SENADO FEDERAL
Secretaria-Geral da Mesa

ATA DA 3ª REUNIÃO DA SUBCOMISSÃO PERMANENTE DE DEFESA CIBERNÉTICA DA 2ª SESSÃO LEGISLATIVA ORDINÁRIA DA 57ª LEGISLATURA, REALIZADA EM 18 DE JUNHO DE 2024, TERÇA-FEIRA, NO SENADO FEDERAL, ANEXO II, ALA SENADOR ALEXANDRE COSTA, PLENÁRIO Nº 7.

Às quinze horas e três minutos do dia dezoito de junho de dois mil e vinte e quatro, no Anexo II, Ala Senador Alexandre Costa, Plenário nº 7, sob a Presidência do Senador Esperidião Amin, reúne-se a Subcomissão Permanente de Defesa Cibernética com a presença dos Senadores Fernando Dueire, Sergio Moro e Astronauta Marcos Pontes, e ainda dos Senadores Weverton, Izalci Lucas, Angelo Coronel, Professora Dorinha Seabra, Paulo Paim, Zenaide Maia e Marcos do Val, não-membros da comissão. Deixa de comparecer o Senador Nelsinho Trad. Havendo número regimental, a reunião é aberta. A presidência submete à Comissão a dispensa da leitura e aprovação da ata da reunião anterior, que é aprovada. Passa-se à apreciação da pauta: **Audiência Pública Interativa**. **Finalidade:** Debater os seguintes temas: I – Política Nacional de Cibersegurança: Estratégia Nacional de Segurança Cibernética e Plano Nacional de Cibersegurança; II – Relações entre Segurança e Defesa Cibernética; e III – Anteprojeto de lei sobre Política Nacional de Cibersegurança (PNCiber) e o Sistema Nacional de Cibersegurança (SNCiber). **Participantes:** Senhor Marcos Antonio Amaro dos Santos, Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República (GSI); e Senhor André Luiz Bandeira Molina, Secretário de Segurança da Informação Cibernética. **Resultado:** Audiência Pública Interativa realizada. Nada mais havendo a tratar, encerra-se a reunião às dezesseis horas e dezesseis minutos. Após aprovação, a presente Ata será assinada pelo Senhor Presidente e publicada no Diário do Senado Federal, juntamente com a íntegra das notas taquigráficas.

Senador Esperidião Amin
Presidente da Subcomissão Permanente de Defesa Cibernética

Esta reunião está disponível em áudio e vídeo no link abaixo:
http://www12.senado.leg.br/multimidia/eventos/2024/06/18

SENADO FEDERAL
Secretaria-Geral da Mesa

NOTAS TAQUIGRÁFICAS REVISADAS

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC. Fala da Presidência.) – Havendo número regimental, declaro aberta a 3ª Reunião da Subcomissão Permanente de Defesa Cibernética da 2ª Sessão Legislativa Ordinária da 57ª Legislatura, conforme pauta publicada.

Antes de iniciarmos, proponho a dispensa da leitura e a aprovação da Ata da 2ª Reunião da Subcomissão, ocorrida no dia 21 de maio de 2024.

As Sras. Senadoras e os Srs. Senadores que a aprovam permaneçam como se encontram. (*Pausa.*)

Não havendo nenhuma manifestação, está aprovada e será publicada.

Conforme pauta publicada, a presente audiência pública tem como objetivos:

I. Debater a Política Nacional de Cibersegurança, a Estratégia Nacional de Segurança Cibernética e o Plano Nacional de Cibersegurança;

II. As relações entre segurança e defesa cibernética;

III. O anteprojeto de lei sobre a Política Nacional de Cibersegurança (PNCiber) e o Sistema Nacional de Cibersegurança.

Para tanto, recebe como convidado o Exmo. Sr. Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República, Marcos Antonio Amaro dos Santos.

A reunião será interativa, transmitida ao vivo e aberta à participação dos interessados, por meio do Portal e-Cidadania, na internet, em senado.leg.br/ecidadania ou pelo telefone da ouvidoria: 0800 0612211.

Já temos a honra de contar aqui com a presença do Sr. Ministro General Marcos Antonio Amaro dos Santos, e me cabe esclarecer que será dada a palavra ao Sr. Ministro, pelo tempo que julgar necessário, para a sua exposição.

Em seguida, abriremos a fase de interpelações por Senadores ou Senadoras e inscritos, em prazo de até cinco minutos.

Na sequência, o Sr. Ministro terá igual prazo para resposta.

Cabendo, réplica e tréplica também serão reguladas.

Quero ainda registrar que se encontra conosco na mesa o Sr. André Luiz Bandeira Molina, Secretário de Segurança da Informação e Cibernética. Eu tive a honra de o ter como companhia, em recente missão na Cidade do Panamá.

Já antecipo que nós distribuímos um convite aos integrantes da Subcomissão, ou seja, o Senador Sergio Moro, de quem faço a questão de registrar a presença e convidá-lo para ficar aqui conosco, se desejar; o Senador Nelsinho Trad; o Senador Fernando Dueire; o Senador Chico Rodrigues e o Senador Marcos Pontes receberam cópia de um convite enviado por Digi Americas Alliance, que está sob escrutínio dos queridos membros.

Registro aqui a presença do nosso nobre companheiro Fernando Dueire. Fazia menção ao convite que eu fiz chegar a todos, para que avaliem a conveniência de nos fazermos presentes e quem, eventualmente, deseja estar presente nesse evento, que deverá ser realizado nos dias 8 e 9 de agosto.

Próximos.

Registrando mais uma vez a presença dos Senadores Sergio Moro e Fernando Dueire, eu passo a palavra ao ilustre Ministro Marcos Antonio Amaro dos Santos, para que se desincumba da tarefa para a qual foi convidado.

O SR. MARCOS ANTONIO AMARO DOS SANTOS (Para expor.) – Muito obrigado, Exmo. Sr. Senador Esperidião Amin, Presidente da Subcomissão Permanente de Defesa Cibernética, da Comissão de Relações Exteriores e Defesa Nacional. Sr. Senador Sergio Moro, Senador Fernando Dueire, muito obrigado pela presença, prestigiando também esta atividade; Senador Astronauta Marcos Pontes, membro também desta Subcomissão, que está ausente aqui neste auditório, mas nos acompanha por videoconferência.

Senhoras e senhores, é uma satisfação para o Ministro Chefe do Gabinete de Segurança Institucional estar presente aqui nesta Subcomissão, para trazer informações relacionadas às atividades, a esta temática tão importante que é a segurança cibernética no nosso país. Eu farei uma apresentação em cerca de 30 minutos, eu espero. E, posteriormente, Senador, eu me colocarei totalmente à disposição, com a minha equipe também.

Eu destaco também aqui a presença do nosso Secretário-Executivo, General Corrêa Filho, que tem conhecimento bastante aprofundado na área. Temos ali também o nosso Brigadeiro Luiz Fernando, que tem muito conhecimento na área de segurança cibernética, e nosso Assessor Especial

Marcelo Malagutti, também. Estão todos aqui em condições de trazer todas as informações que forem de interesse desta Subcomissão, no que se trata de segurança cibernética do nosso país.

Então, eu passarei aqui a apresentar alguns eslaides, Senador, até para motivar os debates, já trazendo também algumas informações, alguns esclarecimentos sobre esta matéria, conforme foi designado pelo senhor. Eu vou seguir esse sumário e, como eu disse, espero apresentar esses pontos aí em cerca de 30 minutos. Posteriormente, nós nos colocaremos à disposição para os questionamentos que se façam de interesse dos senhores.

Apresentarei, rapidamente, a estrutura organizacional do GSI, para entendermos por que o GSI se envolve com esta temática; falarei da segurança da informação e cibersegurança de maneira geral no Brasil; farei uma síntese da Política Nacional de Cibersegurança: os princípios e objetivos, os instrumentos da PNCiber e o Comitê Nacional de Cibersegurança; trarei alguns fatos e dados relacionados a esta temática; e apresentarei algumas perspectivas antes de concluirmos.

Então, quanto à estrutura organizacional do Gabinete de Segurança Institucional da Presidência da República (GSI), eu destaco aquelas duas secretarias: a Secretaria de Acompanhamento e Gestão de Assuntos Estratégicos (Sagae) e a Secretaria de Segurança da Informação e Cibernética (Ssic). As outras duas secretarias, que são também importantes logicamente: a Secretaria de Segurança Presidencial não tem muito a ver com esta temática de segurança cibernética, por isso eu não vou detalhá-la, tampouco aquela Secretaria de Coordenação de Assuntos Aeroespaciais.

Em relação à Sagae – como chamamos aquela secretaria, a segunda ali –, nós temos o Departamento de Assuntos do Conselho de Defesa Nacional, e o outro departamento, que também se envolve com esta temática, o Departamento de Assuntos da Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo (Dacreden). Cito a primeira, por ter, no seu bojo, aquela Coordenação-Geral de Apoio ao CDN – Conselho de Defesa Nacional –; e a segunda, por ter a Coordenação-Geral de Segurança de Infraestruturas Críticas, que também trata, logicamente, de segurança cibernética, tendo em vista que essa é uma ferramenta, vamos dizer assim, não ferramenta, mas uma temática que é transversal a todas as infraestruturas críticas.

Já no lado direito, na Secretaria de Segurança da Informação e Cibernética, nós temos dois departamentos: o Departamento de Segurança da Informação, com aquelas duas coordenações gerais – Coordenação-Geral do Núcleo de Segurança e Credenciamento e Coordenação-Geral de Gestão de Segurança da Informação –; e, mais ainda enfronhada com essa temática, o Departamento de Segurança Cibernética, com aquelas duas coordenações gerais.

Então, logicamente, essa quarta secretaria, a Secretaria de Segurança da Informação e Cibernética, é aquela que mais está envolvida com a temática de segurança cibernética, mas também aquela secretaria, Sagae, por termos ali aqueles dois departamentos que têm relação também com essa temática de segurança, especialmente o Departamento de Assuntos Dacreden, por causa da segurança de infraestruturas críticas.

Segurança da Informação e Cibersegurança no Brasil.

Estabeleço aqui uma primeira ideia da distinção que existe entre ciberdefesa – ou defesa cibernética – e cibersegurança – ou segurança cibernética. É uma diferença apenas de conceito. A segurança cibernética tem uma amplitude, tem um escopo maior.

Então, no nosso nível aqui, no nível Presidência da República, nós temos lá o Gabinete de Segurança Institucional, que trata desta temática num nível, logicamente, de governança desse sistema, num nível de gestão.

Depois, vendo já o aspecto mais relacionado ao Ministério da Defesa, com as Forças Armadas, o nível estratégico. Temos lá o Comando de Defesa Cibernética, que é um comando conjunto que envolve as três Forças Armadas, no âmbito do Ministério da Defesa.

Descendo para os níveis operacional e tático, são os comandos subordinados que possam ser estabelecidos, num caso do emprego de um comando conjunto. Temos lá, então, o nível operacional, guerra cibernética, o nível tático, uma força conjunta de guerra cibernética, por exemplo, já num nível de menor escalão.

Então, a diferença básica ali, no nível mais abrangente, a segurança cibernética; e, num nível específico do Ministério da Defesa, a defesa cibernética.

Vou fazer aqui um breve histórico da segurança da informação e cibersegurança no Brasil.

Começando ali, tem muitos documentos, muitas iniciativas ao longo de cerca de 20 anos – mais de 20 anos, na realidade, quase 30 anos já.

Começa ali em 1995, com a criação do primeiro Csirt brasileiro, a criação lá do Comitê Gestor da Internet do Brasil, através de uma portaria ainda.

Já em 1997, foi criado lá o Cert.br, o Cais, que é o Centro de Atendimento a Incidentes de Segurança, da Rede Nacional de Ensino e Pesquisa.

Depois, ali, uma diretriz do Mare, ministério antigo de reforma do estado, o Ministério da Administração e Reforma do Estado, estabelecendo a segurança da informação no Poder Executivo federal.

Em 2000, a primeira política de segurança da informação na administração pública federal, já no Gabinete de Segurança Institucional da Presidência da República, por meio daquele Decreto 3.505.

Competências estabelecidas através de leis ao GSI, já em 2002. Então, é aquela lei de organização da Presidência da República e dos Ministérios, estabelecendo na lei esta competência do GSI para tratar da temática de segurança da informação.

Em 2003, a elaboração, o aprimoramento do Comitê Gestor da Internet no Brasil, já por meio de um decreto.

Em 2004, a criação do Ctir Gov – Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos –, da rede de Governo, através ainda de uma portaria do GSI, em 2004; e posteriormente, em 2005, o Estatuto NIC.br, que é a organização que é gestora do Comitê Gestor da Internet, que tem sob a sua responsabilidade o Comitê Gestor da Internet e também o Cert.br.

O Dsic era um Departamento de Segurança da Informação e Comunicações, à época, no GSI, por meio daquele decreto, em 2006. Hoje, o Dsic já é um Departamento de Segurança da Informação e Cibernética, não mais de comunicações, mas foi criado dessa forma, naquela oportunidade.

Destaco ali que, em cor laranja, são atividades ou entidades da sociedade civil; em azul, o Governo Federal e em laranja, a academia, mais amarelada.

Continuando, ainda nesta linha do tempo: em 2011, Lei de Acesso à Informação, uma lei que tem enorme aplicação, ainda nos dias de hoje, logicamente. A criação daquele Núcleo de Segurança e Credenciamento do GSI, que trata de informação classificada.

Já em 2012, dispõe sobre o Núcleo de Segurança e Credenciamento, por meio de um decreto, e estabelece o GSI, o Ministério Chefe do GSI, como Autoridade Nacional de Segurança, para fins de acordos e tratados entre governos. Normalmente, é o Ministério Chefe do GSI que assina esses acordos de troca e proteção mútua de informação classificada, fruto deste decreto.

O marco civil da internet, também de grande importância, a Lei nº 12.965, de 2014. Já a segunda política de segurança da informação, Política Nacional de Segurança da Informação, da Administração

Pública Federal, no GSI, por meio de um decreto, e a Lei Geral de Proteção de Dados, em 2018, Lei nº 13.709.

Foi criada também, fruto da lei, a Autoridade Nacional de segurança de Dados, de Proteção de Dados, já estabelecida.

Em 2019, competência de segurança cibernética, também estabelecida ao GSI, na Lei nº 13.844. É a lei também de organização da Presidência e dos Ministérios, cada vez que se renova o que está em decreto, é colocado já como competência na lei.

Criação da rede, melhor, da estratégia cibernética, ou seja, da primeira Estratégia Nacional de Segurança Cibernética, Decreto nº 10.222, que era para ter uma validade de quatro anos, então: 2020, 2021, 2022 e 2023. Ela já está desatualizada – vamos dizer assim – e já está em andamento o trabalho do Comitê Nacional de Cibersegurança para revisar essa estratégia.

Em 2021, foi criada a Regic, Rede Federal de Gestão de Incidentes Cibernéticos na área do Governo, uma rede importante também por onde transitam recomendações estabelecidas, pelo Ctir Gov, da Presidência da República.

Em 2022, então, bastante recente aquele Cisc, no âmbito do Ministério da Gestão e Inovação, na Secretaria de Governo Digital (SGD) do Ministério da Gestão e Inovação. Foi criado o Cisc – Centro Integrado de Segurança Cibernética – que trata especificamente dos órgãos vinculados ali ao Ministério da Gestão, todo o sistema de tecnologia da informação que é vinculado ao Ministério da Gestão e Inovação, então, a segurança cibernética é coordenada por aquele órgão atualmente.

Já em 2023, como sabemos, no final do ano passado, em 26 de dezembro, é estabelecida a Política Nacional de Cibersegurança, pelo Decreto 11.856.

A Lei 14.600, a última lei de organização da Presidência da República e Ministérios, estabelece também a Secretaria de Segurança da Informação e Cibernética. É também colocada na lei, agora, a secretaria; antes, era um departamento. Pela primeira vez, aumentando o escopo, o departamento se transformou, então, em uma secretaria.

Já no âmbito da defesa nacional, como a gente fez aquela distinção entre defesa cibernética e segurança cibernética, estamos vendo, agora, as iniciativas, no âmbito da defesa. Começando, lá em 2005, aquela não é a primeira Política de Defesa Nacional, a primeira foi estabelecida em 1996. A

gente não colocou também todas ali, apenas as mais aproximadas, em relação à temática de cibersegurança.

Em 2008, temos a Estratégia Nacional de Defesa. Um decreto estabelece a estratégia e também estabelece que ficaria a cargo da Força Aérea a temática aeroespacial e, logicamente, o Programa Espacial Brasileiro; a cargo da Marinha, o Programa Nuclear Brasileiro; e para o Exército Brasileiro, a temática de segurança cibernética – de cibernética, é melhor –, no âmbito da Defesa, Defesa Cibernética, portanto.

Diretriz Ministerial atribui ao EB o setor cibernético, em 2009.

Já em 2010, é criado o Projeto Estratégico do Exército de Defesa Cibernética e também o Centro de Defesa Cibernética. Essas iniciativas já tinham em vista os grandes eventos que aconteceriam no Brasil, a Olimpíada, a Copa do Mundo, aqueles grandes que exigiam essa estrutura estabelecida quando da sua ocorrência.

Prosseguindo, ainda, na área de defesa cibernética, com a Política Cibernética de Defesa, uma portaria ministerial, lá do Ministério da Defesa, há nova Política Nacional de Defesa, nova Estratégia Nacional de Defesa – a revisão.

Ali há a criação do Programa de Defesa Cibernética na Defesa Nacional. É conveniente destacar que existem dois programas de defesa cibernética. Há um no nível conjunto, no nível Ministério da Defesa. É um programa conjunto esse de que estamos falando aí, com a ComDCiber, na área do Comando de Defesa Cibernética. Ademais, existe um programa também estratégico singular, no âmbito do Exército Brasileiro, cada um cuidando da sua parte, uma parte conjunta, outra parte singular.

Há a ativação do Comando de Defesa Cibernética, no ano 2016, com o ComDCiber. Em 2017, dá-se a instituição do Programa Estratégico do Exército de Defesa Cibernética, em comparação com aquele outro que eu acabei de citar, que é o conjunto, o programa conjunto.

O 1º Exercício do Guardião Cibernético, talvez, seja o maior exercício de segurança cibernética do mundo esse Guardião Cibernético. O primeiro aconteceu, em 2018, e nós estamos indo já para a sexta versão do exercício no corrente ano.

Com a criação do Sistema Militar de Defesa Cibernética, há nova Política Nacional e nova Estratégia Nacional de Defesa. Já também ali está a Doutrina Militar de Defesa Cibernética, estabelecida, em 2023.

Então, era essa pequena lembrança, nessa linha do tempo, dessas iniciativas, nessas duas áreas: segurança cibernética e defesa cibernética.

Vamos falar um pouquinho, então, agora da Política Nacional de Cibersegurança, começando ali pelos princípios e objetivos.

Como citei anteriormente, essa política foi aprovada dia 26 de dezembro de 2023. Já no apagar das luzes do ano passado, nós conseguimos, então, a publicação, o Presidente da República assinou o decreto estabelecendo essa política com todas essas... É uma iniciativa muito importante. Nós não tínhamos uma política ainda dando essa orientação geral para os esforços na temática de cibersegurança. Nós tínhamos uma estratégia, que está sendo revisada, como eu disse, mas, como era a primeira estratégia, sem orientação de uma política, e, também, como foram, Senador, as primeiras estratégias em outros países, tinha um teor muito acadêmico e pouco operacional, vamos dizer assim, ou seja, as estratégias mais modernas, estudando muitas delas, nós vemos que têm um teor e uma orientação mais operacional, uma coisa mais operativa, com indicadores, com muitas delas já atribuindo o volume de recursos orçamentários para sua implementação, inclusive.

Então, os princípios ali.

É muito interessante destacar – eu não vou nem citar isoladamente um deles porque todos são muito importantes – a soberania nacional e a priorização dos interesses nacionais; a garantia dos direitos fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade e o acesso à informação; a prevenção de incidentes e de ataques cibernéticos, em particular aqueles dirigidos a infraestruturas críticas nacionais e serviços essenciais prestados à sociedade; a resiliência das organizações públicas e privadas a incidentes e ataques cibernéticos; a educação e o desenvolvimento tecnológico em segurança cibernética; a cooperação entre órgãos e entidades públicas e privadas em matéria de segurança cibernética e a cooperação técnica internacional na área de segurança cibernética. São esses os princípios.

Continuando agora com os objetivos da Política Nacional de Cibersegurança: promover o desenvolvimento...

Todos os objetivos têm relacionamento, obviamente, com os princípios e também com as atribuições, com as competências do próprio Comitê Nacional de Cibersegurança.

Então, os objetivos agora: promover o desenvolvimento de produtos, serviços e tecnologias de caráter nacional destinados à segurança cibernética; garantir a confidencialidade, integridade, autenticidade e disponibilidade das soluções e dos dados utilizados para o processamento, o armazenamento e a transmissão eletrônica ou digital de informações; fortalecer a atuação diligente nos ciberespaços, especialmente das crianças, dos adolescentes e dos idosos; contribuir para o combate aos crimes cibernéticos e às demais ações maliciosas nos ciberespaços; estimular a adoção de medidas de proteção cibernética e de gestão de riscos para prevenir, evitar, mitigar, diminuir e neutralizar vulnerabilidades, incidentes e ataques cibernéticos e seus impactos; incrementar a resiliência das organizações públicas e privadas a incidentes e ataques cibernéticos; desenvolver a educação e a capacitação técnico-profissional em segurança cibernética na sociedade; fomentar as atividades de pesquisa científica, de desenvolvimento tecnológico e de inovação relacionadas à segurança cibernética; incrementar a atuação coordenada e o intercâmbio de informações de segurança cibernética entre União, estados, Distrito Federal e municípios, os Poderes Executivo, Legislativo e Judiciário, o setor privado e a sociedade em geral; desenvolver mecanismos de regulação, fiscalização e controle destinados a aprimorar a segurança e a resiliência cibernéticas nacionais; implementar estratégias de colaboração para desenvolver a cooperação internacional em segurança cibernética.

O único dos objetivos que destacamos foi esse em vermelho, com a margem e a borda em vermelho: desenvolver mecanismos de regulação, fiscalização e controle. Isso aí, já na política, então, inserimos esse objetivo como o que almejamos, que é exatamente a criação de um órgão que tenha essas atribuições de regular, fiscalizar e controlar o ambiente cibernético. Pode ser, Senador, por meio de uma agência, por meio de um centro; o formato tem várias possibilidades, está sendo muito bem estudado pelo Comitê Nacional de Cibersegurança. Tem um grupo de trabalho já debruçado sobre a melhor formatação desse órgão, que terá que existir para regular, fiscalizar e controlar as atividades relacionadas à segurança cibernética no Brasil.

E, logicamente, essa iniciativa, Senador, passará por esta Casa. Vai ser, logicamente, por meio da proposta de um projeto de lei, que terá o aprimoramento, certamente, aqui, no Congresso Nacional.

São estes os instrumentos estabelecidos na política: uma Estratégia Nacional de Segurança e o Plano Nacional de Cibersegurança. Essa estratégia vai transformar aqueles grandes objetivos em

medidas mensuráveis, outros objetivos intermediários que permitam alcançar aqueles grandes objetivos estabelecidos na política. Já há um trabalho que nos apoia, do BID – nós temos até um exemplar para deixar aqui, Senador –, que estudou 17 países, mais de 30 estratégias nacionais. Tem países que já estão na sua terceira estratégia nacional de cibersegurança. Então, há uma evolução ao longo do tempo, daquelas mais teóricas, mais acadêmicas, para estratégias mais operacionais, com objetivos, com propósitos mais bem definidos e inclusive estabelecendo a necessidade de indicadores para que se acompanhe a evolução dessas medidas no campo da cibersegurança. Então, já existe um grupo de trabalho do CNCiber estudando a revisão da nossa Estratégia Nacional de Cibersegurança, e, posteriormente, a estratégia vai se desdobrar ainda num Plano Nacional de Cibersegurança.

O Comitê, que foi também estabelecido, por decreto, pela nossa Política Nacional de Cibersegurança, suas competências estão todas também relacionadas àqueles objetivos: propor atualizações para o PNCiber, em relação a Estratégia Nacional de Cibersegurança, que já está acontecendo – tem um grupo já revisando essa estratégia anterior e, posteriormente, irá elaborar também o Plano Nacional de Cibersegurança; avaliar e propor medidas para incremento da segurança cibernética; formular proposta para o aperfeiçoamento da prevenção, detecção, análise e resposta; propor medidas para o desenvolvimento da educação e segurança cibernética; promover interlocução com entes federativos; propor estratégias de colaboração para o desenvolvimento da cooperação técnica internacional; manifestar-se por solicitação do Presidente da Creden (Câmara de Relações Exteriores e Defesa Nacional) sobre assuntos relacionados à segurança cibernética.

A composição desse comitê. São 25 integrantes, sendo que aqueles em azul mais escuro estão no nível de ministério: o Gabinete de Segurança Institucional, a Controladoria-Geral da União, a Casa Civil, o Ministério do Desenvolvimento, Indústria, Comércio e Serviços; o Ministério da Fazenda, o Ministério da Defesa, o Ministério da Educação, o Ministério da Justiça e Segurança Pública, o Ministério das Comunicações, o Ministério da Ciência, Tecnologia e Inovação; o Ministério das Relações Exteriores, o Ministério de Minas e Energia, o Ministério da Gestão e da Inovação em Serviços Públicos. Logo abaixo, o Comitê Gestor da Internet, a Anatel e o Banco Central, e mais nove integrantes, sendo três de entidades da sociedade civil, três de instituições científicas e tecnológicas de inovação e três de entidades do setor empresarial, todos, logicamente, relacionados à segurança cibernética. Então, são 25 integrantes.

Os três grupos de trabalho já em funcionamento, grupos de trabalho temático já em funcionamento. Tem um grupo já debruçado sobre a Estratégia Nacional de Cibersegurança para atualizar, revisar uma estratégia que já existe e que já está vencida. Como eu disse, lá atrás ela tinha

um prazo de validade – vamos dizer assim – de quatro anos, e já estamos no quinto ano; então, ela está sendo revisada para, em breve, ser colocada em vigor; um grupo de trabalho internacional para definir os parâmetros de atuação internacional do Brasil em cibersegurança – quem está à frente desse grupo de trabalho temático é o Ministério das Relações Exteriores, da mesma forma que, do anterior, é o Comitê Gestor da Internet no Brasil –; e um terceiro grupo, o grupo de trabalho de governança, para a elaboração da proposta de projeto de lei para a criação de um órgão para a governança da cibersegurança, justamente uma possível Agência Nacional de Cibersegurança ou um centro – como isso está em estudo, está em avaliação a melhor forma de ser proposto esse órgão de governança. Esse grupo está a cargo do Ministério da Gestão e da Inovação em Serviços Públicos e da Anatel; uma co-Presidência desse grupo de trabalho, uma Presidência compartilhada.

Alguns fatos e dados relacionados. Esta imagem é bastante complexa – vamos dizer assim – para mostrar também como é complexo o sistema de cibersegurança no Brasil, um país de dimensões continentais, com uma população de quase 220 milhões de habitantes, que tem uma complexidade também nessa área de cibersegurança. Aqui, à esquerda, está a defesa cibernética, num verde mais claro aqui, parte da defesa cibernética; e, já do lado direito, a segurança cibernética.

Em relação à defesa, nós já comentamos alguns desses órgãos que integram o Ministério da Defesa – as Forças Armadas, o ComDCiber, que é o Comando Conjunto, o Centro de Defesa Cibernética do Exército e por aí vai, com essas relações também de defesa cibernética e de infraestruturas críticas com outros países, órgãos e organismos multilaterais.

O Governo Federal tem aqueles Ministérios, como o Ministério da Justiça e ministérios em geral, que têm a si vinculadas agências reguladoras, como a Cnen e todas as agências reguladoras. Mais ainda para a direita, estão o GSI, o Ministério da Gestão e da Inovação, o MCTI; são os ministérios mais envolvidos neste âmbito, especialmente no âmbito governamental, com a temática da cibersegurança.

E todos aqueles desdobramentos... Nós vemos mais à direita o .br, o Comitê Gestor da Internet, o CERT.br, NIC.br, que é essa organização que tem o Comitê Gestor da Internet a seu controle, juntamente com o CERT.br, que cuida de todo o .br, de todo esse domínio .br no Brasil; então, é de responsabilidade do Comitê Gestor da Internet. Aqui é para vocês verem que é um grande sistema, especialmente vendo a área de Governo, em relação ao universo no qual se insere a cibersegurança.

Sobre a maturidade em cibersegurança do Brasil, esse gráfico aí tem um pequeno deslocamento do pentágono mais escuro e do pentágono mais claro. Esse afastamento dos vértices demonstra que,

quanto mais próximo, logicamente, mais completo – vamos dizer assim – o pentágono, o que significa que o país está em melhores condições.

Então, aquele vértice de medidas técnicas, *technical measures*, com o grau 18.73... quando o grau está completo, é 20.0. Então, ali é onde estão os mais fracos, segundo a avaliação daquele órgão, o Global Cybersecurity Index, do International Telecommunications Union (ITU). Segundo esse instituto, nessas duas áreas de medidas técnicas e medidas organizacionais, é onde estamos um pouco mais fracos, ou seja, isso estabelece depois um *ranking*, que nós podemos ver aqui.

Em relação ao Brasil, vemos que, nas Américas, o Brasil está em terceiro lugar, atrás somente dos Estados Unidos e do Canadá. E, no mundo, o Brasil está lá em 18º lugar, depois de vários países – segundo esses indicadores e essa metodologia.

(*Intervenção fora do microfone.*)

O SR. MARCOS ANTONIO AMARO DOS SANTOS – É o país todo, mais geral. Tem outros indicadores, vamos mostrar mais alguns aqui, na frente, também.

Esse é um indicador... é um sistema também que nós estamos adotando, por base, da Universidade de Oxford: Capacidade de Segurança Cibernética do Brasil – Cyber Maturity Model –, que é um sistema de medição de maturidade, que é muito na base de consultas, de pesquisas, com cinco setores: um de padrões de tecnologias, outro de política e estratégia de cibersegurança, de cultura e sociedade da segurança cibernética, construindo conhecimentos e capacidade de segurança cibernética, e outro de marcos jurídicos e regulatórios.

Quanto mais longo, quanto mais próximo do círculo de maior diâmetro, maior é o grau – vamos dizer assim. O país está em uma situação melhor quanto mais longos forem aqueles setores do círculo.

Essa aqui é a segunda avaliação que a Universidade de Oxford fez no Brasil, no ano de 2023; então, já é a segunda. Evoluímos em alguns aspectos e encolhemos em outros. Nesses em que houve uma pequena degradação, não significa que nós pioramos, mas que foram introduzidos outros parâmetros de medição principalmente, ou seja, para completar aquele círculo mais externo, nós temos muito caminho ainda para percorrer.

Em relação à insegurança cibernética como risco mundial, isso aí também é uma avaliação feita pelo Fórum Econômico Mundial, Riscos Globais, um levantamento de percepções aí, já de 2024. Nós vemos que a insegurança cibernética aqui está em quarto, quando se considera que o horizonte é de dois anos. Então, em quarto, a insegurança cibernética.

Depois, ela vem aqui para oitavo, já num horizonte de dez anos, mas a gente vê que não foi uma queda muito grande, considerando que todos os que foram acrescidos aqui, à frente, estão relacionados a este parâmetro aqui: eventos climáticos extremos. E aí, consequências também da primeira, foram incluídas outras três ali, à frente, da insegurança cibernética, ou seja, é um risco global reconhecido plenamente, não apenas no Brasil, mas mundialmente. A insegurança cibernética é considerada um grande risco, especialmente no curto prazo aqui, mas também num horizonte de dez anos.

Estão surgindo aqui outras preocupações, como, num período maior aqui, *misinformation*, *disinformation* aqui, informação e desinformação, e efeitos adversos das tecnologias de inteligência artificial.

Ainda aqui, uma coisa que interessa também: dados sobre cibersegurança. Regulações cibernéticas são consideradas um método eficaz para reduzir os riscos cibernéticos. Então, pesquisas realizadas, aqui, também do Fórum Econômico Mundial, mostram que, neste caso, você acredita que as regulamentações cibernéticas e de privacidade reduzem efetivamente os riscos cibernéticos? Trinta e nove por cento acreditam que sim – eram somente, em 2022, 39%; em 2024, já são 60%, ou seja, tem aumentado a percepção de que uma agência ou um órgão regulador, controlador, fiscalizador reduz os riscos cibernéticos. Em 2022, os que não acreditavam eram 24%, e já caiu para 18,8% em 2024; ou seja, é muito interessante observar que, possivelmente, a criação de um órgão de regulação, fiscalização e controle contribuirá para reduzir essa percepção de risco.

Outro aqui: há uma crescente desigualdade cibernética entre organizações que são ciber-resilientes e aquelas que não o são. Também aqui, nós vemos que, em 2022, 14% dessas que consideram que a resiliência é insuficiente – 14%. Isso aqui, considerando qual o estado da resiliência cibernética da sua organização neste ano. Aqui em 2022, 14%; em 2023, 21%; em 2024, 25% acreditam que é insuficiente. Nessa linha mediana aqui, 67% acreditam que atende o mínimo de requisitos de resiliência: 67%, 51% e 36%. E esses que estão totalmente resilientes excedem os requisitos: 19%, 28% e 39%, em 2024.

No entanto, quando a gente vê aqui essa distinção entre organizações que têm poder econômico menor, elas sofrem mais em relação a este aspecto quando comparadas com organizações que têm receitas de maior vulto. Então, essas percepções mudam conforme o poder das organizações, e aquelas que têm poder econômico menor sofrem mais em termos de resiliência cibernética – essa percepção tem crescido quanto a isso.

Aqui também: a escassez de competências cibernéticas de talentos continua a aumentar a um ritmo alarmante. Também é um gráfico muito interessante, que demonstra a dificuldade e a escassez quanto a pessoas competentes para trabalhar na área de segurança cibernética, pessoas capacitadas.

A escassez de competência cibernética de talentos continua a aumentar a um ritmo alarmante. A pergunta é: a sua organização possui as habilidades necessárias para responder e se recuperar de um acidente cibernético? Em 2022, 88,3% das empresas de maior porte acreditavam que tinham essas capacidades – continua muito próximo do que se tinha. No entanto, naquelas de baixo poder econômico, de 94,7% em 2022, cai para 49,6%; ou seja, tem aumentado a percepção da ameaça e a capacidade de resposta das empresas de menor poder aquisitivo, de menor capacidade econômica e poder econômico. Essas são as que mais sofrem.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Envolvendo pessoas, pode servir também ao aumento da insegurança a percepção de que não há preparo.

O SR. MARCOS ANTONIO AMARO DOS SANTOS – Possivelmente sim, Senador. Acreditamos que sim. Em relação a pessoas, sim.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – É uma percepção crescente, apesar de ser decrescente ali... O decrescente é a segurança, não é, Senador?

O SR. MARCOS ANTONIO AMARO DOS SANTOS – Decrescente é a segurança.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Ou seja: a percepção de insegurança é porque eu estou percebendo que eu não estou equipado, inclusive pessoalmente.

O SR. MARCOS ANTONIO AMARO DOS SANTOS – Exato.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Ou seja: eu reconheço que o risco é grande, e a minha capacidade não cresceu tanto.

O SR. MARCOS ANTONIO AMARO DOS SANTOS – Outra pergunta aqui é desse outro gráfico: as lacunas de recursos ou competências são o maior desafio para a sua organização quando planejando a resiliência cibernética? A gente vê aqui que as organizações públicas são as que mais têm essa percepção, de que a falta de recursos humanos de competência são o maior desafio. Depois, as empresas médias. As que menos têm essa preocupação, essa percepção, são aquelas empresas de maior poder econômico.

Rapidamente, então, Senador – eu creio que já esteja ultrapassando o meu tempo aqui.

Perspectivas: o que está acontecendo, o que a gente imagina que – no curto e, no máximo, no médio prazo – estará acontecendo? A atualização da estratégia, como já citamos; a elaboração da proposta de projeto de lei para a criação do órgão para governança da cibersegurança nacional...

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Já está sendo elaborado?

O SR. MARCOS ANTONIO AMARO DOS SANTOS – Já está. Tem um grupo de trabalho do Comitê Nacional de Cibersegurança trabalhando sobre isso.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Está em curso.

O SR. MARCOS ANTONIO AMARO DOS SANTOS – Ou seja, já existe.

Como o senhor sabe, Senador, nós já tínhamos um esboço, vamos dizer assim, de um projeto de lei, lá no início. Depois, com a criação do comitê, expandimos essa capacidade de análise, vamos dizer assim, e eu creio que vai ser aprimorado aquilo que já tínhamos em mente.

A elaboração do plano, decorrente da estratégia, a padronização da atuação internacional do Governo Federal em cibersegurança, um grupo de trabalho coordenado pelo Ministério das Relações Exteriores em andamento, a atualização da Política Nacional de Segurança da Informação, que também já tem vários anos – tem que ser atualizada também –, a implantação da Política Nacional de Segurança de Infraestruturas Críticas (PNSIC) e de seu comitê.

Esse comitê também está para... Em 30 dias, imaginamos que esteja estabelecido esse Comitê Nacional de Segurança de Infraestruturas Críticas. Já existe uma estratégia, já existe uma política, mas não temos o comitê – o próprio TCU recomendou a criação desse Comitê Nacional de Segurança de Infraestruturas Críticas.

E a harmonização das iniciativas correlatas à proteção de dados, cibersegurança...

Como nós sabemos, existem muitas ideias, muitas iniciativas isoladas em cada um desses temas. Talvez seja interessante que ocorra uma harmonização dessas iniciativas.

A gente ouve dizer, Senador, que existe uma profusão de agências. Nós temos a Autoridade Nacional de Proteção de Dados, recentemente criada a Autoridade Nacional de Segurança Nuclear, iremos propor um órgão de governança para a segurança cibernética... E não temos, também, um órgão de coordenação e governança de segurança de infraestruturas críticas. Então, talvez seja a

oportunidade de juntarmos algumas dessas temáticas dentro de um mesmo órgão controlador e regulador.

Considerações finais.

O Fórum Econômico Mundial avalia que cerca de 14% do PIB dos países do mundo todo são consumidos pelos crimes cibernéticos. Ou seja: transpondo isso aí para o ambiente nacional, considerando o nosso PIB, 14% do nosso PIB seria R$1,5 trilhão.

Se as iniciativas relacionadas à criação de um órgão de governança, fiscalização e controle resultarem numa economia de 10% do que hoje ocorre, do que se perde, seriam R$150 bilhões. Lógico que não é uma matemática, é uma estimativa, talvez até grosseira, mas o volume de recursos que se perde com crimes cibernéticos, sem dúvida, é inimaginável. Quando a gente observa esses valores, são coisas, assim, são até inacreditáveis essas estimativas, mas isso é o que o Fórum Econômico Mundial estima.

Nós temos aí também, como um convite até, Senador, esse evento internacional previsto para novembro deste ano, um evento de dois dias, com quatro temas, oito painéis, envolvendo aquelas temáticas ali: cibersegurança, tecnologias emergentes, infraestruturas críticas e cooperação internacional.

Vamos organizar esse evento com base também na cooperação de outros órgãos, local a ser definido, mas já estabelecido aqui.

E fica aqui o convite para prestigiarem – os Senadores que puderem, aqueles que aqui estão presentes e que puderem – esse evento, em novembro de 2024.

Era isso o que eu queria apresentar, Senador.

Obrigado.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Muito obrigado ao nosso Ministro.

Antes de passar a palavra, de liberar a palavra para o Senador Fernando Dueire, eu diria o seguinte: esse gráfico anterior que o senhor mostrou, essa última informação, deveria ser o imediatamente anterior. Isso aí deveria ser o primeiro da próxima. Certo? Porque... O estudo que fala do impacto financeiro.

Se o prejuízo estimado é dessa ordem, e nós temos uma outra estatística – eu pediria até que o Diego e o próprio Dr. Molina também me socorrem –... Nós tivemos – se é que essa estatística é confiável – quantos bilhões de tentativas de ataques no Brasil em 2022? Se a minha memória não me falha, cento e alguma coisa..

O SR. MARCOS ANTONIO AMARO DOS SANTOS (*Fora do microfone*.) – Cento e três...

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – ... bilhões de ataques. E, em 2023, isso caiu para 63 bilhões – está certo? Ou seja, houve uma queda de número e um aumento de qualidade no ataque. Dessa ordem: de 103 para 63.

Não sei quantificar... Nessa estatística, não tem uma quantificação de quanto essa lesão financeira seria. O que se sabe é que o ataque está mais sofisticado. Reduziu a quantidade e melhorou, ou seja, piorou – piorou para nós – a qualidade do ataque.

Então, eu acho que isso elimina, de uma vez por todas, aquela despreocupação que motivou a criação desta Subcomissão e motivou, em 2019, que nós criássemos, na Comissão de Relações Exteriores e Defesa Nacional, uma preocupação com a avaliação da nossa situação. Como é que nós estamos no mundo? Estamos desprevenidos? Mais ou menos?

Esse é o comentário que eu gostaria de fazer, porque... Não vou responder. Essa é a nossa missão. Nós temos a missão de avaliar a Política Nacional de Cibersegurança. Para isso, foi criada esta Subcomissão, que tem um prazo definido, ou seja, vamos fazer essa avaliação e entregar para a Comissão de Relações Exteriores e Defesa Nacional. Por isso essa sua apresentação, e eu fixaria este. Este aí é o primeiro eslaide da próxima.

Só isso que eu queria dizer, mas passo a palavra ao nosso Senador Fernando Dueire.

O SR. FERNANDO DUEIRE (Bloco Parlamentar Democracia/MDB - PE. Pela ordem.) – Presidente, Senador Amin, Ministro Marco Antonio Amaro, equipe aqui presente do Ministério, senhoras e senhores.

A exposição que V. Exa. fez, agora há pouco, foi muito didática. Colocou uma régua de tempo para que nós pudéssemos ter muita clareza no desenvolvimento da competência do Estado brasileiro com relação a esse assunto; revelou também a questão das bases, das competências dessa estrutura, do comitê, uma matriz de transversalidade necessária, mas que, de toda forma, mostra o tamanho da complexidade desse assunto dentro do próprio Governo.

Mas, Senador Amin, a gente reforça a preocupação, depois de ouvir essa exposição, em razão da nossa velocidade de resposta.

O senhor colocou, com propriedade, que nós tivemos uma diminuição no volume de ataques, mas, por outro lado, uma sofisticação. Isso mostra, naturalmente, mais eficiência, e é necessária uma capacidade de defesa de forma objetiva.

O Ministro, salvo engano, por três vezes ressaltou aqui a necessidade, ora de uma maneira mais suave, ora de uma maneira mais objetiva, mas sempre elegante, a necessidade de um órgão, de uma agência, para que se tenha efetividade no dia a dia do desenvolvimento desse trabalho.

Dá-nos preocupação quanto – se não me engano, são 32 membros –...

(*Intervenção fora do microfone.*)

O SR. FERNANDO DUEIRE (Bloco Parlamentar Democracia/MDB - PE) – ... 25 – ao tamanho do conjunto e da necessidade que esse conjunto precisa, face às suas outras competências. Cada um está focado em suas outras disciplinas também.

Então, ressalto que foi de muita valia esse encontro aqui.

Abraço o senhor, com relação à apresentação que o senhor fez, de excelente nível, mas saio daqui tão preocupado quanto entrei, porque nós percebemos o tamanho do desafio, e é preciso que nós estejamos efetivamente aparelhados, de forma objetiva, para esse enfrentamento.

Portanto, Senador Amin, se já não é pouco o trabalho da equipe de Governo que faz a gestão dessa atividade, também não é pouco o nosso aqui nas Comissões e nas atividades parlamentares, mas eu vejo, com clareza, que nós também temos um dever de casa muito grande nessa avaliação, de forma que esta Comissão, eu acredito, já está na sua terceira reunião, terceiro encontro, e acho que... Acho não: eu tenho certeza de que nós já avançamos muito com relação à clareza do tamanho do desafio que nós temos pela frente nessa avaliação, nessa responsabilidade de avaliação do que nós estamos garimpando nesses encontros.

De forma que, mais uma vez me congratulo, Ministro, com a sua exposição e cumprimento o Senador Amin pela condução na liderança dos trabalhos aqui da Comissão Especial que trata desse assunto.

Muito obrigado a todos!

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Eu gostaria de acrescentar, não para resposta imediata, mas para consideração do Ministro, da sua assessoria e do Molina – se quiser fazer algum comentário adicional –, um conjunto de perguntas que eu acho que já lhe foi disponibilizado, do nosso e-Cidadania, que eu achei muito interessante.

Rodrigo, do Distrito Federal: "Quais são os principais desafios enfrentados pelo Estado na implementação de políticas eficazes de segurança cibernética?".

Eu acho que o histórico demonstrou como esses desafios foram encarados.

Airon, de Pernambuco, estado do nosso querido Senador Fernando Dueire: "Como os órgãos públicos podem promover a qualificação [...]?".

Se o senhor puder retornar mais um, é o outro; aliás, mais dois. (*Pausa.*)

Mais um.

É aquele em que aparece aquela sensação de insegurança.

Esse aí.

Veja bem, nas grandes organizações, houve um crescimento do pessimismo, vamos dizer assim, da situação de insegurança, mas foi nas organizações menos capacitadas que se percebeu mais a incapacidade. E aqui a pergunta é sobre corpo técnico em TI (Tecnologia da Informação) na segurança e defesa cibernética, como é que se forma esse pessoal.

Fábio, do Rio de Janeiro: "O investimento no setor tecnológico está alinhado ao privado para melhoria profissional e de material?".

Acho que ainda é muito cedo para nós avaliarmos isso, não é? Nós estamos quase que na proto-história para fazer essa avaliação.

O especialista em tecnologia da informação realmente está sendo formado, claro, em muitos estados, com deficiência; em outros, com menos sensibilidade quanto a isso.

No meu estado, propriamente, há uma grande percepção de que faltam recursos humanos, porque nós temos um polo de informática bem desenvolvido, e, por isso, a requisição de gente qualificada é quase que inesgotável.

Hígor, do Distrito Federal – saliento que "Hígor" tem a mesma grafia do centroavante do Avaí, ou seja, não é "Ígor", sem "h"; é com "h". (*Risos.*) O Avaí, aliás, derrotou, numa circunstância absolutamente anormal, o Sport de Recife.

"Quais são as maiores dificuldades que o CNCiber [Agora eu vou adotar a sua pronúncia e nacionalizar a minha: quando tiver "y", eu vou falar "sáiber"; quando for "i", eu vou falar "cíber". Está certo.] vem enfrentando desde a sua criação? Estamos atrasados em relação aos países do Mercosul?".

Isso é uma pergunta que eu acho que pode ser respondida, mas eu já vou passar. Essa o senhor fica devendo, e o Molina também, porque eu acho que é uma pergunta fácil de responder.

Com Mercosul, aí nós só vamos até a Bolívia; não vamos até a Venezuela.

João, do Rio de Janeiro: "Quais medidas estão sendo adotadas frente à grande diferença tecnológica entre os países mais desenvolvidos?".

Essa eu acho que não precisa ser respondida, mas pode ser reconhecida. E nós só falamos aqui do Ocidente, não é? Não falamos sobre Rússia, China, Irã... E nem queremos falar agora.

Ageu, do Distrito Federal: "Há planejamento de aumento do orçamento destinado à defesa cibernética [este aqui deve ter alguma formação militar, porque ele continua:] do Exército Brasileiro?". Ele não perguntou sobre as outras Forças Armadas, nem sobre os civis, nem sobre os eclesiásticos; só perguntou sobre o Exército.

Mas eu queria converter as perguntas em duas, essa relacionada à comparação com os países do Mercosul e o que está sendo...

Quais são as reuniões e contatos que o nosso aparato oficial tem, pelo menos com os países mais desenvolvidos?

E o Molina poderia também complementar, se o senhor determinar.

O SR. MARCOS ANTONIO AMARO DOS SANTOS (Para expor.) – Obrigado, Senador.

Em relação à pergunta "Quais são as maiores dificuldades que o CNCiber vem enfrentando desde a sua criação?", na realidade, no dia de amanhã, nós teremos a segunda reunião do CNCiber, dos grupos de trabalho, a segunda reunião do comitê como um todo, que tem a previsão de quatro reuniões por ano.

Trimestralmente, esse comitê vai se reunir, a não ser que seja convocado extraordinariamente. Então, estamos apenas na segunda reunião. Foi estabelecido o comitê no início deste ano, e estamos apenas na segunda reunião do comitê.

Já temos três grupos de trabalho em andamento, como citamos aqui, e, certamente, ele trará grandes contribuições em relação a essa temática da segurança cibernética.

Em relação aos países do Mercosul, ou mesmo aos países das Américas, nós vimos aqui que o Brasil, num determinado levantamento, numa determinada avaliação, se coloca como o terceiro país no hemisfério ocidental, nas Américas, atrás apenas de Estados Unidos e Canadá. Já no âmbito mundial, o Brasil se colocou ali na 18ª posição.

Então, não estamos atrasados em relação aos países do Mercosul. Um ou outro país, sim, já vem vendo o aspecto da criação de uma agência, de um órgão regulador.

Sim, já existem países sul-americanos que têm órgãos reguladores, como a gente pretende criar aqui. Não significa que, no âmbito de segurança cibernética, estejamos defasados em relação a esses países, em relação à resiliência e à proteção cibernética.

Não sei se o Molina quer também acrescentar alguma coisa...

O SR. ANDRÉ LUIZ BANDEIRA MOLINA (Para expor.) – É, eu gostaria sim.

E, acrescentando, quando a gente compara as dimensões territoriais, populacional, com os outros países da América do Sul, se nós tivéssemos as mesmas dimensões, com certeza estaríamos muito mais à frente, muito mais avançados, mas os nossos desafios, muitos, são justificados pelo tamanho, as desigualdades regionais, o tamanho da população, a dificuldade em alcançar toda a população na parte de conscientização. Então, isso, necessariamente, se coloca como um grande obstáculo para o nosso avanço rápido.

O SR. MARCOS ANTONIO AMARO DOS SANTOS – Senador, eu estava vindo de casa para cá, agora há pouco, e eu estava pensando em uma analogia em relação a essa questão da educação na área cibernética.

O mundo, todos nós aqui ingressamos nesse mundo digital, e esse mundo foi crescendo de forma avassaladora. Hoje, tudo se faz por meio digital: pagamento de contas, compra de passagem... Antigamente, ia lá no aeroporto ou numa agência comprar uma passagem, para imprimir o cartão de embarque somente no local. Hoje, nós mesmos despachamos nossa bagagem. Ou seja, o mundo

digital nos envolveu de maneira muito rápida, e, de maneira geral, nós não nos educamos para viver neste mundo digital.

Fazendo uma analogia, é como se todos nós...

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC. *Fora do microfone*.) – Estamos nos adaptando.

O SR. MARCOS ANTONIO AMARO DOS SANTOS – ... nos adaptando.

Os mais velhos, especialmente, e os mais novos também são aqueles mais vulneráveis.

Eu também estava fazendo uma analogia, e é assim como no trânsito, como se todo mundo começasse a dirigir sem ter carteira de motorista, carteira de habilitação.

As crianças, desde pequenas, são educadas para, ao atravessar a rua, olhar para um lado, olhar para o outro, o sinal vermelho, o sinal verde. As crianças vão sendo educadas, nesse mundo perigoso do trânsito, mas não foram educadas para o mundo digital, da mesma forma como também nós não nos preparamos para vivermos neste novo ambiente, que atinge a todos.

E, com maior possibilidade de sofrerem as consequências, estão os mais idosos e os mais jovens que não têm essa educação digital.

Então, o nosso assessor, o Marcelo Malagutti, nos diz que, somente com esforços na área de educação, se consegue resolver um número muito grande de problemas da área cibernética.

E, às vezes, mesmo tendo conhecimento de determinadas medidas que deveríamos tomar, ainda assim nós deixamos de colocá-las em prática, porque trazem mais dificuldade, algum trabalho para trocar senha todo mês, essas coisas que evitam grandes problemas relacionados à segurança cibernética.

É questão, então, de educação.

É por isso que um dos objetivos, um dos princípios é educação; e é por isso que o Ministério da Educação participa, também, deste Comitê Nacional de Cibersegurança.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – É um dos 13 integrantes do Governo.

O SR. MARCOS ANTONIO AMARO DOS SANTOS (*Fora do microfone*.) – Exato.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Treze, mais três e, depois, nove da sociedade civil, se eu bem me lembrei daquela sua colmeia, onde não havia abelhas.

O SR. MARCOS ANTONIO AMARO DOS SANTOS (*Fora do microfone*.) – Exatamente.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Eu considero que a nossa reunião cumpriu o seu objetivo para o momento.

Eu esclareço que os nossos Senadores, como eu também, estamos sendo chamados para a sessão deliberativa. Hoje temos assuntos relevantes e atuais, de forma que eu me vejo na contingência de dar por encerrada a reunião, não sem antes agradecer a V. Exa., a sua equipe, que prestigiou grandemente esta reunião.

Creio que, antes de encerrarmos a nossa avaliação, deveríamos ter outro encontro – pode ser uma visita que se faça ao gabinete –, mas não tenho dúvida de que vamos depender muito de informações institucionais, ou seja, como vamos desenvolver – não para "trasmente", mas para "frentemente" – as circunstâncias institucionais, ou seja, qual vai ser a ideia de lei de criação do órgão, qual será a participação do... Enfim, a partir daquele último eslaide.

Em homenagem ao Senador Izalci, que comparece, passe, por favor, para aquele último, que fala dos prejuízos. Aqui.

Senador Izalci, nós estamos encerrando a nossa reunião, mas não sem antes lhe conceder a palavra, para o senhor avaliar isso aí.

A estimativa de prejuízos levantada no fórum de...

(*Intervenção fora do microfone.*)

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – ... lá na Suíça... em Davos, na Suíça, na cidade que foi objeto do grande livro de Thomas Mann, o alemão.

Este é o prejuízo que seria estimado ao Brasil: o que os ataques cibernéticos podem produzir, em um ano, seria praticamente 14% do PIB do Brasil, ou seja, seria quase R$1,5 trilhão de prejuízos que nós teríamos.

Até para justificar o esforço de todos nós, como o senhor é o nosso "Contador-Geral do Senado", eu coloco isso como *teaser*, como início para a sua fala que encerrará a reunião.

O SR. IZALCI LUCAS (Bloco Parlamentar Vanguarda/PL - DF. Para interpelar.) – É uma pena que eu estava em outras reuniões. Depois eu vi, quando eu estava entrando no Plenário, a audiência e falei: "Vou para lá, é GSI, é alguma coisa interessante". Não acompanhei, mas vou acompanhar isso.

Nós estamos na área de ciência e tecnologia, somos da Comissão e estamos falando em inteligência artificial, essas coisas...

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Aliás, hoje pela manhã, o ponto alto da exposição feita sobre lítio e sobre terras raras, tanto por parte do Ministério de Minas e Energia e do Ministério da Ciência, Tecnologia e Inovação, quanto da empresa Sigma Lithium... Eu fiz o registro no seu nome. A grande novidade, a partir do ano passado, foi a liberação do FNDCT, esforço para o qual a sua inteligência e a sua dedicação foram essenciais.

O SR. IZALCI LUCAS (Bloco Parlamentar Vanguarda/PL - DF) – Obrigado.

Nós vamos nos aprofundar nisso aí, na segurança cibernética. É o GSI que está responsável por isso lá? Isso é com relação ao Governo, não é? A interferência?

O SR. MARCOS ANTONIO AMARO DOS SANTOS (Para expor.) – É. Nós temos a exposição aqui, Senador, colocando uma linha do tempo, a evolução da defesa cibernética, da segurança cibernética, e temos a incumbência de apresentar, futuramente, um projeto de lei tratando da criação de um órgão para regulação, fiscalização e controle da atividade de segurança cibernética, relacionado à segurança cibernética.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – E essa parte institucional...

O SR. IZALCI LUCAS (Bloco Parlamentar Vanguarda/PL - DF) – Tem alguma coisa nas Forças Armadas já, não é?

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Sim.

O SR. MARCOS ANTONIO AMARO DOS SANTOS – Sim.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Todo esse relatório... A linha do tempo sobre o que foi criado, sim. Agora, em elaboração, é o texto do que seria um projeto de lei institucionalizando...

O SR. IZALCI LUCAS (Bloco Parlamentar Vanguarda/PL - DF) – Ah, legal.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – ... não em termos de Forças Armadas, mas em termos de Brasil.

O dispositivo, vamos chamar assim, a agência, enfim, o órgão caberá ao Governo propor, uma vez que isso vai envolver criação de cargos.

O SR. IZALCI LUCAS (Bloco Parlamentar Vanguarda/PL - DF) – O.k. Vou acompanhar.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Eu digo, certamente.

Nada mais havendo a tratar, agradeço, mais uma vez, a participação das senhoras e dos senhores, dos Senadores em especial, das autoridades aqui presentes, especialmente do Exmo. Sr. Ministro de Estado Chefe do Gabinete de Segurança Institucional, Marcos Antonio Amaro dos Santos, e sua equipe.

Eu percebo que alguns integrantes do comitê estão aqui também. Provavelmente, já vieram para a reunião.

É assim, Eduardo?

(*Intervenção fora do microfone.*)

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) – Quais são os membros do comitê que estão aí? Podem se levantar? (*Pausa.*)

São todos bem-vindos, foram muito bem recebidos e com satisfação por todos nós.

Muito obrigado.

A sessão está encerrada.

(*Iniciada às 15 horas e 02 minutos, a reunião é encerrada às 16 horas e 16 minutos.*)