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

REUNIÃO
30/10/2024 - 5ª - Subcomissão Permanente de Defesa Cibernética

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC. Fala da Presidência.) - Havendo número regimental, declaro aberta a 5ª 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 4ª Reunião da Subcomissão, ocorrida no dia 9 de julho deste ano.

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

Aprovada a ata, que será publicada no *Diário do Senado Federal*.

Conforme pauta publicada, a presente audiência pública interativa tem como objetivo debater as relações entre segurança e defesa cibernética.

Para tanto, recebemos como convidado o Exmo. Sr. General de Divisão Alan Denilson Lima Costa, Comandante de Defesa Cibernética do Exército Brasileiro.

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 nº 0800 0612211.

Tenho a honra de cumprimentar e convidar para integrar esta mesa - já está aqui conosco - o Exmo. Sr. General de Divisão Alan Denilson Lima Costa.

Convido igualmente para se incorporar aqui à mesa o nosso querido Senador Fernando Dueire, por favor.

Quero desde já justificar a ausência do Senador Sergio Moro e de outros integrantes da Comissão de Constituição e Justiça, cuja sessão terminou por volta de 13h30.

Esclareço a todos as diretrizes que seguiremos.

Inicialmente, será dada a palavra ao convidado pelo tempo que julgar necessário para sua exposição inicial. Em seguida, abriremos a fase de interpelações pelas Sras. Senadoras e pelos Srs. Senadores inscritos, pelo prazo de cinco minutos, em blocos de três interpelantes até. Na sequência, o Exmo. Sr. Comandante terá o prazo de cinco minutos para a resposta; e, por fim, poderá ser concedida a réplica e a tréplica, com o limite de até três minutos para ambos.

Gostaria de registrar ainda, além da presença do Senador Fernando Dueire, a presença... Eu vou pedir depois que a Secretaria, por favor, forneça-me o nome dos demais representantes das Forças Armadas aqui presentes, para que eu enuncie os seus nomes, já que não os tenho aqui. E gostaria de registrar também a presença de uma ilustre delegação catarinense. Não pretendo aqui também esgotar os seus nomes, mas começo pelos veteranos Vereadores Lourenço e Miri, das cidades de Navegantes e Criciúma, e demais companheiros que eu pedirei depois que me sejam declinados os seus nomes.

Concedo a palavra, neste momento, ao General Alan Denilson Lima Costa, pelo tempo que julgar útil e adequado, confiando no seu bom senso. *(Pausa.)*

Antes, vou mencionar aqui a presença do General de Brigada Luiz Carlos Soares, do Almirante Marcelo do Nascimento e do Brigadeiro Paulo César Milaré

Com a palavra, o General Lima Costa.

O SR. ALAN DENILSON LIMA COSTA (Para expor.) - Exmo. Sr. Senador Esperidião Amin, Presidente da Subcomissão Permanente de Defesa Cibernética da Comissão de Relações Exteriores e Defesa Nacional, Sr. Senador Fernando Dueire, titular desta Comissão, estimada assistência aqui presencialmente e também virtualmente a esta nossa audiência pública, onde eu vou apresentar os passos que a defesa vem dando na implantação do setor cibernético no âmbito da defesa nacional e trazer então essas informações para que a gente possa debater essa relação entre a segurança cibernética e a defesa cibernética, que é o tema e o que nos traz aqui a esta audiência pública.

Então, o nosso Comando de Defesa Cibernética é o responsável por conduzir o setor cibernético no âmbito da defesa, e isso nasce na nossa Estratégia Nacional de Defesa, que é a de 2008. Então, um detalhe interessante é que o Brasil percebe muito cedo a ameaça cibernética como uma ameaça à segurança nacional e cria um setor estratégico próprio a ser desenvolvido para se contrapor a essa ameaça percebida. Então, nós já tínhamos dois setores clássicos: o setor nuclear, que já vinha sendo conduzido pela nossa Marinha do Brasil; o setor espacial, conduzido pela Força Aérea, e surge um setor novo, o setor cibernético, que, nessa época, em dezembro de 2008, ainda era bastante desconhecido.

Por favor.

Então, quando a gente olha para essa evolução - e nós estamos falando de 14 anos -, nós vemos que foi uma caminhada exitosa, e eu vou dizer o porquê.

Lá em 2008, nós começamos com a Estratégia Nacional de Defesa interpretando o que seria isto: construir um setor de defesa cibernética no país. Criamos a nossa primeira estrutura em 2010, entramos nos grandes eventos, já com a incumbência de coordenar a segurança e a defesa cibernética nesses grandes eventos, a partir de 2012 até 2016, e isso fez com que a gente desenvolvesse essa capacidade e, mais do que isso, desenvolvesse as relações com as estruturas do país que fazem a segurança cibernética praticando, sendo efetivamente empregados na condução da segurança e da defesa cibernética nesses grandes eventos.

O nosso comando nasce somente em 2016, então nós temos oito anos como Comando de Defesa Cibernética. A estrutura se tornou mais robusta e nós, a partir daí, começamos a intensificar a cooperação internacional nessa área - é outro aspecto que eu vou pontuar aqui na nossa apresentação - e, quando nós paramos, em 2022, para fazer uma avaliação, um diagnóstico, a gente percebeu que, nesses 14 anos, nós havíamos construído uma capacidade, obviamente uma capacidade que continua se desenvolvendo, porque qual era o mote à época? Nós temos que tirar o Exército da era industrial e levá-lo para a era da informação, ou seja, usar intensivamente tecnologias da informação.

Eu lembro que, em 2007, foi lançado o iPhone. O primeiro iPhone foi lançado em 2007, então, se a gente se posiciona ali em 2008, a gente vê mais ou menos como era o entendimento, não só das Forças Armadas, mas da população em geral, com relação ao uso dessas tecnologias. E hoje nós estamos imersos em uma sociedade digital, faz parte do nosso dia a dia.

Então, nesses 14 anos, nós construímos essa capacidade, só que agora nós estamos olhando para 2040 - por favor -, já percebendo as transformações que virão pela frente.

Hoje, diversos autores já consideram que nós estamos vivendo a era da inteligência artificial, então o próximo salto é o salto da era da informação para a era da inteligência artificial. E, olhando para 2040, nesse salto de 16 anos, a gente ainda vai encontrar algo desconhecido, que são essas tecnologias emergentes, que são as tecnologias quânticas, que, somadas à inteligência artificial - e hoje nós estamos vivendo o nascimento dessa inteligência artificial -, vão transformar totalmente o que nós fazemos hoje, em termos de defesa cibernética.

Então, a mensagem disso é que nós temos que continuar avançando, e rápido, e nos adaptando de forma muito célere a essas transformações que nós já estamos vivendo. Isso é um alerta. Nós não podemos ser surpreendidos com essas novas tecnologias e com o impacto que isso pode trazer para a defesa cibernética.

A computação quântica vai suplantar qualquer sistema criptográfico, o mais atual que seja. E hoje isso já está sendo tratado em publicações. Hoje ataques estão sendo feitos, e essas informações estão sendo guardadas, essas que estão criptografadas, para que, quando a computação quântica estiver disponível, esses dados classificados, sigilosos, possam ser descriptografados. Então isso é uma realidade.

Então, hoje nós temos que estar preocupados com isso. E por isso que vem a tal da criptografia, dos algoritmos criptográficos pós-quânticos, que é aquela que vai resistir ao advento da computação quântica. São algoritmos que hoje já estão disponíveis e têm que ser implementados, até de forma célere, nas nossas infraestruturas, para proteger aqueles

ativos que são críticos, porque com o advento da computação quântica, essa criptografia convencional hoje e nada será a mesma coisa. Não estaremos protegidos.

Por favor.

E o nosso Comando de Defesa Cibernética é o encarregado de conduzir esse setor no âmbito da defesa. Então nós somos um comando operacional conjunto, permanentemente ativado e com capacidade interagências. Esse é o nosso comando. Aqui eu tenho comigo os nossos oficiais generais. Essa é a nossa organização de alto nível. Então o Comandante de Defesa Cibernética.

E eu tenho o Centro de Coordenação de Operações Cibernéticas, coordenado pelo Almirante Marcelino, que está aqui conosco, o Centro de Gestão Estratégica, pelo Brigadeiro Milaré, que também se encontra aqui conosco, o Centro de Defesa Cibernética, que é o braço operativo do comando. Ali estão os nossos especialistas técnicos, comandados pelo General Luiz Carlos. E a nossa Escola Nacional de Defesa Cibernética, que eu vou falar um pouco sobre isso, que é a responsável pela capacitação da nossa força de trabalho, dos nossos recursos humanos especializados, comandada pelo Coronel Cordeiro, que também está aqui conosco. Então essa é a nossa organização de alto nível.

Por favor.

E como nós estamos posicionados em âmbito nacional? Nós já tivemos aqui, na Subcomissão, a exposição do GSI, quando o Ministro, General Amaro, apresentou essa mesma figura; mas agora eu quero explorar na ótica do Comando de Defesa Cibernética.

Então, em nível político, a segurança cibernética é atribuição do GSI. Ele faz a coordenação, normatiza, em âmbito nacional, a segurança cibernética. E o Comando de Defesa Cibernética atua no nível estratégico, implantando esse sistema no âmbito das Forças, no âmbito da defesa; atua como um comando operacional permanentemente ativado; e entrega capacidades para o nível tático. Esse é um aspecto importante que eu vou abordar mais à frente.

Então essa relação com a segurança cibernética, essa interlocução é muito fluida. E nós estamos em contato praticamente diário com o GSI. Inclusive temos o representante do GSI aqui nos prestigiando nesta atividade, Brigadeiro Luiz Fernando, da secretaria que trata o tema de segurança cibernética no país.

Próximo, por favor.

Essa é a nossa missão síntese, como órgão central do Sistema Militar de Defesa Cibernética. Então o comando enxerga a defesa como um todo. Desenvolver e aplicar a capacidades cibernéticas. Então, o nosso foco é a operacionalidade. Obviamente essa capacidade militar é da defesa nacional.

Então, se nós precisarmos aplicar com ênfase a expressão militar do poder nacional e uma resposta a um problema de segurança, aí estarão os nossos especialistas com essa capacidade disponível para a nação. Então, essa é a essência da força militar e da capacidade militar.

Por favor.

Uma portaria do MD, de 2020, define as nossas principais tarefas, competências. E é o que eu vou explorar aqui durante a minha apresentação.

Ao centro nós vemos o que está lá na nossa missão. É desenvolver e aplicar capacidades militares - é a nossa essência. Mas também nós colaboramos com o GSI nos assuntos relacionados à segurança de infraestruturas críticas de interesse da Defesa Nacional. Vamos exemplificar como estamos fazendo isso com o GSI.

Uma outra tarefa importante é propor e executar cooperação internacional no setor de interesse da Defesa. Também vamos falar sobre isso.

Obviamente: assessorar o Ministério da Defesa e os comandos das forças no emprego da capacidade cibernética e fomentar o desenvolvimento de soluções tecnológicas de interesse da defesa cibernética.

Então, são as grandes áreas que nós trabalhamos. São eixos que são efetivamente guarnecidos e nós temos diversas ações para exemplificar essas atividades. Eu vou começar pelo central, pelo desenvolver e aplicar capacidades.

Pode prosseguir, por favor.

Se falamos em desenvolvimento de capacidades nessa área, o foco tem que estar nos recursos humanos, na força de trabalho. Nessa atividade especializada de defesa cibernética, a maior parte está no especialista, no homem, na mulher que trabalha efetivamente como especialista de defesa cibernética.

Nós temos uma escola onde nós temos capacitação em todos os níveis. Nós trabalhamos desde o nível de fundamentos, para aqueles que estão ingressando no setor; passando pelo nível de infraestrutura, para aqueles que estão provendo os serviços e têm que prover esses serviços com segurança - então, nós temos capacitação para esses homens e mulheres que estão nos

postos de trabalho, efetivamente - e também há cursos específicos para as operações cibernéticas defensivas e ofensivas. Nós vemos ali que nós temos, ao centro, uma zona onde esses cursos são de interesse tanto para as atividades defensivas quanto para as atividades ofensivas. Esse mosaico de cursos forma efetivamente um bom especialista nessa área.

Interessante é que o olhar do Comando de Defesa Cibernética não é somente para aqueles militares que estão trabalhando conosco no Comando de Defesa Cibernética. Como eu disse, nós somos o órgão central de um sistema. Então, nós olhamos para todo o sistema militar de defesa cibernética. Esses especialistas que estão na Marinha, no Exército e na Aeronáutica, desdobrados no território nacional, protegendo as nossas infraestruturas críticas da informação, são alvos dessa capacitação e formam a nossa força de trabalho. Isso é o mais importante: a nossa força de trabalho não está no Comando de Defesa Cibernética, ela está nos especialistas que formam o sistema.

Próximo, por favor.

Isso permite que o Comando possa trabalhar nisso que é o principal, a geração de força.

Então, eu tenho condições de, usando os especialistas do setor -requisitando, mobilizando -, organizar esses destacamentos de especialistas para apoiar uma operação conjunta ou uma operação singular. E hoje nenhuma operação ocorre sem a capacidade cibernética estar sendo empregada. Todas, estamos presentes em todas as operações, sejam conjuntas, sejam singulares.

Nesse lado esquerdo aqui do destacamento conjunto, do emprego em operações, eu incluo também a possibilidade de um apoio à segurança cibernética nacional. Então, obviamente que no caso de uma demanda de que a defesa possa ser empregada em apoio à segurança cibernética nacional, o Estado-Maior Conjunto das Forças Armadas e o Ministério da Defesa serão acionados e nós estaremos disponíveis para apoiar qualquer eventualidade que assim ocorra. Para isso que a capacidade existe e está disponível para a nação brasileira.

O próximo, por favor.

Um outro ponto importante nessa relação nossa com o GSI, especificamente com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, é a nossa Rede Federal de Gestão de Incidentes Cibernéticos. Então, o Comando de Defesa Cibernética é o coordenador da nossa setorial de defesa. Nós temos diversas equipes de tratamento de incidentes de rede no nosso sistema que nós coordenamos, nós somos a cabeça do sistema. Mas não é só essa coordenação, a gente provê recursos para a montagem da infraestrutura dessas equipes, nós proporcionamos treinamento para os especialistas dessas equipes e exercícios também de adestramento dessas equipes de tratamento de incidentes. Então, nós podemos dizer que temos uma setorial, realmente, que funciona e que os incidentes cibernéticos que acontecem na nossa estrutura são tratados e são reportados ao GSI por intermédio do nosso Centro de Tratamento de Incidentes de Redes do Governo. Da mesma forma, as outras setoriais têm que fazer o mesmo para que a rede federal funcione como foi concebida lá no decreto de 2021.

Passando para outra tarefa importante, que é a de propor e executar cooperação internacional, eu vou apresentar algumas iniciativas que nós temos.

Essa atividade de cooperação internacional é tão relevante para o setor que tem uma estratégia própria no nosso planejamento estratégico. Então, existe um objetivo estratégico nosso de ampliar as capacidades cibernéticas e nós utilizamos essa cooperação internacional para ampliar essas capacidades. Então, tem uma estratégia específica de ampliar e fortalecer os relacionamentos internacionais do ComDCiber para promover essa estabilidade no espaço cibernético. Na nossa diretriz está lá muito claro por que nós fazemos isso, para posicionar o Comando de Defesa Cibernética e o Brasil como parceiros confiáveis e dotados de elevada capacidade técnica e organizacional para conduzirem ações cibernéticas. Então, isso é o que nos motiva a buscar essa cooperação internacional.

A diplomacia militar é um instrumento das relações internacionais do país. Nesse sentido, nós estamos participando de diversos fóruns internacionalmente. O primeiro deles é esse fórum dos comandantes cibernéticos, que reúne comandantes de cinco continentes. São 46 comandantes cibernéticos de diversos países que se reúnem para a troca de informações, atualidades, sobre como eles estão implementando a defesa cibernética nos seus países.

É uma troca fantástica - experiências recentes dos conflitos que estão ocorrendo no mundo. E nós estamos participando desses encontros desde o ano passado. São dois por ano: ano passado foi na Estônia e na Polônia; este ano, na Estônia e na Espanha, o último. E o Brasil é o único país latino-americano que participa desses encontros, representando aqui a América do Sul.

Próximo, por favor.

Mas, aqui na nossa região, nós também temos o nosso fórum, o Fórum Ibero-Americano de Defesa Cibernética. Nós temos Brasil, Portugal e Espanha e mais dez países latino-americanos nesse nosso fórum, e nós nos reunimos também anualmente.

O objetivo é prover capacitação, treinamento, exercícios e compartilhamento de informações sobre ameaças cibernéticas. Nós temos uma plataforma integrando todos esses centros e comandos, onde nós também trocamos informações sobre ameaças cibernéticas; isso no âmbito da defesa. São órgãos congêneres ao comando de defesa cibernética.

E aqui na nossa região, nós temos de tudo: uns mais maduros, outros ainda em iniciação, e é uma oportunidade de o Brasil cooperar com os países latino-americanos para que a gente possa reduzir de alguma forma essas assimetrias que ainda existem com relação à defesa cibernética nesses países.

Nós também proporcionamos treinamentos. Então, nesse último encontro que nós fizemos do fórum, foi no Rio de Janeiro, agora no mês de setembro. Fizemos um exercício com todos os comandos e centros de defesa cibernética, um exercício virtual.

E, anualmente, nós oferecemos também para as nações amigas um estágio internacional aqui em Brasília. Nós estamos fazendo isso desde 2016, e até hoje são mais de cem oficiais de nações amigas que participaram desse evento conosco. O próximo será em maio do ano que vem. São diversos países. Nós convidamos todos os países com os quais o Brasil mantém relações diplomático-militares para que enviem seus militares para esse treinamento.

Quando nós espacializamos essa informação, o que nós observamos? Os países parceiros aqui da nossa região, da América do Sul, alguns países da América do Norte, o oeste africano, também área de interesse do nosso entorno estratégico, e um ou outro país fora dessas regiões.

Então, é o Brasil se colocando também como um ator aberto à cooperação nessa área, e essa cooperação é eminentemente técnica. São duas semanas em que os especialistas trocam experiências em ambientes virtuais, experiências de nível técnico.

Por favor.

Aí estão os exercícios cibernéticos de que, fruto dessa cooperação internacional, nós estamos participando. Esses são os exercícios deste ano. Nós começamos em fevereiro com um exercício com o Japão, o exercício Cyber Kongo, e passamos todo o ano. O último exercício vai ser agora, em novembro, com o Reino Unido, e vou falar um pouquinho sobre esse exercício.

Eu selecionei três exercícios para tocar com os senhores, mas a gente pode ver ali Japão, Estônia, Reino Unido, Estados Unidos, México, Chile - os países do FIC -, Portugal e Singapura. Então, essas foram as atividades internacionais de exercícios de que nós participamos este ano.

E para o Comando de Defesa Cibernética, isso é adestramento, é uma oportunidade de nós constituirmos os nossos destacamentos e participarmos efetivamente dessas atividades, mas como um adestramento dessa capacidade militar, a capacidade cibernética.

Próximo, por favor.

O primeiro deles que eu quero apresentar é o exercício *Locked Shields.*

Esse exercício é coordenado pelo Centro de Excelência em Defesa Cibernética da Otan. Ele fica em Tallinn, na Estônia. É um exercício anual. É talvez o exercício com maior número de participantes no mundo, não só em termos de países, mas também pela quantidade de especialistas que o país tem que colocar para responder àqueles incidentes que são criados durante o exercício. Ele tem uma parte técnica e também uma parte de jogo de guerra de nível estratégico. Foi em abril, e nós participamos sempre ou com Portugal ou com Espanha, juntamente com esses dois países.

Então, na imagem nós vemos a equipe lá na Espanha, e naquela sala ali, na Espanha, tinha mais de 200 pessoas, especialistas, defendendo o mesmo ambiente de rede. Em Portugal, já tinha umas 50 pessoas. Nós tínhamos especialistas nos dois locais. Um representante em Tallinn, na Estônia, como nossa ligação, e a participação no nível estratégico, onde nós convidamos, para o nosso Comando de Defesa Cibernética, representantes de diversas agências para responder, junto com a Defesa, a esses incidentes.

Então, ali nós vemos o Governo Digital, o Banco Central, o Operador Nacional do Sistema Elétrico, a Anatel, que participaram conosco desse exercício. Então, são oportunidades não só de adestramento para os nossos militares do sistema, mas também para nós exercitarmos essa atuação interagências, porque quando tivermos que ser efetivamente empregados em uma emergência em nível nacional, essa atuação vai ser interagências. Então, também é um momento de treinar e estar em contato com esses atores em âmbito nacional.

E, obviamente, lá em cima está o nosso GSI, sempre conosco nessas atividades.

Próximo, por favor.

O outro exercício também que eu quero trazer foi esse exercício com os Estados Unidos, em maio, agora, deste ano, a Cyber Flag. Esse exercício foi organizado pelo Comando Cibernético americano - nós temos um plano de trabalho com

os Estados Unidos também. E nesse exercício haverá participação todos os anos agora - este ano foi o primeiro. Um exercício muito interessante - o próximo, por favor -, onde o Comando Cibernético americano certifica os seus Cyber Protection Teams.

Então, ali nós vemos que cada organização de cibernética do Exército, da Marinha, da Força Aérea apresenta dois Cyber Protection Teams para serem certificados. Alguns países ali, dos *Five Eyes*, também, com seus Cyber Protection Teams e alguns países convidados.

Eu gosto de olhar essa imagem - o próximo, por favor -, espacializando essa informação. E aí a gente consegue ver os participantes desse exercício. Um exercício cuja finalidade era a proteção de uma infraestrutura crítica de energia, exatamente aquilo que nós procuramos também praticar no nosso Guardião Cibernético deste ano - eu vou falar um pouquinho mais à frente sobre esse exercício.

Mas essa experiência nós internalizamos. Basicamente, é uma infraestrutura crítica de energia que está passando por problemas em seus sistemas, e a Defesa é chamada a cooperar com os técnicos daquela empresa para a solução do problema. Então, é basicamente a busca avançada de ameaça profunda. Então, exige um conhecimento técnico muito grande, e é por isso que eu digo que esses exercícios para nós são adestramentos. É aonde nós vamos levar os nossos especialistas para que realmente apliquem essas capacidades em situações muito próximas do real.

O próximo, por favor.

E o exercício, agora, com o Reino Unido, que vai ser no próximo mês, é a Cyber Spartan, que também é um exercício onde o Exército britânico certifica as suas unidades de comunicações na parte da proteção cibernética. Então vamos participar agora, também em novembro, com o Reino Unido.

Então são exemplos de exercícios, de atividades, de treinamentos, fruto de cooperação internacional, que permite essa troca de informações, troca de boas práticas, troca de intercâmbio de técnicas, táticas, procedimentos, em um ambiente simulado - hoje esses exercícios simulam realmente um ambiente bastante próximo do real.

Por favor.

Esse quadro sintetiza, Senador, as nossas cooperações internacionais. Claro que tudo isso nasce de reuniões bilaterais, por intermédio do Ministério da Defesa ou do Comando do Exército, e são estabelecidos entendimentos bilaterais, e a partir daí a gente chega até esse nível de poder participar de exercícios de forma conjunta com esses países. Então é um leque realmente de oportunidades para que possamos intercambiar boas práticas nessa área de defesa cibernética, e isso tem contribuído e muito para alavancar a capacidade cibernética no âmbito da defesa.

Próximo, por favor.

No que diz respeito à colaboração com o GSI, no que diz respeito à proteção de infraestruturas críticas de interesse da defesa, a primeira é a nossa participação no Comitê Nacional de Cibersegurança. Então essa lâmina também foi apresentada pelo Ministro General Amaro, e o Comando de Defesa Cibernética - mais um, por favor -representa o Ministério da Defesa no comitê. Então é o olhar da Defesa nos assuntos relacionados à segurança cibernética. E nós temos três grupos de trabalho em andamento, um revisando a Estratégia Nacional de Segurança Cibernética, outro grupo trabalhando numa proposta de projeto de lei para criação de um órgão de governança, uma agência, um centro, o que seja, para coordenar esses trabalhos em âmbito nacional, e outro grupo que foi chefiado pelo MRE, esse já está concluído, que tratou de cooperação internacional, sabendo que esse tipo de atividade é fundamental para a gente desenvolver e também inserir o Brasil nesse contexto, no sistema internacional, tratando desses aspectos relacionados à segurança e defesa cibernética.

Próximo, por favor.

Outra atividade que materializa essa cooperação com a segurança cibernética é o nosso exercício, o Guardião Cibernético, que nós fizemos agora, de 14 a 18 de outubro. Nós já estamos com todos os setores das infraestruturas críticas participando efetivamente do nosso exercício.

A próxima, por favor.

Essa lâmina mostra a evolução do exercício. Então nós começamos em 2018 com 23 organizações. Este ano, agora, nós vamos ver mais a frente, já passamos de 140 organizações, passamos de 600 pessoas participantes do exercício. E levamos esse exercício para a Escola Superior de Defesa, com instalações muito apropriadas para receber não só um efetivo desse tipo, mas para conduzir um exercício dessa magnitude, que é o Guardião Cibernético.

Próximo, por favor.

Esse outro eslaide mostra as organizações, as empresas, por setor. Então aí nós temos todos os setores das infraestruturas críticas. E quando a gente olha ali para qualquer um daqueles setores, a gente identifica os principais atores no país; ou seja, é um exercício que tem atraído o interesse das organizações porque elas percebem que isto é extremamente positivo para as suas organizações: praticar como responder a um problema cibernético que ocorra nas suas estruturas.

Outra coisa interessante: quem convida as empresas são as agências reguladoras. Então, elas mobilizam as empresas para participar dos exercícios, elas trabalham os problemas simulados com as suas organizações, com as suas empresas, com os órgãos regulados, com base naquilo que está acontecendo no mundo. Então, a gente pega as experiências que estão acontecendo no mundo de problemas no espaço cibernético: "E se acontecessem aqui no Brasil, como o setor reagiria?". E é o momento de colocar todos esses entes reunidos, e o principal: em contato com os órgãos parceiros. Isso talvez seja o mais importante do Guardião Cibernético, porque, para aquele problema simulado, ele tem ali, na própria escola, os representantes dos órgãos parceiros que vão ajudá-los na solução daquele problema. Então, a troca, essa rede de relacionamentos que se forma é fantástica. Por isso, as organizações percebem o exercício como algo relevante e importante e, durante cinco dias, enviam seus representantes para participar desse exercício.

O próximo, por favor.

Aí algumas imagens do nosso exercício. Nós vemos muitos civis; o exercício é para as organizações civis, a maioria deles. Embaixo, nós vemos ali a dinâmica. Embaixo, à direita, nós vemos quatro pessoas. Aquilo ali representa o gabinete de crise de uma empresa. Ali estão um representante da direção da empresa, um representante do setor de TI, um da jurídica e outro da comunicação estratégica. Eles estão ali tratando de como aquela organização vai reagir àquele problema cibernético e compartilham isso com o coordenador que está na outra sala, na direção do exercício - é essa sala, à esquerda, aí embaixo -, que vai avaliar se a resposta foi adequada, segundo os protocolos do setor; se não estiver, devolve-a e interage com a equipe. Ou seja, é um trabalho bastante intenso de simulação construtiva que nós chamamos. É um jogo de guerra de simulação construtiva em que eles têm que esgotar o assunto em relação àquele problema simulado.

O próximo.

Mas também nós temos uma dinâmica de simulação virtual. Então, já não são mais aqueles representantes da empresa, e, sim, os técnicos. Cada empresa também manda um especialista, o camarada que está lá nos bastidores defendendo os sistemas para que possa também participar de uma simulação virtual. E olha o interessante: naquelas mesas ali, eles estão agrupados por setores, por exemplo, setor de telecomunicações. Nós temos ali vários especialistas que muito provavelmente não se conheciam, mas que trabalham com o mesmo problema: proteger a infraestrutura das suas organizações, e começam a trabalhar juntos, a trocar informações e conhecimentos técnicos. A gente pode perceber o ganho que é um exercício dessa natureza.

E, do lado direito, a simulação de defesa - como eu mencionei, era exatamente aquela fotografia -, um destacamento conjunto sendo empregado em apoio a uma infraestrutura crítica de energia que estava passando por problemas. Então, foi a dinâmica de simulação virtual; essa foi própria de defesa.

Na sequência... Ah, sim!

E nós temos também, no ápice da crise - vejam que são cinco dias de exercício; então, vai em uma crescente -, a conformação de um gabinete de crise. Então, aquilo que estava acontecendo no âmbito setorial, nos âmbitos das organizações, vai crescendo e gera uma crise que tem que ser tratada no nível político.

Ali nós vemos o Secretário-Executivo do GSI coordenando ações de nível político com o Secretário da Casa Civil. Ali temos a embaixadora, temos o Secretário do Governo Digital e outras autoridades de Governo, ali dos ministérios, discutindo o que fazer com aquele problema criado - obviamente fictício, não é? "Qual é a mensagem que nós vamos enviar para a sociedade?". "Qual é a manifestação do Governo?". "Qual é o assessoramento que nós vamos dar ao Presidente?". "Vamos levar esse assunto à Comissão de Relações Exteriores e Defesa Nacional?". Ou seja, são esses os assuntos tratados ali naquele gabinete de crise.

Então, é um momento também de treinarmos a crise, com os atores que estariam presentes, para solucionar esse problema. Isso tudo está dentro do Guardião Cibernético. A gente trabalha no nível das organizações, daquele pequeno gabinete de crise das organizações, trabalhamos no nível técnico e trabalhamos também, no nível político, a resposta a uma crise no espaço cibernético.

E temos um pequeno vídeo de um minuto que mostra o que foi esse Exercício Guardião Cibernético deste ano.

Por favor.

(Procede-se à exibição de vídeo.)

O SR. ALAN DENILSON LIMA COSTA - Bom, Senador, e, como conclusão - essa é a minha última lâmina -, após apresentar como que nós estamos desenvolvendo essas capacidades no âmbito da Defesa, eu quero aqui, nestas minhas considerações finais, deixar bem caracterizada essa disponibilidade da capacidade cibernética que nós estamos construindo, para apoio à segurança cibernética do país.

Não faz sentido termos uma capacidade tão qualificada e só a empregarmos nas operações militares. Não, ela está pronta para ser empregada sempre que estivermos necessitando ou surgir uma situação de crise e, também, como um instrumento da nossa política externa, para contribuir com a estabilidade regional e com a segurança e a paz mundial, nessas relações que nós temos com esses comandos de defesa cibernética em vários continentes, posicionando o Brasil como um parceiro relevante na comunidade internacional de defesa cibernética, reconhecido por sua capacidade técnica e gerencial; e também para passar essa mensagem, que é muito importante, de que temos as nossas Forças Armadas aprestadas, modernas, porque temos uma capacidade cibernética implantada e perfeitamente integrada, em um comando conjunto, onde nós temos militares das três Forças Armadas.

Com isso, Senador, eu agradeço a oportunidade de poder, no tempo disponível, fazer esta breve apresentação sobre o nosso Comando de Defesa Cibernética, sobre o setor cibernético de defesa. E fico à disposição para os debates das perguntas que surgirem.

Muito obrigado, Senador.

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

Quero, em primeiro lugar, cumprimentá-lo pela objetividade da apresentação. Vou solicitar, ainda, que a Secretaria colete, por favor, os nomes dos nossos participantes, para que conste o maior número possível dos presentes na nossa ata decorrente desta reunião.

Eu vou apresentar, depois, ao General Alan as perguntas do e-Cidadania. Foram cinco intervenções dos Srs. Alexandro, de Minas Gerais; Eduardo, do Distrito Federal; seu xará Allan, do Rio de Janeiro; Niraldo, do Ceará; Fábio, de Rondônia; Juarez, de Santa Catarina; Lucas, de Tocantins; e Paulo, de São Paulo.

Em função da premência - hoje é um dia de deliberações -, não podemos estender a sessão indefinidamente. Eu vou solicitar à sua assessoria que, em conjunto com o nosso pessoal, disponibilize as respostas para que nós possamos endereçá-las. Eu vou pedir ao Diego que cuide disso.

Coloco à disposição do nosso Senador Fernando Dueire a palavra, para a sua intervenção, se achar oportuno.

O SR. FERNANDO DUEIRE (Bloco Parlamentar Democracia/MDB - PE. Para interpelar.) - Presidente Senador Esperidião Amin, Sr. General de Divisão Alan Denilson Lima Costa, senhores representantes das Forças Armadas e da sociedade civil aqui presentes...

General, a exposição, como foi colocada pelo Senador Amin, foi objetiva, didática e muito esclarecedora. Traz um histórico importante, com clareza, de 2008, de 2010, de 2012, de 2016, de 2022, como marcos importantes do trabalho, numa régua de tempo bem delineada. Projeta, com clareza, para 2040, um portentoso desafio que se tem à frente e que está se impondo à sociedade brasileira.

Prestei muita atenção à questão dos níveis político, estratégico, operacional, técnico, que foram bem apresentados.

Chamou-me muito a atenção a cooperação internacional, que eu acho que é um condão valioso. Acho não, tenho absoluta certeza, e, pelo que foi desenvolvido até agora, demonstra essa preocupação.

A questão da preocupação com a formação do capital humano... Ele é essencial, é a base.

Foi claramente percebida a presença do GSI, Ministério da Defesa, Governo Digital, ONS, Bacen, Anatel, Comitê Nacional de Cibersegurança.

O que me chama a atenção é que isso é uma massa crítica que precisa... porque é transversal. Na verdade, nós estamos tratando de um assunto que tem transversalidade. Essa articulação, que foi bem colocada, e que, pelo que está relatado, existe em razão até dessa transversalidade e do tamanho do desafio, na minha percepção, na minha modesta percepção, talvez tivesse uma maior ou uma melhor coordenação através de um órgão de governança. Nós estamos falando de um comitê. Um órgão de governança tem competências e condições de enfrentamento talvez mais adequadas em função desse conjunto de agentes envolvidos.

Eu pergunto ao senhor, General, dois pontos: orçamento; e o que o senhor entende, o senhor que vive o dia a dia junto com um conjunto interdisciplinar de colaboradores, por esse organismo de governança? Então, basicamente: orçamento e órgão de governança; porque é tamanho o desafio que até hoje vem sendo enfrentado, mas a complexidade e o que nós

estamos vivendo e com que estamos convivendo, com relação aos ataques, a cada dia exige do mundo e do Brasil uma capacidade de gerenciamento disso mais eficiente.

Portanto, basicamente, órgão de governança e orçamento. É a minha provocação, a minha boa provocação ao que o senhor acabou de relatar.

O SR. ALAN DENILSON LIMA COSTA (Para expor.) - Eu agradeço a pergunta, Senador. Eu vou começar pelo órgão de governança. Olhando o modelo da Defesa, o que a Defesa fez? Para implantar o setor, como estava previsto, na Estratégia Nacional de Defesa, nós começamos a construir uma organização para dar conta desse desafio, porque, quando nós olhamos a implantação do setor, o que nós percebemos? Diversas frentes, e cada frente dessa tem que ser muito bem guarnecida, então, tem que ter uma estratégia própria, tem que ter gente vocacionada para que aquilo avance.

Então, se eu estou falando de cooperação internacional, nós temos que ter uma estrutura que esteja olhando e trabalhando focada em ações estratégicas para atingir esses objetivos relacionados à cooperação internacional. Se eu estou falando em autonomia e independência tecnológica, de soluções nacionais para a defesa cibernética, eu tenho que ter gente trabalhando com esse foco, para que a gente tenha efetividade nessas ações. Se eu estou falando em treinamento, eu tenho que ter gente pensando só em treinamento.

Então, uma estrutura muito enxuta para conduzir um desafio tão grande e com tantas áreas importantes a serem guarnecidas a gente verifica que não vai dar conta. Precisa-se efetivamente de ter uma estrutura maior, mais robusta, para poder fazer essa governança, com um planejamento estratégico muito bem delineado, com ações concretas a se atingir, com instrumentos para que a gente possa medir o atingimento dessas metas. Então, isso tudo remete a uma estrutura mais robusta, é disso que hoje o Brasil necessita. Nós temos uma estrutura ainda incipiente, pequena, que faz essa normatização, essa coordenação, que está no âmbito da Presidência da República, ali no GSI, mas é uma estrutura muito pequena para o desafio que é imenso.

Quando olhamos para modelos internacionais, vemos que outros países estão avançando justamente nessa direção de criar uma estrutura de governança que permita conduzir esse desafio. Essa é a questão. Se colocarmos poucas pessoas para conduzir, nós vamos atingir alguns objetivos.

Agora, eu acho que com a importância que a segurança cibernética está ganhando nos dias atuais e a relevância disso para o país, porque isso pode afetar a segurança nacional, acho que nós temos que encarar realmente esse desafio e estruturar um centro, um órgão - o nome que se dê, a estrutura que se dê -, uma agência, mas que tenha capacidade efetiva de conduzir esse desafio, conduzir essa governança, como o senhor muito bem colocou.

Em termos de recursos financeiros, é difícil até falar em números, porque, se existe uma ameaça, e essa ameaça é percebida, é porque ela explora vulnerabilidades nas nossas infraestruturas. Então, se não tiver um investimento nessa base, nas infraestruturas, vira talvez um parque de diversões para o agente de ameaça, porque fica uma coisa muito fácil de explorar em um sistema. Então, nós temos que investir forte na base, nas infraestruturas. Isso é investimento.

Então, se eu tenho equipamentos obsoletos, se eu tenho uma infraestrutura com sistemas operacionais antigos, se eu não tenho capacidade de fazer esse tipo de investimento em atualizar meu parque tecnológico, eu crio um ambiente de vulnerabilidade que vai ser explorado por essas ameaças. Eu não estou nem falando de elementos especializados em proteção cibernética, de segurança cibernética, estou falando do básico. Às vezes um investimento na nossa infraestrutura, na modernização da nossa infraestrutura, seja o primeiro passo. Ou seja, aqueles órgãos que têm o encargo de proteger os seus ativos de informação têm que ter uma infraestrutura que permita que eles possam, efetivamente, proteger, e isso é investimento. E, em paralelo, obviamente, nós temos que trabalhar a qualificação dessa força de trabalho, para que eles possam prover esses serviços com qualidade, proporcionar segurança não só entregar um serviço, disponibilizar um serviço para uso na organização, mas fazer isso com o pensamento de segurança. Então, temos que investir também na qualificação desse pessoal.

E há outras áreas em que nós também temos que fazer investimento, como no nosso próprio empresariado, para que tenhamos soluções nacionais para poder utilizar nos órgãos da administração pública, nas nossas organizações que tratam de assuntos críticos...

Então, tem uma série de setores que precisam de investimento. Assim, quando falarmos em um número, a gente sempre vai chegar à conclusão de que é pouco. Mas, nesse estágio atual de desenvolvimento, onde vamos aplicar o recurso? Eu acho que nós temos que aplicar o recurso na melhoria das nossas infraestruturas - na Defesa é experiência que nós temos. Se eu não tenho uma infraestrutura adequada, atualizada, na Marinha, no Exército, na Força Aérea, eu abro portas, eu deixo espaços vulneráveis para que essa ameaça entre. E aí, depois, como conversávamos aqui antes da apresentação, é controle de danos. Aí, depois, nós vamos controlar danos.

Então, essa atitude preventiva de atualizar os nossos sistemas é fundamental, talvez seja o grande investimento, senão, as vulnerabilidades estarão ali, e estaremos sempre tratando de controlar danos.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC. *Fora do microfone*.) - Com a palavra o Senador Fernando Dueire.

O SR. FERNANDO DUEIRE (Bloco Parlamentar Democracia/MDB - PE) - Agradeço muito as respostas. Foi muito em direção ao que eu pensava.

Eu queria registrar aqui, por um dever de justiça, que o Senador Amin, pela sua vasta experiência, de Governador, de Senador, algumas vezes, identificou que o Senado Federal poderia oferecer essa contribuição de fazer uma escuta, de ouvir, e articulou esta Comissão com o Presidente da Comissão de Relações Exteriores e Defesa Nacional e com o Presidente do Senado. E veio muito boa hora, porque essa escuta está permitindo que nós possamos ter um conteúdo para apresentar as competências que poderão nos direcionar melhor para esse horizonte além de 40, mas que precisa ser discutido e decidido agora.

Muito obrigado pelas suas respostas e pela sua exposição.

O SR. PRESIDENTE (Esperidião Amin. Bloco Parlamentar Aliança/PP - SC) - Eu reitero o pedido para que o General Alan, por favor, promova posteriormente a resposta a essas questões e que a Secretaria e a nossa assessoria também disponibilizem a resposta para os que formularam as perguntas.

Eu gostaria de dizer que esta reunião tinha como principal objetivo colher essas informações, e ela plenamente cumpriu os seus objetivos.

Eu ressalto que a indagação do Senador Fernando Dueire vem confirmar as nossas cinco prioridades: primeiro, conhecer e avaliar o diálogo institucional entre segurança e defesa cibernética; segundo - e talvez seja o ponto imediatamente mais relevante -, nós precisamos ou não precisamos de uma agência nacional de cibersegurança?; terceiro, qual é a participação do nosso país junto ao concerto dos países da América, especialmente da América Latina, em esforços de investigação colaborativa? Acho que a sua palestra preencheu perfeitamente essa indagação com respostas objetivas; quarto ponto, qual o nível de interoperabilidade dos órgãos e agências governamentais no campo cibernético? Também veio ao encontro disso; e, finalmente, qual o grau de independência tecnológica do Brasil no campo e qual o grau de sua vulnerabilidade cibernética?

Portanto, se eram esses os nossos pontos críticos que convocaram esta reunião, eles foram plenamente satisfeitos pela natureza e pelo conteúdo da sua exposição, de sorte que a nossa reunião cumpriu os seus objetivos.

Nós temos que apresentar, no âmbito da Comissão de Relações Exteriores e de Defesa Nacional, uma proposta que responda a essas questões e a sua participação em muito colaborou para que nós possamos promover uma resposta adequada.

Antes de encerrar, eu quero mais uma vez agradecer a participação de todos quantos, com a sua presença, participaram e deram dimensão a este encontro.

Vou convidá-los todos, aos que puderem ser fotografados, alguns talvez não possam, que depois se postem aqui para nós fazermos uma foto que registre a nossa reunião.

Agradecendo - eu repito o agradecimento - a todos pela sua participação, declaro encerrada a nossa reunião.

Muito obrigado.

(Iniciada às 14 horas e 06 minutos, a reunião é encerrada às 15 horas e 07 minutos.)