras do Cel. Aviador Éric Cézzane Cólen.

De pronto, passo a palavra ao último que apresentará as suas considerações, o Cel. Arthur Pereira Sabbat, representante do Gabinete de Segurança Institucional da Presidência da República (GSI).

O SR. ARTHUR PEREIRA SABBAT (Para exposição de convidado.) - Cumprimento o Exmo. Sr. Senador Nelsinho Trad, Presidente desta Comissão, a quem felicito ainda uma vez mais pela passagem de sua data natalícia - Deus o abençoe

e a toda a sua família -, o Exmo. Sr. Senador Esperidião Amin, Relator de nosso requerimento, o Exmo. Sr. Senador Marcos do Val. Cumprimento as autoridades presentes nesta audiência, tanto as que aqui se encontram como aquelas que nos assistem pela internet.

A minha abordagem, senhoras e senhores, residirá em três tópicos essencialmente.

Primeiro, a descrição de um cenário global e nacional; segundo, algo sobre a atividade de segurança cibernética desenvolvida pelo Governo Federal com o apoio de toda a sociedade, porque esta não é uma atividade, como bem foi frisado pelo Gen. Amin e pelo Gen. Corrêa Filho, que se faça sozinho, de forma isolada; e o papel do Gabinete de Segurança Institucional com relação ao tema.

Bem, em termos globais, temos alguns dados.

Em 2018, mais da metade da população mundial utilizou a internet. Isso significa 4,1 bilhões de usuários, representando 54% da população, sendo que 93% desses acessos se deram por dispositivos móveis. Estima-se ainda que, até 2020, teremos 30 bilhões de equipamentos classificados como pertencentes à Internet das Coisas. Em termos de ataques cibernéticos, estimam-se perdas anuais da ordem de US$600 bilhões. Em consequência disso também há uma previsão de que o mercado mundial de segurança cibernética até 2020 seja avaliado em US$151 bilhões. Isso demonstra a preocupação que o mundo possui em relação a esse tema.

No Brasil, 100% dos órgãos federais e estaduais utilizam a internet. Cerca de 80% dos nossos domicílios, mais ou menos 116 milhões de pessoas, têm acesso à internet. Noventa e oito por cento de nossas empresas utilizam também a rede mundial de computadores. Mas a segurança, de fato, não está no nível que nós queremos.

Segundo relatório da União Internacional de Telecomunicações, o Brasil ocupa o 70º lugar no índice de segurança global. Disso, em 2018, resultou que cerca de 70 milhões de brasileiros foram vítimas de ilícitos cibernéticos.

De 2017 para 2018, tivemos uma perda, em termos financeiros, de empresas nacionais, computando cidadãos inclusive, da ordem de US$20 bilhões - isso no Brasil. E isso resulta no seguinte quadro: o Brasil hoje é o segundo país com maior prejuízo com ataques cibernéticos.

Permitam-me então, senhoras e senhores, entrar na parte de segurança cibernética.

O Gabinete de Segurança Institucional - é importante situar isso também - é responsável pela coordenação das atividades de segurança da informação.

Essa atividade de segurança da informação, conforme a Lei 13.844, que organizou os Ministérios, e também conforme o Decreto 9.637, de 26 de dezembro de 2018, abrange quatro grandes áreas: a segurança cibernética, que é o carro-chefe; a defesa cibernética, que obviamente está a cargo do Ministério da Defesa; a segurança física da informação; e a proteção de dados em termos conceituais, sejam eles pessoais ou sejam eles organizacionais.

A segurança cibernética possui algumas características que a diferem da defesa, mas, sem entrar muito no mérito, ela é baseada na prevenção, essencialmente em ações preventivas. Ela é ilimitada no tempo e no espaço, com características de perenidade, e visa elevar o nível de resiliência de sistemas, instituições e da sociedade em geral. Ela é calcada na proteção, por isso é que tem esse maior viés preventivo, em parte uma exploração, mas não realiza o ataque cibernético. O contra-ataque ao ataque cibernético está a cargo da defesa cibernética.

E o que o Governo, então, vem fazendo acerca disso? Entendendo que é uma atividade estratégica, porque os países entendem assim, e aqui não poderia ser diferente, foi criado, em 2006, na estrutura do Gabinete de Segurança Institucional, 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. E é claro que não paramos por aí. Esses normativos formam um arcabouço interessante e importante, mas eles não são suficientes.

O GSI ainda possui, em termos de segurança cibernética bem especificamente, na estrutura do Departamento de Segurança da Informação, o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo, o CTIR GOV.

Esse é um dos centros de responsabilidade nacional, ele é governamental, e ele possui contato com mais de 300 equipes de tratamento de incidentes no Brasil pertencentes aos órgãos dos Três Poderes, a Estados, Municípios, Distrito Federal, e também integra uma rede global composta por 72 centros de outros países. Isso resulta num monitoramento contínuo dos ataques e dos incidentes cibernéticos contra redes governamentais.

Um número interessante: em 2018 nós tivemos cerca de 9.600 incidentes contra redes governamentais, sendo que, em primeiro lugar, estão as fraudes, *phishings*, tentativas de invasão. Já em 2019, até o momento, foram cerca de 8 mil incidentes cibernéticos envolvendo redes governamentais, sendo que, em primeiro lugar - houve uma inversão - agora

estão os vazamentos. E isso chama muita atenção por conta da preocupação dos órgãos públicos que têm chegado a nós, sobre a Lei Geral de Proteção de Dados Pessoais, porque um dos pilares é, exatamente, claro, a proteção dos dados pessoais, especialmente contra ilícitos cibernéticos, com atenção especial para o vazamento. Esse número aqui, realmente, nos desperta uma grande preocupação, por isso é que estamos atuando, realizando ações de sensibilização, para que essa Lei Geral de Proteção de Dados, que representa uma quebra de paradigma no modo como nós tratamos dados pessoais, realmente possa ser incorporada e possa ser utilizada em sua plenitude pelos órgãos públicos.

Nós também temos emitido alertas, recomendações e estatísticas sobre incidentes cibernéticos. Também temos algumas iniciativas e projetos em andamento.

Em 2018, já foi narrado aqui, houve a publicação do decreto que institui a Política Nacional de Segurança da Informação. Muito embora, como decreto que é, seja voltado para a Administração Pública Federal, visualiza esse *gap*, essa vacância normativa que existe e que foi muito bem citada pelo General Amin, no campo cibernético. Assim, tem servido também, exatamente por sua ênfase na governança, como fonte de inspiração para outras organizações públicas e privadas também.

Em 2019, foi reativado o Comitê Gestor de Segurança da Informação, que é um órgão que tem a finalidade de deliberar sobre esses assuntos de segurança da informação, inclusive cibernética, e, em poucos dias, deverá ser colocada em consulta pública a Estratégia Nacional de Segurança Cibernética. Essa estratégia foi construída com a participação de mais de 40 representantes de órgãos do setor público, do setor privado, inclusive de representante das nossas infraestruturas críticas nacionais, com representantes do meio acadêmico e de outras personagens icônicas da sociedade de notório saber.

Essa estratégia sinaliza claramente a posição do Estado brasileiro, do Governo, sobre qual seria o melhor caminho a ser adotado pelo País para que possa elevar a resiliência de modo assertivo. Essa estratégia é bastante pragmática, ela foge de subjetividades, e ela é calcada, essencialmente, em sete eixos: proteção e segurança; universo conectado seguro; proteções estratégicas; dimensões normativas; pesquisa, desenvolvimento e inovação; dimensões internacionais e parcerias estratégicas; e também aborda, com bastante profundidade, o ramo educacional. Como mencionado pelo Gen. Amin, há essa baixa maturidade, que é consequência de uma baixa cultura em segurança cibernética de toda nossa sociedade; e esse eixo vem exatamente tentar solucionar esse *gap* de maturidade, esse *gap* de cultura, que nós atravessamos.

E é intenção também do GSI, já para o final do ano, elaborar - está em estágio bem avançado - um projeto de lei geral de segurança cibernética. A ideia é que esse projeto de lei realmente traga um alinhamento macropolítico e estratégico para todas as ações de segurança cibernética no País. E, como lei, é claro, terá uma amplitude tal que poderá trazer todos os órgãos e toda a sociedade a um trabalho conjunto na área de segurança cibernética e tratar o tema estratégico como ele deve ser tratado.

Inclusive, 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. Então, na verdade, isso está sendo bastante embasado e nós acreditamos que será um instrumento determinante para atender as necessidades do nosso País nesse quesito.

Com isso, concluo a minha exposição já agradecendo pelo brilhantismo da iniciativa.

Muito obrigado.

O SR. PRESIDENTE (Nelsinho Trad. PSD - MS) - Agradecemos ao Coronel Arthur Pereira Sabbat.

Encerrada a exposição dos palestrantes, vou conceder a palavra aos Srs. Senadores inscritos.

Concedo a palavra ao Senador Esperidião Amin para fazer a sua consideração e eventual pergunta.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Unidos pelo Brasil/PP - SC. Como Relator.) - Em primeiro lugar, eu quero cumprimentar *(Fora do microfone.)* os nossos ilustres palestrantes, convidados especiais, que trazem realmente dados e informações que habilitam, ainda mais, a iniciativa desta Comissão, Sr. Presidente. Eu vou destacar cinco pontos, fazendo referência sempre a quem primeiro falou sobre o assunto, mas que de alguma forma foi respaldado por outros palestrantes.

Então, da exposição do General Amin, que, por ter sido a primeira, inaugurou algumas das preocupações que eu quero aqui salientar, eu destaco, primeiro, a falta de um alinhamento normativo, corroborada essa informação por todos os que o seguiram e com ilustrações muito detalhadas do último palestrante, o Coronel Sabbat, que realmente detalhou essa ausência de normas abrangentes, quando focalizou a questão do que ia ser um projeto de lei geral de segurança de informática, de segurança cibernética e de informação, que resultou num decreto cuja amplitude é restrita ao próprio Governo.

Eu conheço, porque recebi uma explicação pormenorizada desse processo numa visita que recebi, e acho que, realmente, o fato de ter sido editado o decreto num final de Governo justifica que se retomem os fundamentos desse decreto e se pense num projeto de lei abrangente. Pode ser até mais do que um projeto de lei, mas que codifique segurança cibernética

e segurança de dados, uma vez que a informação que o senhor prestou, agora me dirijo ao Coronel Sabbat, de que estamos classificados como o 70º País, ou seja, somos número 70 em matéria de segurança cibernética, nos expondo a todos, portanto, a sociedade, a essa vulnerabilidade, corrobora tudo que foi dito inclusive dos esforços que estão em curso.

Portanto, alinhamento normativo, isso tem a ver com o quê?

Na hora que eu falei do que é necessário, preste atenção aos sinais, Senador Nelsinho Trad, chegou o Mecias, então temos esperanças. Falei da necessidade e o Mecias chegou. Não poderia haver maior oportunidade. *(Risos.)*

Então eu acho que isso é uma responsabilidade legislativa, no mínimo, para provar, e se pudermos estabelecer uma parceria, Presidente, eu acho que nós poderíamos ajudar que esse processo legislativo, que foi retardado pelo incidente já revelado no final do Governo passado, foi retardado por isso, é verdade... Por que não se fez um projeto de lei? Porque era fim de Governo. Fez-se um decreto, lógico, que é uma coisa sensata, mas cuja amplitude é apenas, vamos dizer, chapa branca, não é para a sociedade brasileira, como seria uma lei, mesmo que ela tenha que ser considerada imperfeita, tenha que aperfeiçoar. Isso não vai parar de aperfeiçoar nunca.

Eu queria relatar mais uma vez para os companheiros e para os senhores, que eu fui Relator, eu fui analista de sistemas e programador no tempo do Burroughs, isso no final dos anos 60 e começo dos 70, e consegui concluir o doutorado em engenharia e gestão do conhecimento já com 62 anos de idade. Então eu tenho uma carreirazinha nessa história, nesse brinquedo. Ajudamos a constituir em Santa Catarina um polo de informática que foi, com esse nome, o segundo do mundo, depois de Bari na Itália, e a economia catarinense sofreu grandes benefícios. Eu comentava que quase 7% do PIB de Santa Catarina deriva da tecnologia da informação. Muita gente não sabe que o Guardião é produzido lá, rivalizando, em matéria de tecnologia sensível, com países de ponta no mundo.

Então eu acho que essa parte legislativa é crucial e nós podemos contribuir. O desenvolvimento é outra questão.

O segundo ponto, e aí eu queria me dirigir especialmente ao representante do Ministério da Defesa e a todos os demais, porque é a consequência: a nossa assessoria preparou uma informação que eu gostaria que os senhores filtrassem. No PPA, no Programa Plurianual de 2016/2019, a defesa cibernética está sobre o Programa de Defesa Nacional 2058, inserido no Objetivo 1119: "Desenvolver e elevar capacidades nas áreas estratégicas de cibernética, nuclear, espacial e nas áreas de comunicações, comando e controle, inteligência e segurança da informação". Portanto é civil, militar, eclesiástica, terrestre, marítima e aérea, tendo as iniciativas de: "0500 - Implantação do Comando de Defesa Cibernética" do Exército Brasileiro, e isso aqui foi tudo referido na exposição do General Amin; "05OP - implantação da Escola Nacional de Defesa Cibernética" - todos enalteceram a necessidade de nos educarmos para isso; "05OQ - Implantação do sistema de homologação e certificação de produtos de Defesa Cibernética" - eu até incluiria de documentos também, porque afinal afeta toda a sociedade.

Contudo, no projeto do PPA, que chegou aqui dia 31 de agosto, aliás, dia 30 de agosto, houve um grande processo de simplificação no Orçamento e não há menção à Defesa Cibernética. Vou repetir: na proposta orçamentária, até onde a nossa assessoria leu, e aí, como ensinam os gaúchos: quando um erro cometeres, o que bem se pode dar, não deves ignorar como se sai da enrascada; a culpa é da peonada, o patrão não pode errar; se a informação estiver errada, a culpa é dele. Mas é o que eu recolho.

Essas três iniciativas do PPA 2016/2019 não foram totalmente concretizadas. Elas já existem, mas são muito mais um processo do que um produto. E, para o período 2020/2023, o que nós podemos esperar do PPA? E aí, Senador Nelsinho Trad, mais uma vez convalida a iniciativa que foi tomada, inclusive que pode habilitar a nossa Comissão a apresentar propostas estruturantes para o orçamento da União e para o PPA porque essa prioridade já foi definida ainda no primeiro semestre nesta Comissão. Então, o que esperar e o que seria não o ideal, mas o razoável no orçamento, agora falando do orçamento anual?

Também uma chegada ilustre que eu quero registrar é a do Senador Antonio Anastasia, num momento crucial, porque eu estou falando de orçamento. E todos sabem que os mineiros têm grande capacidade de influenciar os orçamentos públicos do Brasil, especialmente alguém com as credenciais do querido Senador Anastasia.

Então, vou dar três números que eu mencionei ontem: orçamento, R$3,8 trilhões; orçamento da Seguridade Social, R$914 bi; investimentos previstos no orçamento de 2020, R$19 bilhões, ou seja, 0,5% do orçamento. Então, num quadro desse, eu não posso falar em ideal, mas o que seria minimamente necessário para que os passos iniciais, que foram relatados aqui, de 2008 para frente, de 2006 para frente, não sejam interrompidos ou prejudicados estruturalmente no orçamento de 2020 e no PPA.

Terceiro ponto. Eu só queria que um dos senhores enunciasse quais são os seis exercícios que são previstos para o terceiro exercício de ataque cibernético. Foram descritas aqui as quatro áreas, né? Pelo que eu sei, em 2020, nós teremos seis áreas

em vez de quatro. Eu já tinha passado aqui, mas que fique constando nos registros que teremos acrescentados, então, o sistema hídrico, vamos chamar assim, e transportes.

(Intervenção fora do microfone.)

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Unidos pelo Brasil/PP - SC. Para interpelar convidado.) - Não preciso dizer o quanto transporte significa, além dos outros quatro que já foram mencionados. Mas a gente sempre lembra da greve dos caminhoneiros e sabe o que aquilo significou até hoje para a nossa economia. Nós não nos recobramos daquele baque. É a logística, é a circulação.

E, me referindo aí especialmente às palavras do Coronel Éric Cézzane Cólen, o que o senhor quis dizer com essa quarta arma - é uma quarta arma, né? Pelo que eu sei, em alguns países, ela já é a quarta arma mesmo, ou seja, Aeronáutica, Marinha, força terrestre e cibernética. E quais são os prós e os contras dessa definição estrutural - aí uma questão característica das nossas Forças Armadas -, mas qual seria a cogitação, no caso, que o Ministério da Defesa faz a respeito do viés dessa reorganização, que em outros países já resultou na criação de uma quarta Força Armada, que tanto pode ser transversal quanto pode ser uma a mais?

Sobre os dois últimos pontos, eu só quero reforçar, porque já falei dessa nossa fragilidade que é sintetizada nessa classificação como 70º posto. Então, bastaria nós falarmos sobre a população brasileira - hoje nós somos o sexto mais populoso - para mostrar que nós não somos desimportantes para ficarmos tão folgados assim em matéria de cuidados. Nós somos muito importantes. E isso fica mais evidenciado ainda quando a gente faz a seguinte colocação, e eu me dirijo também ao Coronel Éric: eu participei, como Senador, da opção do Sivam. Nós tínhamos o sistema Thomson no Cindacta, não é isso? E migramos, por pressão diplomática do governo americano, nós dissecamos, não houve mensagens cifradas, houve contato pessoal do Presidente Clinton com o Presidente Fernando Henrique Cardoso para influenciar, com facilidades orçamentárias, até construção civil os americanos se dispuseram a financiar, e nós migramos, no caso, do Sisvam para o grande fornecedor Ratio. E eu lembro que, naquele pacote, havia aqueles aviões Avakin, de sistema de controle. Aquilo existe ainda? E aquilo não serve para fiscalizar queimada?

(Intervenção fora do microfone.)

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Unidos pelo Brasil/PP - SC) - Mas se botar um outro componente ali dentro?

O SR. ÉRIC CÉZZANE CÓLEN GUEDES (Para exposição de convidado.) - A área de cobertura de uma aeronave para esse tipo de emprego é muito limitada.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Unidos pelo Brasil/PP - SC) - Muito limitada. Melhor seria o satélite, né?

O SR. ÉRIC CÉZZANE CÓLEN GUEDES - O ideal são os satélites.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Unidos pelo Brasil/PP - SC) - Mas, quando o satélite aponta, não daria para ele colher o detalhe?

O SR. ÉRIC CÉZZANE CÓLEN GUEDES - Hoje a nossa aeronave não tem essa capacidade.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Unidos pelo Brasil/PP - SC) - Não, mas dá para capacitar porque é apenas um *software* a mais.

O SR. ÉRIC CÉZZANE CÓLEN GUEDES - São os sensores diferentes.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Unidos pelo Brasil/PP - SC) - Um sensor e uma programação diferente a partir do constatado pelo satélite. O satélite dá o alarme. Essa aeronave está voando, não está?

O SR. ÉRIC CÉZZANE CÓLEN GUEDES - Sim, senhor.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Unidos pelo Brasil/PP - SC) - Permanentemente?

O SR. ÉRIC CÉZZANE CÓLEN GUEDES - Não, não permanentemente.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Unidos pelo Brasil/PP - SC) - No programa inicial, era permanentemente?

O SR. ÉRIC CÉZZANE CÓLEN GUEDES - Hoje é sob demanda.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Unidos pelo Brasil/PP - SC) - Então, já houve uma modificação. Mas no pacote original era permanente.

Então, eu acho que esse uso múltiplo do pouco que nós temos... O uso múltiplo eu acho que é uma questão que ficou latente.

Finalmente, volto para o ponto inicial. Eu acho que o principal dever nosso é agir no que é da competência do Congresso. Primeiro, orçamento. Nós não podemos ficar omissos diante dessa aparente fragilização orçamentária noticiada pela nossa assessoria técnica. E, segundo, eu acho que nós somos parceiros obrigatórios na formulação dessa política geral de defesa cibernética.

O SR. PRESIDENTE (Nelsinho Trad. PSD - MS) - General Amin, V. Exa. podia responder ao Senador Amin? Vocês ficam em casa.

Marcos do Val, Senador, General.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Unidos pelo Brasil/PP - SC) - General Marcos do Val. Hoje ele está usando uma gravata das Forças Militares.

O SR. PRESIDENTE (Nelsinho Trad. PSD - MS) - É de treinamento essa aí.

Quer fazer alguma pergunta, Senador Mecias?

Não.

Então, com a palavra V. Exa. para fazer as considerações, e eu tenho as perguntas do e-Cidadania para encerrar a nossa reunião.

O SR. GUIDO AMIN NAVES (Para exposição de convidado.) - Obrigado, Sr. Presidente.

Senador, muito obrigado pelas suas considerações. Já vínhamos conversando antes a respeito desses assuntos e eu tenho algumas coisas para agregar aos comentários que o senhor brilhantemente nos expôs.

Com relação a orçamentos primeiro. Na verdade, nós passamos na questão cibernética um período bastante longo envolvidos com questões tipicamente operacionais, com todo o período dos grandes eventos de 2012 a 2016. E era um período em que tínhamos que rapidamente obter capacidades técnicas de proteção de sistemas principalmente, aplicar essas capacidades, para que pudéssemos passar pelos grandes eventos numa situação tranquila.

Nos gráficos que mostramos aqui do Cert.Br, 2014 foi um pico de incidentes no Brasil, e foi justamente o ano da Copa do Mundo. Após esse período, na época, o Comandante Gen. Villas Bôas me chamou no seu posto de comando e me deu a notícia de que eu iria então comandar a defesa cibernética e me passou algumas orientações, orientações essas que permanecem válidas, o General Leal Pujol endossou essas coisas todas, porque nós precisávamos estruturar melhor a demanda, estruturar melhor o nosso planejamento estratégico. Agora que estávamos numa situação que nos permitia parar para pensar um pouco, comparar, fazer estudos comparativos com as soluções de outros países, para podermos definir um delineamento estratégico para a defesa cibernética no Brasil. Isso, sem dúvida, resulta numa estruturação de demanda, uma demanda mais estruturada, mais clara, mais objetiva, e nos permite então partir para as questões de orçamento para poder financiar esse avanço estratégico.

Nós conseguimos uma modificação bastante significativa no PPA, que era o primeiro passo para isso, o PPA 2020/2023. Lá no comando eu proíbo o pessoal de pronunciar a expressão "série histórica" porque nós vínhamos de uma série história de orçamentos realmente bastante acanhada, mas por culpa também de uma demanda não muito bem estruturada.

Agora, com a demanda estruturada, nós partimos, naquele último eslaide que foi mostrado pelo Gen. Corrêa Filho, nós temos aí R$60 milhões para o ano que vem e R$150 nos três restantes. Isso significa, primeiro, uma estimativa, porque nós não completamos ainda a estruturação dessa demanda, mas eu calculo que vai ficar por aí. Primeira conclusão, cibernética é uma coisa que não é muito cara em relação a outras necessidades nossas. E são valores que nós consideramos que seremos capazes de executar com eficiência e com efetividade, principalmente esses valores propostos de R$60 para o ano que vem e R$150 nos três restantes. Então, em termos de orçamento, isso é o que nós esperamos. Vamos agora ver, quando se efetivar a nossa LOA, se realmente esses valores que nós conseguimos colocar no PPA da Defesa serão contemplados.

Com relação ao que o senhor comentou, um exemplo claro do que o senhor comentou é a Alemanha. A Alemanha criou uma quarta força armada, que, na verdade, é um comando informacional, e não só de cibernética; é um comando informacional, que engloba também a cibernética. No nosso caso, eu veria, Senador... A cibernética é bastante transversal a tudo que se faz. Em tudo que há um sistema de TI envolvido, o senhor tem aí uma preocupação cibernética também envolvida. Essa transversalidade gera um sem-número de atores interessados nessa questão, cada um deles com a sua própria linha de comando e subordinação, o que dificulta enormemente a governança disso tudo. Então, a cibernética tem

essa característica. Nós temos que ser, como eu costumo dizer, mais do que conjuntos, ou seja, englobando as três Forças - Marinha, Força Aérea e Exército -, nós temos que ser interagências porque também as infraestruturas críticas têm um papel importante em tudo isso.

Como exemplo, isso não é uma preocupação minha, a primeira prioridade de defesa do US Cyber Command escrita em estratégias publicadas por eles é o setor elétrico americano, é o *grid* de energia americano, que é todo privatizado, inclusive. Então, o senhor veja que até a relação público-privada nessa hora tem que ser revista. As questões de gestão, nós temos que rever as questões de gestão porque o *clock* cibernético anda no mínimo quatro vezes mais rápido que o relógio normal. Então, não há tempo para burocracia, não há tempo para grandes... Nós temos que modernizar essa questão de gestão.

Mas essa necessidade de sermos conjuntos, de sermos interagências, nós não podemos ficar fixados numa questão puramente de defesa. Nós temos que, mesmo sendo um órgão central de um sistema militar de defesa cibernética, que estender a nossa preocupação também às infraestruturas críticas. Haja vista o nosso exercício, que é feito lá e montado inclusive juntamente com o nosso GSI.

Essas questões todas e a transversalidade, na minha opinião, contraindicam que nós passemos para uma solução semelhante à que a Alemanha fez porque é preciso agregar dentro da nossa cibernética esse, digamos, cadinho de culturas organizacionais, essas diferenças de posicionamento que há em todos esses atores nas Forças Armadas e no âmbito civil também. Isso tudo está representado num comando operacional conjunto, ativado permanentemente. Isso tudo vai somar e nos vai permitir uma governança melhor hoje do que estabelecermos uma verticalização dessa questão, que é muito transversal. Então, é melhor nós termos todos embarcados nesse desafio, que as soluções certamente serão melhores.

Com relação aos pontos que o senhor falou, eu creio que...

(Soa a campainha.)

O SR. GUIDO AMIN NAVES - ... abrangi, de certa forma, aquilo que o senhor nos provocou aqui.

Muito obrigado, Senador.

O SR. PRESIDENTE (Nelsinho Trad. PSD - MS) - Agradecemos ao General de Divisão Amin.

Vou aqui reportar as perguntas do e-Cidadania, agradecendo a participação de todos e incentivando, pois aqui, na nossa Comissão, serão sempre bem-vindas as perguntas da população.

Adelson Rodrigo, de Santa Catarina: "O sistema de comunicações das Forças Armadas usa satélites nacionais? Ou passa por satélites estrangeiros?"

Quem pode responder a essa pergunta já se manifeste ao final das outras.

"Quais os avanços na área da defesa cibernética?" Leonardo Toledo, de São Paulo.

Giovanni José, lá da Paraíba: "Quais as principais normas jurídico-legais que regulamentam a defesa cibernética?".

Sônia Beatriz, também do Rio de Janeiro: "Haverá alguma categorização para diferenciar os tipos de crimes cibernéticos?"

Que tipo de punição poderá ser utilizada nesse caso?

Jaqueline Burque, de São Paulo, parabeniza a Comissão: "Ótimo tema". E faz a seguinte pergunta: "Nossa tecnologia é compatível com o programa de defesa cibernética?".

Coronel Aviador Éric para responder à questão dos satélites.

O SR. ÉRIC CÉZZANE CÓLEN GUEDES (Para exposição de convidado.) - Obrigado pela pergunta. Em relação ao satélite, hoje o comando da Aeronáutica opera um satélite de forma conjunta. Hoje nós temos o nosso comando aeroespacial, onde nós temos o SGDC, que é o Sistema Geoestacionário de Defesa, o nosso satélite de comunicação, em que esse satélite presta serviço para as três Forças. Ele faz parte então do nosso programa estratégico de sistemas espaciais. E a parte militar das comunicações de suporte ao Governo, grande parte dela já é utilizada por esse satélite.

Nós temos outras comunicações, principalmente as relacionadas ao sistema de controle de tráfego aéreo, que, sim, nós terceirizamos o emprego da comunicação via satélite. Mas as empregadas em operações militares hoje são utilizadas com satélite sob controle desse comando conjunto, que é um satélite de apoio à defesa.

A SRA. LUCIANA MASCARENHAS DA COSTA MARRONI (Para exposição de convidado.) - Eu gostaria de complementar a resposta. A Marinha, quando apoia a operação de paz da ONU, que é a Unifil, a operação no Líbano, realmente utiliza um satélite, uma constelação Syracuse, que é disponibilizada pela Otan, mas na banda X, que é militar. Então, nesse caso, a gente usa realmente um satélite que é estrangeiro, mas nessa operação específica.

O SR. PRESIDENTE (Nelsinho Trad. PSD - MS) - O General Amin se habilita para responder às demais, em função de a área ser compatível com a sua explanação das perguntas.

O SR. GUIDO AMIN NAVES (Para exposição de convidado.) - Eu vou abranger aqui os temas do Leonardo, Giovanni, Sônia e Jaqueline, mais ou menos, conjuntamente, pois eles têm alguma coisa a ver. Depois, se alguém quiser complementar - o Sabbat, enfim, o restante - acho que poderíamos providenciar isso.

Bom, com relação à tecnologia e avanços na área de defesa cibernética, nós temos, no Brasil, pesquisa acadêmica; nós temos parque industrial, não só em Santa Catarina, como disse o nosso Senador, mas nós temos o porto digital no Recife e em outras áreas dedicadas à pesquisa; nós temos empresas de sucesso nessa área. Então, eu posso dizer que, na cibernética, a tríplice égide funciona muito bem: o Governo, com a necessidade, com a demanda, com o fomento; a academia, com as pesquisas; e as empresas, enfim, fornecendo aquilo de que nós temos necessidade.

Então, há avanços importantes em todas as áreas da cibernética. Nas áreas de proteção, nas áreas de exploração, de inteligência, *softwares*, nós temos programas, temos ferramentas nacionais. Recentemente, no comando, nós trocamos uma ferramenta importante de inteligência cibernética. Era uma ferramenta, um *software* estrangeiro e recentemente estamos trocando por um nacional, desenvolvido por uma empresa, inclusive aqui de Brasília.

Com relação às normas jurídico-legais, discutimos bastante a respeito disso. Nós temos já aí a nossa Política Nacional de Defesa Cibernética, a Política Nacional de Segurança da Informação, que já foi definida, explicada. Nós temos também, no âmbito militar, a doutrina militar, a defesa cibernética, a estratégia de defesa cibernética. Nós temos alguma regulamentação. Já discutimos que é preciso completar esse marco legal. Ele não está completo. Nós precisamos atualizar, precisamos complementar, mas estamos tratando disso.

Com relação aos crimes cibernéticos, há uma observação interessante. É muito difícil... Não é tão fácil quanto parece você diferenciar uma ação entre crime cibernético e uma ação que demande uma ofensa à defesa cibernética do País. Não é tão fácil quanto pareça isso. Há um espectro de ações muito grande. Nas pontas do espectro é mais clara essa diferença. Mas, por exemplo, vou citar aqui aleatoriamente. Uma pessoa, alguém comete um crime, uma fraude contra um banco, num valor de x milhões. Talvez possa ser mais claro que seja um crime, mas essa mesma pessoa faz uma negação de serviço ou tira do ar a câmera de compensação do nosso sistema financeiro. Ela começa a afetar não só o País como um todo, a economia do País como um todo. Isso ainda é um crime ou passa para o campo de uma ação que demanda um agir da Defesa Nacional? Ela começa a ameaçar o Estado como um todo. Então, não é muito fácil caracterizar isso.

De qualquer maneira, existem tipificações legais. A investigação disso normalmente é a cargo da Polícia Federal. Não é, vamos dizer assim, competência nossa investigar, produzir provas e assim por diante. Nós temos a Polícia Federal, que geralmente é encarregada disso. Mas essa categorização existe, como também as punições já estão todas elas definidas, e os crimes tipificados. Mas, como bem disse o Senador Esperidião Amin, essas normas são vivas. Nós nunca estaremos abrindo mão de modernizar, de complementar, enfim, de mudar esse marco legal.

E no final aqui, como eu já disse, a nossa tecnologia é sim bastante compatível com as necessidades da defesa cibernética. Agora, a transversalidade desse assunto não é só internamente no País. Para a defesa cibernética, as fronteiras geográficas não significam muita coisa. Eu quero dizer com isso que é importante interagirmos tanto internamente, no nosso País, quanto externamente, com as nações irmãs e amigas.

Obrigado, Senador.

O SR. PRESIDENTE (Nelsinho Trad. PSD - MS) - Agradecemos o General Amin.

Apenas para informá-los, antes de encerrar, uma lista de convidados para a segunda audiência pública sobre defesa cibernética já foi elaborada pela assessoria técnica, em conjunto com a assessoria do Senador Esperidião Amin, autor desse requerimento. Então, vai haver um representante do Governo; da ICP; Fernando Moura, Secretário Executivo Adjunto da Casa Civil e Coordenador do Comitê Gestor da Infraestrutura de Chaves Públicas brasileira. Vai estar aqui também Cristine Hoepers, Gerente-Geral do Cert.br; Márcio da Silva Nunes, Vice-Presidente do Conselho Administrativo da Associação Nacional de Certificação Digital; Dr. Ricardo Felipe Custódio, professor e supervisor do Laboratório de Segurança em Computação da Universidade Federal de Santa Catarina.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Unidos pelo Brasil/PP - SC) - Esse é o responsável pela sala-cofre dos documentos certificados, com certificação digital, cuja primeira via, digamos assim, está aqui na Casa Civil.

O SR. PRESIDENTE (Nelsinho Trad. PSD - MS) - Perfeito.

Dr. Ricardo Felipe Custódio professor e supervisor do Laboratório de Segurança em Computação da universidade, conforme bem acabou de relatar o Senador Esperidião Amin.

O Sr. Fabio Reis Cortes, Operador Nacional do Sistema do setor elétrico e Coordenador de Gerência de Arquitetura e Segurança de TI; além de Marcos Lopes, do Serviço Federal de Processamento de Dados; Ilmo Doccine, de empresa do setor de telecomunicações e Professor da Unicamp; e Paulo Felipe Barbosa de Morais, Febraban.

A princípio, essa audiência está marcada para o dia 26 deste mês.

Encerro essa parte, com a participação daqueles que aqui estão na Mesa.

Agradeço, mais uma vez, a participação de todos. Em especial, ao General de Divisão Guido Amin Naves, à Contra-Almirante Luciana Mascarenhas, ao General de Brigada Ivan de Sousa Corrêa Filho, ao Coronel Aviador Éric Cólen e ao Coronel Arthur Pereira Sabbat.

Encerro essa parte da audiência pública.

Posteriormente, entraremos na nossa pauta, pois temos alguns assuntos a serem debatidos.

Apenas para informar, recebemos aqui o convite do General de Divisão Fábio Benvenutti Castro, que convida a nós, ao Senador que se interessar, para participarmos de uma visita ao Comando Militar do Norte, Fronteira Norte, no período de 12 a 13 de setembro - ou seja, daqui a sete dias - de 2019. A visita terá como objetivo permitir o conhecimento da realidade regional, propiciando a verificação da importância estratégica do Exército Brasileiro na Amazônia e conhecer as peculiaridades das atividades desenvolvidas pela Força Terrestre na faixa de Fronteira. Como o assunto está em moda, eu penso que poderá ser de grande proveito a todos que dela puderem participar.

Senador Amin.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Unidos pelo Brasil/PP - SC) - Antes de encerrar, além de reiterar o agradecimento que V. Exa. presta, eu creio que, para a reunião do dia 26, os nossos convidados de hoje são fundadores desse esforço. De forma que, pessoalmente ou através de representante, a presença deles é indispensável para que não se perca a continuidade da coisa.

E nós pretendemos, nessa segunda reunião, agregar as observações, sugestões, propostas, indicação de eficiência ou de deficiência por parte desse segmento, digamos, mais civil do que governamental, ainda que muitos exerçam funções públicas, como é o caso do ICP. O ICP é uma interface, em que um agente de governo opera com documentação privada e também governamental, mas subsidiariamente. É um esforço para fazer a conexão do público com o privado e do militar com o civil na nossa sociedade.

Então, considerem-se convidados. Se um dos senhores não puder vir, designe alguém informado da reunião de hoje para que haja essa continuidade, sob pena de... Como nós temos projetado as cinco grandes reuniões, é importante que se dê continuidade para, no final, conseguirmos produzir um documento lógico, substancial, útil sobre a avaliação da política.

O SR. PRESIDENTE (Nelsinho Trad. PSD - MS) - V. Exa., tabelando, como sempre faz, e completando as intenções que esta Presidência sempre encaminha, captou a minha mensagem. Foi exatamente por isso que eu quis ler os convidados da próxima audiência pública, justamente para fazê-los convidados também, como V. Exa. completou.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Unidos pelo Brasil/PP - SC) - Além de reiterar os cumprimentos, eu quero dizer o seguinte: depois que eu vi a reação do Senador Cid Gomes, eu fiquei mais ligado ainda.

O SR. PRESIDENTE (Nelsinho Trad. PSD - MS) - É, eu vou esclarecer esse assunto, porque eu sou médico cirurgião-geral, urologista, e tive 17 anos de pronto-socorro. Quando eu fui fazer o primeiro atendimento ao Senador Cid Gomes, no Plenário, realmente isso aconteceu, mas foi bom, porque, de um lado, estava um ortopedista fazendo as manobras para que ele pudesse se restabelecer; e, defronte a ele, um urologista. Quando ele soube das especialidades, na hora, ele se levantou e falou que já estava bom. *(Risos.)*

Declaro encerrada essa parte da reunião, convidando as autoridades para uma foto oficial aqui na frente, com os Senadores. *(Pausa.)*

O SR. PRESIDENTE (Nelsinho Trad. PSD - MS) - Srs. Senadores, estamos entrando na segunda parte, deliberativa.

Item 1.

Mensagem 43, de 2019.

A pedido do Relator, Senador Chico Rodrigues, a escolha da Sra. Maria Clara Duclos Clarisio, Ministra de Primeira Classe da Carreira de Diplomata do Ministério das Relações Exteriores, para exercer o cargo de Embaixadora do Brasil junto à República Cooperativa da Guiana, vamos adiar essa matéria, porque ele faz questão de proferir o relatório pessoalmente.

Em função de compromisso que ele assumiu hoje, ele não pôde estar presente. Então, assim será feito.

2ª PARTE

ITEM 2

MENSAGEM (SF) N° 44, DE 2019

- Não terminativo -

Submete à apreciação do Senado Federal, de conformidade com o art. 52, inciso IV, da Constituição, e com o art. 39, combinado com o parágrafo único do art. 41 da Lei nº 11.440, de 2006, a escolha do Senhor LINEU PUPO DE PAULA, Ministro de Primeira Classe da Carreira de Diplomata do Ministério das Relações Exteriores, para exercer o cargo de Embaixador do Brasil junto à Bósnia e Herzegovina.

Autoria: Presidência da República e outros

Relatoria: Senador Humberto Costa

Concedo a palavra ao Senador Humberto Costa para proferir o seu relatório.

O SR. HUMBERTO COSTA (Bloco Parlamentar da Resistência Democrática/PT - PE. Para proferir relatório.) - Sr. Presidente, Sras. Senadoras, Srs. Senadores, esta Casa do Congresso Nacional é chamada a deliberar sobre a indicação que o Presidente da República faz do Sr. Lineu Pupo de Paula, Ministro de Primeira Classe Carreira de Diplomata do Ministério das Relações Exteriores, para exercer o cargo de Embaixador do Brasil junto à Bósnia e Herzegovina.

A Constituição atribui competência privativa ao Senado Federal para examinar previamente e por voto secreto a escolha dos chefes de missão diplomática de caráter permanente (artigo 52, inciso IV). Nesse sentido e observando o preceito regimental para a sabatina, o Ministério das Relações Exteriores encaminhou o currículo do diplomata, bem como informações sobre o país no qual deverá servir.

O indicado é filho de Reynaldo de Paula Júnior e Eufélia Camargo Pupo de Paula e nasceu em 11 de maio de 1954, em São Paulo, capital. É bacharel em direito pela Pontifícia Universidade Católica de São Paulo, formado em 1979. Iniciou sua carreira como Terceiro-Secretário em 1982, após conclusão do Curso de Preparação à Carreira de Diplomata do Instituto Rio Branco (IRBr). Ascendeu a Conselheiro em 2001, a Ministro de Segunda Classe em 2005 e a Ministro de Primeira Classe em 2013.

Entre as funções desempenhadas na Chancelaria, destacam-se: coordenador da Coordenação de Patrimônio (2000); e subchefe do Gabinete do Ministro de Estado das Relações Exteriores (2005).

No Exterior, exerceu, entre outros, os cargos de primeiro-secretário na Embaixada em Buenos Aires (1997); encarregado de negócios na Embaixada em São Salvador (2003); Ministro-Conselheiro na Missão Junto à Organização dos Estados Americanos [OEA (2007)]; encarregado de negócios na Embaixada do Brasil e Tegucigalpa (2010); cônsul-geral no Consulado-Geral do Brasil em Caracas; e, desde 2014, embaixador em Georgetown.

No tocante à Bósnia e Herzegovina, extraímos das informações prestadas pelo Itamaraty resumo para subsidiar os membros da Comissão em sua sabatina ao indicado.

O país é uma república parlamentarista localizada na península balcânica situada no Sudeste da Europa e conta com 3,871 milhões de habitantes.

Essa população formada por bósnios muçulmanos (50,1%), bósnio sérvios (30,8%), bósnios croatas (15,4%) e outros judeus, ciganos etc. (3,7%) - encontra-se nas duas entidades que compõem o Estado: a República Sérvia e a Federação da Bósnia. Os grupos étnicos referidos falam diferentes línguas e professam distintas religiões. Esse contexto, torna a unidade da nação um permanente desafio.

A Bósnia-Herzegóvina, uma das repúblicas integrantes da antiga Iugoslávia, tornou-se independente em 1992. No mesmo ano, teve início a Guerra da Bósnia (1992/1995). O conflito opôs sérvios e uma aliança mulçumana-croata. Os sérvios praticaram a limpeza étnica como estratégia de guerra. Em 1993, a Croácia entra no conflito e reivindica parte do território bósnio. Depois, volta-se contra a Sérvia. O agravamento da luta armada leva a Organização do Tratado do Atlântico Norte (Otan) a intervir. A conflagração termina em novembro de 1995.

No tocante às relações bilaterais, elas remontam a 1992, momento em que o Brasil reconheceu o novo Estado quando do seu ingresso na Organização das Nações Unidas (ONU). Em 1995, ambos os países estabeleceram formalmente relações diplomáticas. Na sequência desses fatos, o Brasil abre embaixada residente em Sarajevo no ano de 2010. Trata-se da única embaixada residente de país latino-americano na capital Bósnia.

As relações ainda são bastante incipientes tanto no plano econômico quanto no cultural. Há, no entanto, possibilidade de expansão nesses domínios, à vista, sobretudo, da forte empatia entre bósnios e brasileiros. Nesse sentido, o entusiasmo comum pelo futebol tem resultado em divulgação positiva do Brasil. Esse quadro reflete nas trocas comerciais com a ampliação, por exemplo, nas vendas diretas de café brasileiro. O comércio bilateral, contudo, segue sendo bastante tímido. Em 2018, exportamos US$2,5 milhões - minérios, metais, máquinas - e importamos US$722 mil - máquinas, ferramentas, papel, couro, têxteis.

Em relação aos assuntos consulares, estima-se em cerca de 30 pessoas a comunidade brasileira no país, que conta com o serviço consular da embaixada.

Tendo em vista a natureza da matéria, essa apreciação cinge-se ao caráter de relatório, o qual se destina, essencialmente, a instruir a sabatina por S. Exas., as Sras. e Srs. Senadores membros desta Comissão, não cabendo serem aduzidas outras considerações.

É esse o relatório, Sr. Presidente.

O SR. PRESIDENTE (Nelsinho Trad. PSD - MS) - Agradecemos ao Senador Humberto Costa, também assíduo nesta Comissão, pelo relatório ora lido.

Em discussão a matéria. *(Pausa.)*

Não havendo quem queira discutir, fica concedida vista coletiva, nos termos do art. 383 do Regimento Interno do Senado Federal.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Unidos pelo Brasil/PP - SC) - Sr. Presidente...

O SR. PRESIDENTE (Nelsinho Trad. PSD - MS) - Pois não, Senador Amin.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Unidos pelo Brasil/PP - SC) - ... eu quero me congratular com o relatório do Senador Humberto Costa. Eu acho que é uma missão diplomática muito importante do ponto de vista daquilo que se chama história sensível. A capital da Bósnia é Sarajevo, cujo nome evoca o início da guerra de 1914.

Eu queria aproveitar a oportunidade para registrar - acho que é muito interessante para a Comissão de Relações Exteriores - que hoje à tarde nós teremos um debate sobre reforma tributária e queria ressaltar até a origem de dois dos grandes debatedores de hoje: o nosso querido ex-Deputado Luiz Carlos Hauly, que é o protagonista da reforma tributária que tramita no Congresso, e o criador da tecnologia de informação que, se aplicada à reforma tributária, como nós pretendemos, afinal o nosso Relator Roberto Rocha está cuidando disso, significará, só a simplificação tecnológica - nós há pouco falamos sobre cibernética, sobre defesa cibernética -, pode representar entre 0,5% e 1% do PIB de ganho, que é o Dr. Miguel Abuhab. O que eu destaco é que é uma extraordinariamente bem-vinda conjugação de talentos dos dois lados do Rio Jordão, ou seja, a origem do Hauly é libanesa e a origem muito destacada e ilustre do Miguel Abuhab é dos melhores rabinos de Haifa e, de um modo geral, da nação israelense. Então, acho que é um bom sinal essa coligação. Eu acho que quando os primos de lá se entenderem, como eles estão bem entendidos, vai sobrar pouca coisa para os outros.

O SR. PRESIDENTE (Nelsinho Trad. PSD - MS) - Fica, com muito prazer, registrada a presença das ilustres personalidades na nossa reunião da Comissão de Relações Exteriores.

Srs. Senadores, eleição do vice-presidente.

Conforme comunicado às senhoras e aos Srs. Senadores na reunião anterior, como manda o Regimento, com a saída do Senador Marcos do Val do Cidadania, houve a vacância do cargo de vice-presidente da Comissão, e será necessária a realização da nova eleição. Foi registrada apenas a candidatura do Senador Marcos do Val para a Vice-Presidência, agora no Podemos.

Consulto as Sras. e o Srs. Senadores se podemos eleger o referido colega, por aclamação, tendo em vista que há apenas um candidato.

Os Senadores que concordam permaneçam como se encontram. *(Pausa.)*

Aprovado.

O SR. ESPERIDIÃO AMIN (Bloco Parlamentar Unidos pelo Brasil/PP - SC. Pela ordem.) - Na condição de cabo eleitoral do Senador Marcos do Val, peço que nem mesmo o Senador Humberto Costa conteste essa unanimidade. *(Risos.)*

O SR. PRESIDENTE (Nelsinho Trad. PSD - MS) - O Senador Humberto Costa é da paz. Quem não enxergou isso é míope.

Então, havendo o acordo de todos, declaro eleito, por aclamação, para a Vice-Presidência da Comissão de Relações Exteriores e Defesa Nacional, o nobre Senador Marcos do Val.

Uma salva de palmas. *(Palmas.)*

Deliberação da ata da reunião anterior.

Proponho ainda a dispensa da leitura e aprovação da ata anterior.

Os Senadores que concordam permaneçam como se encontram. *(Pausa.)*

Aprovada.

Antes de encerrar a reunião, comunico aos Srs. Senadores que foi criada a subcomissão temporária, conforme aprovado pelo Requerimento nº 52, de 2019, de autoria do Senador Jaques Wagner, para, no prazo de 60 dias, informar-se inteiramente sobre a tentativa de favorecimento ilegal a uma empresa brasileira que atua na área de energia, a Léros, à qual fora prometida a venda de energia excedente do Paraguai no mercado livre de energia do Brasil a preços e condições imbatíveis, gerando grande sensibilidade política no contexto das relações bilaterais Brasil-Paraguai.

A Subcomissão é composta pelos seguintes membros: titulares: Senador Jaques Wagner, Senador Telmário Mota e Senador Nelsinho Trad; suplentes: Senador Antonio Anastasia, Senadora Soraya e Senador Chico Rodrigues. Esses foram os interessados que se manifestaram para fazer parte dessa Comissão.

Faremos a eleição, numa próxima oportunidade, do Presidente e do relator dessa Subcomissão.

Agradecemos a todos pela presença.

Declaro encerrada a presente reunião, agradecendo as manifestações de carinho de todos em função do nosso aniversário. Não poderia ser destino melhor neste meu dia do que estar cheio de estrelas aqui ao meu lado durante a reunião.

Muito obrigado.

Está encerrada a reunião.

(Iniciada às 9 horas e 30 minutos, a reunião é encerrada às 11 horas e 35 minutos.)